S. HRG. 107–1048

# SECURING OUR TRADE ROUTES: POSSIBLE SOLUTIONS

## FIELD HEARING

BEFORE THE

SUBCOMMITTEE ON SURFACE TRANSPORTATION AND MERCHANT MARINE

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

JULY 1, 2002

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

U.S. GOVERNMENT PRINTING OFFICE

93–216 PDF WASHINGTON : 2004

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

ERNEST F. HOLLINGS, South Carolina, *Chairman*

| | |
|---|---|
| DANIEL K. INOUYE, Hawaii | JOHN MCCAIN, Arizona |
| JOHN D. ROCKEFELLER IV, West Virginia | TED STEVENS, Alaska |
| JOHN F. KERRY, Massachusetts | CONRAD BURNS, Montana |
| JOHN B. BREAUX, Louisiana | TRENT LOTT, Mississippi |
| BYRON L. DORGAN, North Dakota | KAY BAILEY HUTCHISON, Texas |
| RON WYDEN, Oregon | OLYMPIA J. SNOWE, Maine |
| MAX CLELAND, Georgia | SAM BROWNBACK, Kansas |
| BARBARA BOXER, California | GORDON SMITH, Oregon |
| JOHN EDWARDS, North Carolina | PETER G. FITZGERALD, Illinois |
| JEAN CARNAHAN, Missouri | JOHN ENSIGN, Nevada |
| BILL NELSON, Florida | GEORGE ALLEN, Virginia |

KEVIN D. KAYES, *Democratic Staff Director*
MOSES BOYD, *Democratic Chief Counsel*
JEANNE BUMPUS, *Republican Staff Director and General Counsel*

---

SUBCOMMITTEE ON SURFACE TRANSPORTATION AND MERCHANT MARINE

JOHN B. BREAUX, Louisiana, *Chairman*

| | |
|---|---|
| DANIEL K. INOUYE, Hawaii | GORDON SMITH, Oregon |
| JOHN D. ROCKEFELLER IV, West Virginia | TED STEVENS, Arkansas |
| JOHN F. KERRY, Massachusetts | CONRAD BURNS, Montana |
| BYRON L. DORGAN, North Dakota | TRENT LOTT, Mississippi |
| RON WYDEN, Oregon | KAY BAILEY HUTCHISON, Texas |
| MAX CLELAND, Georgia | OLYMPIA J. SNOWE, Maine |
| BARBARA BOXER, California | SAM BROWNBACK, Kansas |
| JEAN CARNAHAN, Missouri | PETER G. FITZGERALD, Illinois |
| JOHN EDWARDS, North Carolina | JOHN ENSIGN, Nevada |

# CONTENTS


| | Page |
|---|---|
| Hearing held on July 1, 2002 | 1 |
| Statement of Senator Wyden | 1 |
| Prepared statement | 2 |

WITNESSES

| | |
|---|---|
| Bates, Del, Vice-President, Local 19, International Longshore and Warehouse Union | 50 |
| Prepared statement | 51 |
| Brown, Admiral, Erroll M., Commander, 13th Coast Guard District, United States Coast Guard | 11 |
| Prepared statement | 13 |
| Browning, Douglas M., Deputy Commissioner, U.S. Customs Service | 21 |
| Prepared statement | 23 |
| Cantwell, Hon. Maria, U.S. Senator from Washington | 16 |
| Prepared statement | 17 |
| Cushing, John, President, eMODAL.com | 65 |
| Prepared statement | 66 |
| Dinsmore, Mic, Executive Director, Port of Seattle | 25 |
| Prepared statement | 27 |
| Farrell, Timothy, Deputy Executive Director, Port of Tacoma | 39 |
| Prepared statement | 41 |
| Koch, Christopher, President and CEO, World Shipping Council | 69 |
| Prepared statement | 71 |
| Marcus, Captain Don, Vice-President, Pacific International Organization of Masters, Mates and Pilots | 45 |
| Prepared statement | 48 |
| Murray, Patty, U.S. Senator from Washington | 3 |
| Prepared statement | 7 |
| Schorer, Steven, President, L–3 Communications, Ocean Systems Division | 80 |
| Prepared statement | 82 |
| Verma, Vikram, CEO, SAVI Technology | 60 |
| Prepared statement | 62 |
| Yap, Robert, Executive Vice-President, PSA Corporation | 43 |
| Prepared statement | 44 |

# SECURING OUR TRADE ROUTES: POSSIBLE SOLUTIONS

**MONDAY, JULY 1, 2002**

U.S. SENATE,
SUBCOMMITTEE ON SURFACE TRANSPORTATION AND MERCHANT MARINE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
*Seattle, WA.*

The Subcommittee met, pursuant to notice, at 2:30 p.m. in the Commission Chambers, Port of Seattle, Pier 69, Hon. Ron Wyden, Chairman of the Subcommittee, presiding.

## STATEMENT OF HON. RON WYDEN, U.S. SENATOR FROM OREGON

Senator WYDEN. The Subcommittee will come to order, and I am pleased to be able to be here today in Seattle with my colleagues Senator Murray, and Senator Cantwell, who will be arriving shortly to convene today's hearing of the Subcommittee on Surface Transportation and Merchant Marine as part of the Senate Commerce, Science, and Transportation Committee; and it is a special pleasure to be here with Senator Murray.

Senator Murray is particularly influential in this field as a Chair of the important Appropriations Subcommittee that deals with transportation-related issues, and she has been extraordinarily helpful to the people of Oregon and the Northwest on those issues. I am just going to have a brief opening statement, and then I am going to recognize Senator Murray for her complete statement and the substance of the work that she is doing on these important issues.

This is one of a series of hearings that is being held around the country to look at port security questions, and it comes at a critical time. Right now there is a conference between the House and the Senate on legislation to address a number of important port security issues.

I am a member of the conference committee, and I intend to use this input to work on the conference committee on issues that have special importance to the Pacific Northwest, and of course, will be teaming up with Senator Murray in her work on the Appropriations Subcommittee.

It is very clear to me that seaports are tempting targets for terrorists, when you look at how open they are, how accessible they are, how close to metropolitan areas they are, in many instances.

With respect to Portland and Seattle, both of our ports, both of our major Northwest ports are in the top 20 of the ports nation-

wide in terms of moving cargo in and out. It is clear that these are issues that that we are going to have to spend considerable time on.

Just this morning it was reported in USA Today, the newspaper, it was reported that one of Bin Laden's chief lieutenants had papers that were seized that looked to attacks on tankers and cruise ships; and this was just described this morning. So these are important issues for us in the Pacific Northwest.

There will be a number of issues that we will be examining today in Seattle and in Portland; but suffice it to say the central challenge here is to strike a balance between making sure that there are the national security protections in place—the security protections are essential to the people of the Pacific Northwest—while at the same time promoting the efficiency that is so critical in order to be able to move goods in and out of the Pacific Northwest and have the family wage employment that is tied to international trade.

In the Pacific Northwest, something like one out of six jobs revolved around international trade. The trade jobs pay better than the nontrade jobs, and we have got to find a way to address the security issues while at the same time promoting the free flow of goods and services into, into our region.

There will be a number of issues that we will look at that can facilitate striking that balance. In particular the technology allows us some opportunities to address these issues in a cost effective way, and I will be asking our witnesses some questions on that, because I also chair on the Commerce Committee, the Subcommittee on Technology, and so we will ask our witnesses about a number of those issues.

There will also be some questions with respect to privacy rights and the background checks, and others will be essential to addressing these issues, and of course, the bottom line is to make sure that all of our ports have in place a clearly understood, clearly defined security plan, and that will be one of the essential issues that will be addressed in the conference committee that will be meeting when the Congress reconvenes after the Fourth of July.

So I will ask our recorder to put our full statement in the record in its entirety, and I do want to allow Senator Murray to make whatever remarks she chooses, but to again express my appreciation to her. She is, in fact, the Senate's leader on these issues, the Northwest leader on these issues, and I thank her for all of the help she is giving our region, and it is good to be with you, Senator Murray.

[The statement follows:]

PREPARED STATEMENT OF HON. RON WYDEN, U.S. SENATOR FROM OREGON

Senators Murray and Cantwell, I would like to thank you for your hospitality, and that of the Port of Seattle, in hosting the fifth field hearing in series that the Senate Commerce Committee has held on the issue of seaport security. Previously our Committee has held hearings in Florida, Louisiana, Texas, South Carolina, and I am pleased to be chairing the first hearing that we will hold on the West Coast.

Port security is a critical issue for the Pacific Northwest given our region's reliance on trade and maritime commerce. The West Coast/ Pacific Rim is the fastest growing and most dynamic segment of international trade in this nation, and well over 50-percent of all of our overseas trade comes into or leaves our coasts here on the Pacific side of our nation.

The incredible expansion of trade has globalized, for good or bad, all aspects of our economy, last year over 9 million truckloads of marine containers were shipped through U.S. ports (imports and exports), that volume is expected to more than double by the year 2020.

Most importers and exporters rely on just-in-time cargo deliveries, and rarely have more than ten days of inventory before they run out. Many of these manufacturers have to purchase their parts from foreign sources. So, in essence, this long supply chain spanning the globe, functions as a moving warehouse, and disruption of this chain of movement would not only harm the people who work in our ports and work on transportation, but it would devastate our manufacturers, and our suppliers, and every other associated down business. So the stakes are enormous in what we do to ensure the protection of our overseas trade.

Since September 11th, we have looked very intently at the maritime trade of our nation. The protection of our maritime boundaries poses unique challenges because of the breadth of our coastline, the proximity of the public to maritime businesses and endeavors, and the sheer volume of shipments of containerized cargoes and shipments of bulk petroleum product and hazardous materials. Literally, we have thousands of tons of hazardous cargoes, originating from foreign nations being transported by foreign vessels, but being transported right through the heart of many U.S. cities. Additionally, the maritime trade is very open, and we do not have the best or most reliable information about shipments, vessels, or the crew members who man those vessels. It is a difficult issue to address.

**Lloyd's List International reported that a NATO country's intelligence service has identified 20 merchant vessels believed to be linked to Osama bin Laden. Those vessels are now subject to seizure in ports all over the world. Some of the vessels are thought to be owned outright by bin Laden's business interests, while others are on long-term charter. The Times of London reported that bin Laden used his ships to import into Kenya the explosives used to destroy the U.S. embassies in Kenya and Tanzania.**

**Several months ago, a suspected member of the Al Qaeda terrorist network was arrested in Italy after he tried to stow-away in a shipping container heading to Toronto. The container was furnished with a bed, a toilet, and its own power source to operate the heater and recharge batteries. According to the Toronto Sun, the man also had a global satellite telephone, a laptop computer, an airline mechanics certificate, and security passes for airports in Canada, Thailand and Egypt.** We have had repeated information that has indicated that terrorists may attempt to enter into the U.S. through maritime means. So we know of the threat, and we know that we need to work together to address this crucial issue.

We need to work closely with all aspects of the maritime and trade communities to coordinate a policy that can help address some of the glaring problems and issues that face. Tomorrow, the Subcommittee will be taking this show on the road, to visit Portland, and the issues in Portland a river port, are different than they are here in Seattle, so we need to have a certain flexibility to recognize and react to the different threats and circumstances.

In particular, today the Subcommittee is focusing on how we might be able to work with foreign nations to help coordinate law enforcement. If we can agree to station Customs inspectors in foreign ports, we can get the benefit of whatever law enforcement actions they are working on, and vice-versa. I know that Customs has started down this path, but we need to see how it might work, and whether it is feasible.

Using technology to create secure systems of transportation will be critical. Right now, only 2–3 percent of inspected cargo is inspected by customs. We need to develop better systems to identify and screen suspicious cargo.

We also need to work with the private sector to see what can be done to encourage the development of secure systems for the movement of cargo. What can the government do to encourage technology, what can we do leverage the security of the private sector. I know we have some witnesses that can address some of these issues, and I look forward to hearing from them.

## STATEMENT OF HON. PATTY MURRAY, U.S. SENATOR FROM WASHINGTON

Senator MURRAY. Thank you very much, Mr. Chairman, and welcome to Washington State. We are delighted to have you here

today, and I appreciate the opportunity to participate in today's hearing.

As Senator Wyden said, this is one of several hearings that is being held in several ports around the Nation, and these hearings are designed to help us respond to the new security challenges facing our ports since September 11.

Our solutions to these challenges must be comprehensive, but they also must be flexible enough to reflect the unique elements of each port—including those here in the Pacific Northwest.

No survey of our nation's port systems would be complete without a look at what is happening in Washington State. We provide a unique perspective on the challenges and the solutions.

To help us do that, we have assembled representatives from the domestic port community, government, foreign seaports, technology companies and organized labor to share their ideas on improving security. It is going to take all of us working together to implement good solutions, so I want to thank all of the witnesses for being here, and I want to extend a special welcome to one of our witnesses, Mr. Robert Yap. He is the executive vice-president of PSA Corporation which handles the Port of Singapore and other international ports. He is accompanied today by Mr. Vincent Lim, who is deputy president of PSA, and welcome you to the Puget Sound.

Their perspective from a foreign port will help us understand how various proposals would affect our ability to trade with other countries. As we work to improve our security, we do not want to penalize the foreign shippers who use our ports, or we will pay the price in lost jobs and commerce.

Washington State is in a unique position to help shape our Nation's seaports security work. Washington is the most trade dependent State in the Nation, and our seaports are the life blood of our economy.

The Ports of Tacoma and Seattle together form the third largest load center for containerized cargo in the United States; 1.8 million containers pass through this region each year. That cargo generates billions of dollars of goods each day and supports tens of thousands of good paying, family-wage jobs.

The Puget Sound also has marine security challenges that other regions do not. We share a land and sea border with Canada. We have several important defense installations that share our waterfront, and we have the largest passenger ferry system in the country.

In the Northwest, we have to balance all of these security needs with the continuing need to keep cargo moving efficiently. I want to outline the challenge before us, talk about the steps we have taken so far, and lay out some principles that I feel we should have for a national solution.

For decades, we have built our port infrastructure and procedures around economic efficiency, and we have done a pretty good job. The people in this room have helped make our port system efficient, and that has helped our economy and our communities. But since September 11th, we now need to add another element to the equation, security. We have got to realign our port system around efficiency and security, and we really are starting from scratch.

There are few standards for handling or inspecting foreign cargo as it enters our ports. Often, we do not know where a container has come from or what is inside. There are many players involved in moving goods to and from our ports, including buyers, sellers, banks, freight forwarders, inland carriers, foreign seaports, carriers, governments and consolidators. The wide range of participants in itself adds to our security challenge.

Because we are starting from scratch and involving so many players, our response must be prompt, and it must be comprehensive. We cannot wait 10 years for one group or agency to develop a plan. So I hope today's hearing will help lay the foundation for us to meet these challenges together.

We must be mindful that it does not slow down the progress we have made in expanding the productivity and efficiency of our ports. The United States receives some $750 billion of cargo at 360 seaports every year. That is roughly one-fifth of the U.S. economy. We do not want to gamble with such an important part of our way of life.

In Congress, we have been working on seaport security for several months, and I want to briefly summarize some of the things we have already accomplished. First, the Puget Sound is going to get its own Marine Safety and Security Team through funding I secured in last year's Defense Supplemental Appropriations Bill. We are going to receive one of the first of the four teams in the Nation trained to operate fast response boats that can intercept ships carrying suspicious cargo well before they reach the port or the coast. The commissioning ceremony will be two days from now on Wednesday.

I also included $93.3 million in the Defense bill for port security grants to help our ports pay for security assessments, enhanced facilities and operations and create better security partnerships. Those grants were released on June 17th. They provide $5.7 million for seaports and maritime security activities in Washington State, including $653,000 to assist security efforts on the Columbia River.

In addition, I have used my position as Chair of the Senate Transportation Subcommittee to review our Government's security efforts. I have held hearings to examine the proposed budgets for the Coast Guard and for the new Transportation Security Agency. In May, I held a hearing on cargo security in Washington, D.C., and in April I held an Appropriations Subcommittee field hearing on this topic right here in this room. I have also attended a full set of Senate Appropriations Committee hearings on homeland security and seaport security.

Because we have had an overwhelming number of applications for the original funding, I included an additional $200 million in this year's appropriations bill for seaport security grants, and $28 million for an initiative we are calling Operation Safe Commerce. That is an initiative at the Nation's three largest container ports, which includes the Ports of Seattle and Tacoma, to test and deploy a program that applies a system-wide approach to seaport security. It calls for all stakeholders to develop clear security standards from the point of origin to final destination. These standards would provide advanced information about cargo and ways to monitor it dur-

ing transit. The supplemental also includes $59 million for the U.S. Customs Service Container Security Initiative which has similar goals to our Operation Safe Commerce.

Finally, let us not forget that this Committee passed the Port and Maritime Security Act in December of last year. Senator Wyden has explained that to you. We are grateful to those on the conference committee who will be working with us to get that out.

After looking at the challenging work so far, I would like to close by laying out a few principles for policy solutions. First, our solution must involve all of the stakeholders in the shipment of goods, both private and public, foreign and domestic. By developing a plan together, we can establish the trust and cooperation they will need to carry it out.

The nature of container traffic makes it difficult to secure the trade route. Foreign manufacturers, points of origin, shippers, designation port authorities and organized labor are all critical elements in the shipping chain, and they are our best allies to securing the trade lanes. Without the cooperation of all of these players, any system we create will be vulnerable.

Secondly, we must create clear standards where none exist today, and those standards must do two things. They must provide reliable information on cargo to everyone in the supply chain. That way officials at home and abroad can identify suspicious cargo and quickly determine if it poses a security risk. These standards must also ensure good communication among all the players in the system.

Third, the cost of these improvements must be shared so that no single entity in the system is burdened with ensuring the security of the system as a whole. Because most of the players are private businesses, concerned with their bottom line, our approach should provide economic incentives to encourage everyone to work within the system. It must include a way for safe, reliable players to have better access to our markets and to remain active even if an incident should occur.

A complete shutdown in the cargo container business could have a severe impact on our economy, a much larger impact than the one we saw when the aviation industry was grounded after September 11th. I think most of the private entities who are involved in trans-shipment of commercial goods would pay a premium for such an incentive.

Fourth, our new system should not disadvantage American ports in this highly competitive environment.

So our port security plans need to involve all stakeholders, must create international standards for information and communication, must spread the cost around, and must not disadvantage American ports.

I recognize that is a tall order, but I think by working together, we can meet all those principles.

One thing that will would help would be more interest and support from the current administration. Customs, INS, and the Coast Guard are all doing a great job of trying to address the vulnerability of our seaports, but this initiative needs more support from the top right now. So far, the Transportation Security Administra-

tion has only doled out responsibilities and has not yet developed any comprehensive approach that I believe we need.

In fact, the additional $200 million in the pending supplemental for seaport security grants, and the money in the supplemental for our Operation Safe Commerce and for Customs Container Security Initiative, are not supported by the President, and he has said that he will veto any Appropriations bill that is above what he requested. So I hope that we can get a more cooperative approach from the White House and the TSA to help us and our ports make these needed improvements.

One final thought. These initiatives are urgent. We cannot wait to do this. As I mentioned before, I helped to craft the Operations Safe Commerce Initiative that is now pending approval along with the rest of the 1902 Supplemental Appropriations bill.

An important aspect of this government investment will be the requirement that government establish some standards for how we will manage these unique security challenges.

But what we do in Congress will not be enough. We need every stakeholder to step up to the plate and begin addressing these issues. We are going to be your partner, but much of this initiative has to come from within the industry.

Today, as I think you are all aware, the contract between the ILWU and PMA expires. A quick and fair resolution of a new contract is in everybody's interest. I mention this at this time because the discussions surrounding the contract negotiations have helped all of us appreciate the stakes, for our economy and our families, in continuing the efficient trade of goods and services across the Pacific. A disruption from a contract dispute would be costly. A disruption caused by a terrorist act will be lethal.

We need to act together, despite whatever disagreements we might have, to make our ports, and by extension our economy more safe and more secure, and that is why I believe we need to act now.

So again, I thank all of our witnesses for being here today, for Senator Wyden for coming and for the Commerce Committee having this really important hearing today.

[The prepared statement of Senator Murray follows:]

PREPARED STATEMENT OF HON. PATTY MURRAY,
U.S. SENATOR FROM WASHINGTON

Thank you Mr. Chairman. I appreciate the opportunity to participate in today's hearing.

This is one of several hearings being held in port communities around the nation. These hearings will help us in the Senate respond to the new security challenges facing our ports in the wake of September 11th.

Our solutions to these challenges must be comprehensive. But they must also be flexible enough to reflect the unique elements of each port—including those here in the Pacific Northwest.

No survey of our nation's port systems would be complete without a look at Washington state. We provide a unique perspective on challenges and solutions.

To help us do that, we've assembled representatives from the domestic port community, government, foreign seaports, technology companies, and organized labor to share their ideas on improving security. It's going to take all of us working together to implement good solutions so I want to thank all of the witnesses for being here today.

I want to extend a special welcome to one of our witnesses—Mr. Robert Yap—the executive vice president of the PSA Corporation, which handles the Port of Singapore and others international ports. He is accompanied today by Mr. Vincent Lim, Deputy President of PSA. Welcome, Mr. Lim. Their perspective—from a foreign

port—will help us understand how various proposals would affect our ability to trade with other countries. As we improve our security, we don't want to penalize the foreign shippers who use our ports, or we'll pay the price in lost jobs and commerce.

Washington state is in a unique position to help shape our nation's seaport security work. Washington is the most trade dependant state in the nation, and our seaports are the life blood of our economy.

The Ports of Tacoma and Seattle together form the third largest load center for containerized cargo in the United States. 1.8 million containers pass through this region each year. That cargo generates billions of dollars of goods each day and supports tens of thousands of good paying, family-wage jobs.

The Puget Sound also has marine security challenges that other regions do not. We share a land and sea border with Canada. We have several important defense installations that share our waterfront. And we have the largest passenger ferry system in the country.

In the Northwest, we must balance all of these security needs with the continuing need to keep cargo moving efficiently. I want to outline the challenge before us, talk about the steps we've taken so far, and finally lay out some principles for a national solution.

For decades, we've built our port infrastructure and procedures around economic efficiency, and we've done a good job. Many of the folks in this room have helped make our port system efficient and that's helped our economy and our community. But since September 11th, we now need to add a new element to the equation—security. We've got to realign our port system around efficiency and security. We're really starting from scratch.

There are few standards for handling or inspecting foreign cargo as it enters our ports. Often, we don't know where a container has come from—or what's inside. There are also many players involved in moving goods to and from our ports including—buyers, sellers, banks, inland carriers, foreign seaports, carriers, governments, and consolidators. The wide range of participants in itself adds to the security challenge.

Because we're starting from scratch and involving so many players, our response must be prompt and it must be comprehensive. We can't wait 10 years for one group or agency to develop a plan. I hope today's hearing will help us meet these new challenges together.

We must be mindful that it does not slow down the progress we have made in expanding the productivity and efficiency of our ports. The United States receives some $750 billion worth of cargo at 360 seaports every year. That's roughly one-fifth the U.S. economy. We don't want to gamble with such an important part of our economy.

In Congress, we've been working on seaport security for several months, and I want to so briefly summarize what we've accomplished. First, the Puget Sound will get its own Marine Safety and Security Team because of funding I secured in last year's Defense Supplemental Appropriations Bill. We will receive one of the first of four teams in the nation trained to operate fast response boats that can intercept ships carrying suspicious cargo well before they reach the port or even the coast. I'm pleased to report that the commissioning ceremony is this Wednesday.

I also included $93.3 million in the Defense bill for port security grants. This money will help ports pay for security assessments, enhance facilities and operations, and create better security partnerships. These grants were released on June 17. They provide $5.7 million for seaports and maritime security activities in Washington state including $653,000 to assist security efforts on the Columbia River.

In addition, I've used my position as Chairman of the Senate Transportation Subcommittee to review our government's security efforts. I've held hearings to examine the proposed budgets for the Coast Guard and for the new Transportation Security Agency. In May, I held a hearing on cargo security in Washington, D.C. In April, I held an Appropriations Subcommittee field hearing on this topic—in this very chamber. I also attended a set of full Senate Appropriations Committee hearings on homeland security where seaport security was discussed.

Because we've had an overwhelming number of applications for the original funding, I included an addition $200 million in this year's Senate Supplemental Appropriations bill for seaport security grants. I also included $28 million for an initiative called "Operation Safe Commerce" in the Supplemental. This is an initiative at the nation's three largest container ports—which includes the Ports of Seattle/Tacoma—to test and deploy a program that applies a system-wide approach to seaport security. The initiative calls for all stakeholders to develop international standards from the point of origin to the final destination. These standards would provide advanced information about cargo and ways to monitor the cargo during transit. The Supple-

mental includes $59 million for the U.S. Customs Service Container Security Initiative, which has similar goals to "Operation Safe Commerce."

Finally, let's not forget that this Committee passed the Port and Maritime Security Act in December of last year. That legislation would improve cooperation among all the stakeholders, force ports to evaluate their security needs, better secure port facilities, require information about cargo shipments be evaluated before they're granted entry into a U.S. port, improve reporting of cargo and crew, and authorize grants to ports to help comply with these new mandates. That bill is now in conference with the House.

After looking at the challenge and our work so far, I'd like to close by laying out a few principles for policy solutions. First, our solution must involve all the stakeholders in the shipment of goods, both private and public, foreign and domestic. By developing a plan together, we can establish the trust and cooperation we'll need to carry it out. The nature of container traffic makes it difficult to secure the trade route. Foreign manufactures, ports of origin, shippers, destination port authorities, and organized labor are all critical elements in the shipping chain. They are our best allies to securing the trade lanes. Without cooperation among all of these players, any system we create will be vulnerable.

Second, we must create international standards, where none exist today. Those standards must do two things. They must provide reliable information on cargo to everyone in the supply chain. That way officials at home and abroad can identify suspicious cargo and quickly determine if it poses a security risk. These standards must also ensure good communication between all the players in the system.

Third, the costs of these improvements must be shared—so that no single entity in the system is burdened with ensuring the security of the system as a whole. Because most of the players are private businesses—concerned with the bottom line—our approach should provide economic incentives to encourage everyone to work within the system. It must include a way for safe, reliable players to have better access to our markets and to remain active even if an incident should occur.

A complete shutdown in the cargo container business could have a severe impact on our economy—a much larger impact than the one we saw when the aviation industry was grounded immediately after September 11th. I think most of the private entities who are involved in trans-shipment of commercial goods would pay a premium for such a incentive.

Fourth, our new system should not disadvantage American ports in this highly competitive environment.

So as I see it, port security plans need to involve all stakeholders, must create international standards for information and communication, must spread the costs around, and must not disadvantage American ports.

I recognize that's a tall order, but working together I think we can meet those principles.

One thing that would help would be more interest and support from the current Administration. Customs, the INS, and the Coast Guard are all doing a great job of trying to address the vulnerability of our seaport, but this initiative needs more support from the very top. So far, the Transportation Security Administration has only doled out responsibilities. It hasn't yet developed the comprehensive approach that is needed to properly secure our trade routes.

In fact, the additional $200 million in the pending Supplemental for seaport security grants, and the money in the Supplemental for "Operation Safe Commerce" and for the Customs' "Container Security Initiative" are not supported by the President. The President has said he will veto any Appropriations bill that is above what he requested. So I hope we'll have a more cooperative approach from the White House and the TSA to help us and our ports make these needed improvements.

One final thought. These initiatives are urgent. We cannot wait to do this. As I mentioned before, I have helped to craft the "Operation Safe Commerce" Initiative that is now pending approval along with the rest of the '02 Supplemental Appropriations bill.

An important aspect of this government investment will be the requirement that government establish some standards for how we will manage these unique security challenges.

But what we do in Congress will not be enough—we need every stake holder: labor, the shipping lines, the shippers, and foreign and domestic ports to step up to the plate and begin addressing these issues. We will be your partner, but much of this initiative must come from within the industry.

Today, the contract between the ILWU and the PMA expires. A quick and fair resolution of a new contract is in everybody's interest. I mention this at this time because the discussions surrounding the contract negotiations have helped everyone appreciate the stakes—for our economy and our families—in continuing the efficient

trade of goods and services across the Pacific. A disruption resulting from a contract dispute would be costly. A disruption caused by a terrorist act could be lethal.

We must act together, despite whatever other disagreements we might have, to make our ports—and by extension or economy—more safe and secure. And we must act now. So I again thank all of the witnesses and everyone here today. I look forward to hearing your testimony.

---

As Chair of the Senate Transportation Appropriations Subcommittee, which oversees the Coast Guard's budget, Sen. Murray has been a strong advocate for the Coast Guard. Last year, Murray succeeded in increasing the Coast Guard budget by 10-percent, improving the service's search and rescue and communications capabilities, as well as providing a pay raise for personnel.

Already this year, Murray has been briefed by the Customs Service and Coast Guard on port security and cargo security, and has held hearings on those topics both in Seattle and Washington, DC.

Following are some of the successes Sen. Murray has had in her efforts to support the Coast Guard.

**FY 2002 Transportation Appropriations Bill:**

- $6 million was provided within the **Coast Guard AC&I programs** for communications equipment that enhances the Coast Guard's ability to provide Port Security including: Global Maritime Distress and Safety System (GMDSS); Defense Message System Implementation; and, Commercial Satellite Communications. These items were all part of the Administration's request made prior to 9–11.

**FY 2002 Supplemental (within the Department of Defense FY2002 Bill):**

- $93.3 million was provided for Port Security grants within Transportation Security Administration's (TSA's) appropriation. These grants were intended to supplement current security initiatives and assist the states with security assessments and enhancements.
- $41.3 million was provided for Anti-terrorism activities, including **Marine Safety and Security Teams (MSST)** within the Coast Guard Operating Expenses. Funding was provided for an additional 348 full-time permanent positions for four MSST's. While the Bush Administration only requested 2 MSSTs, Sen. Murray insisted that 4 teams be funded. Further, Murray directed that two of those teams be permanently stationed at locations with the greatest concentration of naval military assets—Seattle, Wa. and Norfolk, Va. The first MSST will be commissioned in the Puget Sound on Wednesday, June 3, 2002.
- $2.4 million was provided to enhance the **Coast Guard's Strike Teams** to respond to chemical & biological incidents.

**FY 2002 Supplemental (For Further Recovery from and Response to Terrorist Attacks):** *(this bill is currently in a House-Senate conference committee)*

- $200 million was provided for **Port Security Grants** for TSA within the Senate Passed Supplemental. *The House bill provides $75 million.*
- $27.9 million was provided for TSA for the "**Operation Safe Commerce**" initiative for the purpose of expediting the testing and deployment of the program. This is to be completed through pilot projects involving the three largest container load centers, which includes Seattle/Tacoma. *The House bill has no similar provision.* The elements of these initiatives include:

  Secure packing requirements for loading containers;

  Auditable security standards at docks, manufacturing plants or shipping facilities;

  Mechanical and/or electronic seals and devices intended to identify containers whose security has been compromised;

  Integrated communications systems to track cargo throughout the entirety of its journey;

  The transmission of tracking data in accessible format;

  Demonstration of "secure trading lanes" that ensures container security from point of origin to point of destination; and

  Establishing new requirements for all participants in the supply chain that will allow federal agencies to get information to appropriately target suspicious cargo.

- $59 million is provided within the Customs Service for the **Container Security Initiative.** Money will be provided to the 20 largest seaports in the United States and 3 in Canada to help them better monitor suspicious cargo. That defi-

nition would include the Ports of Tacoma and Seattle. It urges technological solutions to our security problem.

- $20 million was provided for TSA for **incident training** for ports to train and exercise port security personnel. *The House bill has no similar provision.*
- An additional $129 million above the Administration's request was provided for **Coast Guard Operating Expenses.** These additional funds were provided to expedite **Port Vulnerability Assessments** among other things. *The House bill provides $12 million more than the Administration's request for Port Vulnerability Assessments.*
- The other Port Security projects within Coast Guard Operating Expenses include, **Maritime Domain Awareness, Information and Communications, Sea Marshals, Maritime Security Patrols, Security Readiness and Planning, Strike Teams, and two additional MSST's.** The Administration's request makes no reference to any of these projects for the Supplemental; however, all were included in their FY–2003 request.
- $12 million is provided within Coast Guard AC&I account for **Homeland Security Response Boats (87 foot).** The House bill also provides $12 million. This amount is projected to buy 6–8 boats, 2 of which are bound for Puget Sound (Bremerton and Port Angeles).
- $18 million is provided within Coast Guard AC&I for various **communications projects** that will enhance Port Security. *The House bill has no similar provision.*
- $9.4 million is provided within Coast Guard AC&I for **Maritime Domain Awareness Information Management.** *The House bill has no similar provision.*

Senator WYDEN. Senator Murray, thank you for an excellent statement and for all the leadership that you have provided and the great chance to team up with you on these issues.

Our first panel is going to be Rear Admiral Erroll Brown, Commander, 13th Coast Guard District, United States Coast Guard. He is accompanied by Captain Danny Ellis, Captain of the Port of Seattle, and we also have on this panel Mr. Douglas Browning, Deputy Commissioner, U.S. Customs Service, Washington, D.C., and Mr. Mic Dinsmore, Executive Director of the Port of Seattle. So we welcome all of you gentlemen. We are going to put your prepared remarks into the hearing record in the entirety. I know there is also a biological compulsion at Congressional hearings to read word for word your statements. I understand that. If you could just, in the interest of time, highlight the high points for us, we will put your statement into the record in its entirely, and that will leave plenty of time.

Senator MURRAY. Mr. Chairman, this is Captain Ellis' very first day on the job, so we welcome you.

Senator WYDEN. Captain Ellis, welcome, and we are pleased that you accompanied Admiral Brown. Let us proceed, right to you, Admiral Brown.

## STATEMENT OF REAR ADMIRAL ERROLL M. BROWN, COMMANDER, 13TH COAST GUARD DISTRICT, UNITED STATES COAST GUARD

Admiral BROWN. Good afternoon, Mr. Chairman, Senator Murray, Senator Cantwell. Thank you for the opportunity to speak to you today about the Coast Guard's role in maritime approaches, and I would like to express my appreciation for the Senate support of the 209 million dollars in the first homeland security supplemental.

As you mentioned, Mr. Chairman, I am accompanied today by Captain Danny Ellis, Puget Sound. Captain Ellis assumed com-

mand Friday, so has been on the job about 72 hours, and so far, so good.

Clearly, the waterways of the Pacific Northwest are critically important gateways to the global economy. The marine transportation system in this region contributes substantially to the economic growth and stability of our Nation, the quality of life of our citizens and our Nation's security. Maintaining effective maritime domain awareness of this vast geographic watery region, encompassing nearly 3,500 square miles, is the centerpiece of our efforts to achieving Maritime Homeland Security.

Maritime domain enables knowledge of people, cargoes and vessels to filter potential threats from the stream of legitimate commerce. This requires international and multiagency cooperation at all levels of government, as well as strong partnerships with the private sector.

The Coast Guard has a long standing established relationship with the maritime communities in the Pacific Northwest. Using a model of awareness, prevention, response and consequence management, we have worked closely with our integral partners to ensure the safety, and now the security of our ports and waterways.

Long before 9–11 we were already developing an overarching port security strategy which set the tone for leveraging the maritime community in its entirety, both public and private, as part of the solution to security—not just terrorism, but any illegal activity.

In 1996, Puget Sound established a Harbor Safety Committee with representatives from Federal, State and local agencies, including the Coast Guard, Maritime Administration, U.S. Army Corps of Engineers, Washington State Department of Ecology, and Washington State Ferries, numerous maritime industry trade associations, environmental and aquaculture conservation groups, Indian tribes, and Washington Public Ports Association which represents the combined interests of the ports of Seattle, Tacoma, Bellingham, Olympia, Everett and Port Angeles. This body has engaged on numerous maritime safety and security issues, and provided an excellent foundation for the Captain of the Port in establishing nine regional port security committees, which have served as a significant avenue for region-wide security information flow since September 2001. The port security committees collaborate on security strategies, share information and improve security postures. We continue to partner with U.S. Customs, Washington State Department of Agriculture, the Federal Railroad Administration and Washington State Patrol to inspect great numbers of containers and insure cargo manifests and bills of lading are correct.

A Memorandum of Understanding between Customs and the U.S. Coast Guard enables us to combine resources and eliminate duplicative effort in order to improve container and border security measures. While our combined efforts are critical in ensuring the security of our Maritime Transportation System and U.S. border, a container security inspection program must include international engagement to foster point of origin control and inspection of containers as they move.

The Coast Guard maintains strong working relationships with the Navy and Law Enforcement. The Coast Guard continues to coordinate with other U.S. and Canadian Federal agencies who are

instrumental in ensuring the execution of the Ridge/Manley "Smart Border Declaration" and of the entire "30-Point Action Plan." The Cooperative Vessel Traffic Service jointly operated by the U.S. and Canadian Coast Guards since 1979 is a critical traffic management tool for this complex waterway system between Washington State and British Columbia, and is a model of bilateral international cooperation.

The system serves as a critical component serving enhanced maritime domain awareness—the overall knowledge of vessels, cargoes, and people, thus greatly reducing the threat posed by crews and passengers of vessels through advanced reporting and knowledge. We enjoy an equally close relationship with Transport Canada Marine Safety in the conduct of the Port State Control Program regarding eliminating substandard or suspicious foreign vessels entering our respective waters.

In conclusion, the United States Coast Guard in the Pacific Northwest is an integral component of our Nation's homeland security efforts. The massive flow of people and goods across our maritime borders helps fuel our economy, but also serves as a potential conduit for terrorists and weapons of mass destruction. We are a principal agency in defending our Nation's maritime borders and ensuring the integrity of the maritime transportation system.

The security of the several ports within Puget Sound, and particularly the Ports of Seattle and Tacoma has improved. One of the specific challenges we face today is balancing the security and economic needs of our country. Our Nation's harbors, including Puget Sound, are accessible to thousands of maritime workers and ships from all over the globe. We must filter out potential terrorist activities from the massive stream of legitimate commerce.

A key success factor is improved awareness of the cargo entering our country and the people who own, operate and service the thousands of vessels entering the U.S. each year. I am confident that our successes can be directly attributed to outstanding and aggressive partnering resulting in increased information sharing, heightened awareness and implementation of preventive measures. We will make the best use of our existing resources and resources requested by the President to make sure that people and goods move safely.

The Coast Guard is committed to the protection of our Nation against terrorist threats as well as maintaining our Search and Rescue capabilities and the other missions. Thank you for the opportunity to share the initiatives that the Coast Guard and the Pacific Northwest are engaging in today, and for your continuing support of the Coast Guard.

I will be happy to answer any questions.

Senator WYDEN. Admiral Brown. Thank you. Excellent statement.

[The prepared statement of Admiral Brown follows:]

PREPARED STATEMENT OF REAR ADMIRAL ERROLL M. BROWN, COMMANDER, 13TH COAST GUARD DISTRICT, UNITED STATES COAST GUARD

Good afternoon Mr. Chairman and distinguished members. My name is Rear Admiral Erroll M. Brown and I am Commander of the Thirteenth Coast Guard District headquartered in Seattle, Washington. On behalf of the Commandant, Admiral

Thomas Collins, thank you for the opportunity to speak to you today about the Coast Guard's role in securing our ports and waterways and maritime approaches.

**Unique Challenges of Pacific Northwest Port Security**

The waterways of the Pacific Northwest are critically important gateways to the global economy. The marine transportation system in this region contributes substantially to the economic growth and stability of our nation, the quality of life of our citizens and our nation's security. The Pacific Northwest is a gateway to the Pacific trade routes to Asia. Over 5,000 foreign vessels transit our waterways each year. Approximately 50-percent of those proceed to Canadian ports, while nearly 2,500 vessels proceed to and from Puget Sound ports transporting over 1.8 million containers through the Seattle-Tacoma port complex each year making it the third largest container cargo complex in the United States. In addition, 12 billion gallons of oil move through the Strait of Juan de Fuca to four major U.S. refineries, which are crucial to the national economy, and provide all of the refined products used for civilian and military use in the north west. Over 600,000 recreational boaters with 250,000 registered recreational boats enjoy the waters in and around Washington State. Some of these boats have served as smuggling platforms and could potentially mask terrorists' movement. The Washington State Ferry System transports over 26 million passengers and 11 million vehicles on about 180,000 transits a year and is the largest ferry system in the U.S. Our growing cruise industry, with over 230,000 passengers last year, is forecast to triple in volume over the next few years. Ensuring the safety and security of this massive movement of people requires extensive, collaborative effort. In addition, the Puget Sound is home to one of the largest concentrations of U.S. Naval Forces in the country. These strategic, national defense assets, must maintain the highest levels of security against a potential enemy. By all forecasts, use of these waterways for national defense, commerce, fishers, commuters, travelers, and recreation will continue to grow. Protecting our marine transportation system and critical infrastructure, including our ports and the cargo they convey from terrorist activities is a tremendous challenge.

Compared to other U.S. ports, the distances and geography of this region are significant. From the open ocean, it is 123 miles to Seattle and 147 miles to Tacoma each direction, which equates to one-way transit times of six to ten hours. Washington State and Canada share approximately 150 nautical miles of maritime border accessible to anyone with a waterborne craft ranging from a jet ski to a commercial ship, complicating monitoring and enforcement of maritime laws. With distances of 12 to less than three miles between Canada and the United States, the San Juan Islands present a major challenge for law enforcement officials providing an area where smugglers can quickly cross the maritime border with illegal currency, drugs, weapons, and migrants.

Maintaining effective Maritime Domain Awareness (MDA) of this vast geographic water region, encompassing nearly 3,500 square miles, is the centerpiece of our efforts to prevent threats from reaching our shores and achieving maritime homeland security. MDA enables knowledge of people, cargoes, and vessels to filter potential threats from the stream of legitimate commerce. This requires international and multi-agency cooperation at all levels of government as well as strong partnerships with the private sector.

**Cooperative Approaches to Maritime Security**

The Coast Guard has a long-standing, established relationships with the maritime communities in the Pacific Northwest. Using a model of awareness, prevention, response, and consequence management, we have worked closely with our integral partners to ensure the safety, and now the security of our ports and waterways in the Pacific Northwest. Long before 9–11 we were already developing an overarching port security strategy, which set the tone for leveraging the maritime community in its entirety, both public and private, as part of the solution to security-not just terrorism, but any illegal activity.

The Department of Defense Appropriations Act for FY2002 appropriated $93.3 million to the Transportation Security Administration for grants to enable critical national seaports and terminals to enhance their security. I am pleased to learn that the Port of Seattle, Washington State Ferries, Clipper Navigation Inc. and the Columbia River Steamship Operators Association received grants in excess of $5.7 million based on their proposals for increased security.

Harbor Safety Committees have long been a means of sharing information, ideas, and forging cooperative solutions between government and the maritime community. In 1996, Puget Sound established a Harbor Safety Committee with representatives from federal, state and local agencies, including the Coast Guard, Maritime Administration, U.S. Army Corps of Engineers, Washington State Department of

Ecology and Washington State Ferries, numerous maritime industry trade associations, environmental and aquaculture conservation groups, Indian Tribes and the Washington Public Ports Association which represents the combined interests of the Ports of Seattle, Tacoma, Bellingham, Olympia, Everett, and Port Angeles. This body has engaged on numerous maritime safety and security issues and provided an excellent foundation for the Captain of the Port in establishing nine regional Port Security Committees, which have served as a significant avenue for region wide security information flow since September 2001. The Port Security Committees foster local and regional cooperation to identify best practices, collaborate on security strategies, share information, and improve security postures regarding ferries, cruise ships, refineries, and intermodal transport.

Washington State Ferries is a central component of the marine transportation system infrastructure in the Puget Sound. The Captain of the Port established a special port security committee focused solely on ferry security. The Washington State Ferry Security Committee includes members of Washington State Ferries, Coast Guard, and Washington State Patrol, and was chartered to identify preventive security measures, promote increased awareness, decrease vulnerability, and refine the existing response network for this critical extension of the highway system within the State. The internal measures developed and implemented by Washington State Ferries and the Washington State Patrol in coordination with the Coast Guard over the past nine months have incrementally decreased vulnerability of the ferry system. This partnership has been instrumental to decreasing vulnerability and increasing awareness through appropriate and prudent security measures being established to mitigate the current general threat to the public, our nation and its infrastructure.

We continue to partner with U.S. Customs, Washington State Patrol, Department of Agriculture and the Federal Railroad Administration to inspect greater numbers of containers, ensure cargo manifests, and bills of lading are correct. There is an increased emphasis on identifying cargoes that have the potential to inflict the greatest harm on the U.S. Through our container inspection synergies, we have realized a force capability larger than we are, heightening security interest and proactive prevention measures among all elements of the container inspection process. A memorandum of understanding between Customs and the Coast Guard, enables us to combine resources and eliminated duplicative efforts in order to improve container and border security measures. While our combined efforts are critical in ensuring the security of our marine transportation system and U.S. border, a container security inspection program must include the international engagement to foster point of origin control and inspection of containers to most effectively assure the security of containers as they move through our seaports and our Nation.

Since January of 2002, the Coast Guard Thirteenth District and Navy Region Northwest have co-chaired a Regional Force Protection Executive Steering Committee. This Committee has been working to enhance communication between various agencies and formulate Regional Force Protection policies and procedures. This Committee provides the venue for ongoing information sharing to best protect our strategic military assets in the Puget Sound region.

The Coast Guard maintains strong working relationships with Canadian law enforcement and safety authorities. The law enforcement and intelligence communities have partnered to counter the threats along the US-Canada border. The Coast Guard continues to coordinate with other US and Canadian federal agencies who are instrumental in ensuring the execution of the Ridge/Manley "Smart Border Declaration". The Coast Guard has been a key participant in the process to implementing the entire "30-Point Action Plan". The action plan addresses common US-Canada border security needs ranging from the establishment of biometric identifiers to Integrated Border Enforcement Team resources, ferry operations, and joint communications capabilities. The Border Intelligence Group and Northwest Criminal Information Network meet regularly to share information, identify trends, and design and implement consistent solutions. The Cooperative Vessel Traffic Service (CVTS), jointly operated by U.S. and Canadian Coast Guards since 1979, is a critical traffic management tool for this complex waterway system between Washington State and British Columbia, and is a model of bilateral international cooperation. We have reaped huge benefits from this relationship. The system serves as a critical component serving enhanced Maritime Domain Awareness—the overall knowledge of vessels, cargoes, and people using the MTS, thus greatly reducing threat posed by crews and passengers of vessels through advanced reporting and knowledge.

This single system affords us the opportunity to thoroughly vet and screen arriving vessels, and apply appropriate controls over those vessels moving through our waters and into our ports. We enjoy an equally close relationship with Transport Canada Marine Safety in the conduct of our Port State Control program regarding

eliminating sub-standard or suspicious foreign vessels entering our respective waters. Over the past five years, the our agencies have developed an exchange program between our marine inspection forces to ensure a more consistent approach and to develop closer working relationships and confidence in our respective safety regimes.

The Coast Guard's multi-mission assets, military role as an Armed Service, and maritime presence and authorities bridge security, safety, and response capabilities between federal, state, local, and private organizations as well as other military services. We have been the leader for the non-DOD maritime security needs of our nation since 1790 . . . it was the reason we were formed 212 years ago. We possess extensive regulatory and law enforcement authorities governing ships, boats, personnel, and associated activities in our ports, waterways, and offshore maritime regions. We are a military service with 7x24 command, communication, and response capability. We maintain, "at the ready", a network of coastal small boats, aircraft, and cutters, and expert personnel to prevent and respond to safety and security incidents; and we have geographic presence throughout the country, coasts, rivers, and lakes, both in large ports and small harbors. We are a formal member of the national foreign intelligence community. We partner with other government agencies (OGAs) and the private sector to multiply the effectiveness of our services. The Coast Guard is the recognized leader in the world regarding maritime safety, security, mobility, and environmental protection issues. These characteristics form the core of our organization and enable a unity of effort among diverse entities whether preventing or responding to incidents.

**Conclusion**

In conclusion, the United States Coast Guard in the Pacific Northwest is an integral component of our nation's homeland security efforts. The massive flow of people and goods across our maritime borders helps fuel our economy, but also serves as a potential conduit for terrorists and weapons of mass destruction. We are a principle agency in defending our nation's maritime borders and ensuring the integrity of the marine transportation system. The security of the several ports within Puget Sound and particularly the ports of Seattle and Tacoma has improved. One of the significant challenges we face today is balancing the security and economic needs of our country. Our nation's harbors, including Puget Sound, are accessible to thousand of maritime workers and ships from all over the globe. We must filter out potential terrorist activities from the massive stream of legitimate commerce. A key success factor is improved awareness of the cargo entering our country and the people who own, operate and service the thousands of vessel entering the U.S. each year. I am confident that our successes can be directly attributed to outstanding interagency cooperation and aggressive partnering resulting increased information, sharing, heightened awareness, and implementation of preventative measures. We will make the best use of our existing resources and resources requested by the President to ensure people and goods move safely. The Coast Guard is committed to the protection of our nation against terrorist threats as well as maintaining our search and rescue capabilities and other missions. Thank you for the opportunity to share the initiatives that the Coast Guard and the Pacific Northwest are engaging in today, and for your continuing support of the Coast Guard. I will be happy to answer any questions you may have.

Senator WYDEN. We are also joined now by Senator Cantwell, and she had been a great addition to our congressional delegation. In particular, we highlighted a need to strike a balance between security and efficiency so that we can protect our ports and make sure that goods move in and out of the region in a speedy fashion, technology is going to be the key, and there is no member of the United States Senate that is more familiar with these kind of technology issues, and I want to recognize her for her opening statement.

## STATEMENT OF HON. MARIA CANTWELL, U.S. SENATOR FROM WASHINGTON

Senator CANTWELL. Mr. Chairman, I apologize for the delay. I will submit a statement for the record, but I very much appreciate the Chairman being here and conducting this hearing, not only here but in other parts of the West Coast, because it is critically

important to make sure efficiency and security go hand in hand. I thank Senator Murray, who has done a great job in battling for the Coast Guard and battling for appropriations funds for security issues in the Northwest. I think it will help us play the leadership role that we need to play in making sure that our economic and security future are well coordinated.

I am going to submit for the record, Mr. Chairman, a letter that I have sent to the President in the last 24 hours asking that an international protocol for security be accomplished with various ports around the world for the very reasons that you, Rear Admiral Brown, just emphasized, and that is that point of origin has to be a critical focus for us, and we can plan for all the security infrastructure here in Seattle, but once that container arrives on a dock in Seattle, it is too late.

So the strategies that we have to deploy need to have international cooperation, and the only way we can do that is if the Administration at a cabinet level starts working on these protocols with various ports and establishes a standard by which the security measures can be assured.

When you think about it, the Oklahoma bombing of the Federal Building, that level of explosive would take up about one fourth of a container, not to mention what kind of other dirty bomb activities could take place in a container that would be even more devastating to the Puget Sound area, so we must have international cooperation.

I am very interesting in hearing from the panelists today their views about homeland security cooperation in the new agency. I am very interested in hearing specifically what is happening since September 11th as it relates particularly to cargo containers.

We have heard a lot probably about moving of people, but we have not heard enough about moving of products, and we want to understand what has changed since September 11th, and lastly, about how we get this issue of technology right, in the sense that our future here really does depend on efficiency as well as security, and how can we move forward on some of these issues.

And so I thank you, Mr. Chairman, for the ability to make those comments, and I will submit a longer statement.

[The prepared statement of Senator Cantwell follows:]

PREPARED STATEMENT OF HON. MARIA CANTWELL,
U.S. SENATOR FROM WASHINGTON

**Introduction**

Thank you Mr. Chairman, for your work in organizing this hearing and for ensuring that the Committee has a opportunity to take a serious look at some of the unique and common port security issues facing our region. I truly appreciate your work, and the ongoing efforts of Chairman Hollings and Chairman Breaux in persistently working to strengthen the security of our seaports and fighting to rapidly bring the Senate together in addressing these issues. I'd also like to thank my colleague, Senator Murray, who's been such a leader on the Transportation Committee in making sure that the Coast Guard has the resources to effectively carry out its increased port security mandates while also sufficiently fulfilling its other critically important missions for the Pacific Northwest; and who has also fought hard to obtain funding for our priority transportation and port facility needs in the supplemental appropriations bill that the Senate recently passed.

Port activities are a crucial component of the Northwest economy, and I look forward to working with my colleagues to keep them safe and productive.

**Why ports are important to NW**

In order for our Northwest economy grow our ports must remain safe. More than 100,000 workers in the Puget Sound area—including longshoremen and freight forwarders—depend on the ports of Seattle and Tacoma for their jobs. Those same ports generate over $700 million annually for the State of Washington. From those figures alone, it is easy to understand the tremendous impact that a terrorist act would have on the Northwest.

**Since 9–11, concern over Port security has risen to new level**

The threat of attacks on America's ports and waterways is real. Just three weeks ago the U.S. Coast Guard in Seattle issued an alert for Washington state's waterways. The warning was based on what the Coast Guard called a credible threat to maritime interests. Officials gave no details on possible targets, but FBI agents have questioned scuba instructors in Washington and around the country about any suspicious activity.

And we now know that the FBI considers Seattle one of the top targets for terrorist groups, and receives a disproportionate number of terrorism threats compared to other parts of the nation.

And if we're a high-profile target, as unpleasant as this may be, we have to think about worst-case scenarios and vigilantly do everything possible to prevent them. King county is the 12th largest county in the United States, with over 1.7 million residents. On any given weekday there are as many as three-quarters of a million people in the City of Seattle. There are 95 public schools, 42 nursing homes, 10 hospitals, nearly 800 day care facilities, 2 major interstates and seemingly countless bridges, and one of the top 25 busiest airports in the nation. A weapon of mass destruction attack would clearly have devastating consequences, and escape would be virtually impossible.

But we also need to think about less direct threats as well. A port attack anywhere in America would likely have a devastating impact on the Northwest economy. Many manufacturers keep only several days of parts inventory on hand and rely on maritime shipping for many items, especially larger ones. Not only that, but many parts—such as the fuselage for the Boeing 737—arrive from other parts of US by rail. A full-scale disruption of the transportation system could halt Boeing operations within a matter of days, and many analysts predict that it could take months to carefully "turn the system back on".

**Acknowledgement of local efforts Underway**

There is much work to be done in the effort to protect America's ports, but there are a number of initiatives underway already. The Puget Sound ports in cooperation with the Coast Guard have moved rapidly to conduct threat assessments, and they already have deployed gamma-ray scanning technology, which will allow inspectors to scan the contents of vehicles and containers without having to open them.

Security initiatives undertaken by individual ports will go a long way toward strengthening our national security. For example, our Puget Sound ports have taken several steps to increase security. They have initiated a one-year program to develop partnerships with other ports, the shipping lines, and the federal agencies to ensure that containers are securely loaded at point of origin and to provide 100 percent verification of the contents at those ports. Ultimately, these partnerships will also employ the use of electronic seals to be applied at the point of loading and use tracking mechanisms to ensure secure transport of goods to the final destination.

**New Federal programs and mandates**

While local port are on the front lines of keeping our ports safe, they need federal support to be effective. The Senate moved quickly to pass legislation proposed by Senator Hollings. Throughout his distinguished career Senator Hollings has been a strong advocate for national security, and I thank him again for all his work on this issue.

Senator Hollings' bill takes a comprehensive approach to strengthening requirements and funding for improvements in port security and safety, and strengthening international cooperation for cargo security improvements. It will provide grants and loan guarantees for port security, authorize increased funding for customs to continue the deployment of screening technologies at ports and add new Customs inspectors; it would also require local port threat assessments, and allow the president to prohibit shipments from foreign ports considered insecure. The Senate bill also requires more specific manifest information that will help the Customs Service focus its resources on checking the containers of greatest concern, faster reporting of improperly documented cargo, and the development of limited-access security sen-

sitive areas in our ports. Finally, the bill would create a "sea-marshal" program to ensure the safety of arriving vessels.

After September 11th, I worked with my colleagues in Congress to provide the funding and authority necessary for these domestic efforts to be implemented successfully. In addition to our ports, I've worked hard to double the number of INS agents which will be completed by the end of the year.

Senator Murray has spearheaded an effort to upgrade Coast Guard resources to allow it to carry out its many missions. A strong Coast Guard is a critical for the security of our ports and waterways.

I know that the Chairman and the Committee is working hard to get the conference completed on the seaport security bill and I hope that any outstanding issues can be expeditiously resolved. We need to help establish some certainty for our ports, the shippers, and the agencies so that they can most efficiently implement the new system.

Congress also moved swiftly to create the Transportation Security Administration and mandate sweeping passenger and baggage reforms at our nations airports; we've added INS and Customs agents along our northern border; and very quickly provided flexible funds for our ports and federal agencies to implement new security measures.

As a result, our federal agencies **are** taking actions to make our ports safer, and today's hearing will help us get a sense of what has already changed. In consultation with Congress, Customs and the Coast Guard have already taken a number of steps that are very encouraging.

I applaud the efforts of Customs Service Commissioner Robert Bonner for developing the Container Security Initiative, which clearly seems to be heading in the right direction. We should be developing public and private partnerships with other nations and private ports so that we can inspect more cargo and have greater certainty about container contents before that cargo is shipped.

I am concerned, however, that about six months after his initial announcement about CSI and nearly a year after September 11th, specific details of that initiative have yet to be provided and only a few agreements have been reached with foreign ports. Commissioner Bonner, in testimony to Congress, outlined that his objective was to reach agreements with the twenty largest U.S. trading partner ports, but we still need additional information about the timeline for reaching those agreements and specifically what we hope to achieve.

I commend the Commissioner for his work in securing agreements with the governments of Singapore, Canada, Belgium, and the Netherlands to station U.S. Customs officers at specific ports there, but again, the details of those agreements—especially the number of inspectors that we'll be able to place in those ports and the extent of their authority to actually inspect high-risk containers remains unclear. I look forward to hearing more today about those agreements and the status of negotiations with the Pacific Asian ports that handle a vast amount of the cargo sent to Washington State ports.

**Prioritizing point of origin inspection efforts**

If there is one thing that truly makes Puget Sound ports unique, it is that they sit directly adjacent to the downtown areas of our most populous cities.

While inspections at our ports and additional security at those ports are essential, we simply cannot ensure the safety of our residents—and our dockworkers—unless we have systems in place to inspect and secure cargo at its point of origin.

Every day 50,000 containers enter the Ports of Seattle and Tacoma, and nearly 6 million containers enter our nation's ports each year.

Over 90 percent of Seattle's waterborne trade is with Pacific Asian nations, totaling more than $30 billion in total value in 2000. We still need to develop agreements with Hong Kong, Kobe, Tokyo, Shaghai, Kaohsiung, and the many other Asian ports that do large volumes of business with Seattle and Tacoma, and other northwest ports

Now, I realize that this isn't as simple as snapping our fingers and sending money for technologies or law enforcement officers. International negotiations are tough, they take time, and they often require sacrifice. But frankly Mr. Chairman, I don't think we have a second to spare. Expanding security beyond our borders must be a critical element of our homeland defense strategies and it should be at the very forefront of this administration's foreign-policy agenda.

That's why I wrote to President Bush last week suggesting that he establish a cabinet-level task force on cargo security, including the Secretaries of Commerce, State, and Transportation; and that his task force establish detailed plans for point-of-origin container security. I also encouraged the Administration to establish a special negotiating team comprised of the United States Trade Representative, the

Commissioner of Customs, and the Commandant of the Coast Guard to negotiate agreements similar those reached with Singapore, Rotterdam and Antwerp,and the recently enacted Ridge-Manley "Smart Border Declaration" that has been implemented for inspections along the northern border.

We need high-level leadership on this issue and we need it now. We should use our commercial leverage to push for international standards and agreements to place customs inspectors in foreign ports and for ensuring secure transport between ports.

And if this requires additional resources to carry out this mission, I am confident that Congress would act quickly—as we did immediately after September 11th, to make those available. So I've also urged the President to submit a budget request to Congress for funds that he may need to assist foreign governments' and individual foreign ports in deploying inspection technologies in those ports cooperating with the United States in establishing point-of-origin inspections and evaluating systems integrated cargo security systems.

**Conclusion**

Mr. Chairman, any homeland security plan that does not prioritize seaport security would be seriously deficient for cities like Seattle and Tacoma. So I again thank the Chairman for holding this hearing, and Senators Hollings, Murray, and Breaux for their work on this issue, and the witnesses who will share their expertise with us here today. I look forward to working with all of you as continue our efforts to keep our ports safe.

Senator WYDEN. I thank you, and we will also put the letter that you sent earlier into the record. I think it makes a number of important points, and congratulations to you for doing that.

[The information referred to follows:]

---

Hon. GEORGE W. BUSH,
President of the United States,
The White House,
Washington, DC.

Dear Mr. President:

I am writing to express my serious concerns about the security of our nation's seaports and the status of efforts to improve the screening of cargo before it sets sail for ports in the United States, including those in the Puget Sound. Nearly one year after the September 11th incidents, efforts by your administration to develop and implement comprehensive cargo-security safeguards to protect port cities such as Seattle have progressed slowly and with little cohesion.

I am pleased that you have acted expeditiously to strengthen security along our borders and in improving the screening of passengers and baggage at our airports. After September 11th, I worked with my colleagues in Congress to provide the funding and authority necessary for these domestic efforts to be implemented successfully. I am concerned, however, that equivalent administration efforts to screen goods entering U.S. ports for weapons of mass destruction have been considerably less aggressive.

While I applaud the efforts of Commissioner Bonner to develop the container security initiative (CSI), I am particularly concerned that nearly six months after his initial announcement, specific details of that initiative have yet to be provided and only a few agreements have been reached with foreign ports. Commissioner Bonner, in testimony to Congress, outlined that his objective was to reach agreements with the twenty largest U.S. trading partner ports, but did not indicate a timeline for reaching such agreements.

I understand that the first completed accords, at least in principle, have been reached this month with the ports of Singapore, Rotterdam and Antwerp, but am not aware of any target dates set by your administration for the successful completion of the others, particularly with Asian nations that are the primary trading partners for Pacific Northwest ports. I also understand that the Coast Guard has engaged in discussions at the International Maritime Organization on creating strong standards for the inspections of cargo in transit.

I believe that the safety of U.S. citizens living in close proximity to major U.S. ports must be a top priority for this administration. Every day 50,000 containers enter the Ports of Seattle and Tacoma. In a rush to establish strong domestic measures for securing the borders, we must not overlook the fact that some of the great-

est threats to our nation may be delivered in one of the fifty thousand containers arriving in our ports daily. While scanning more cargo as it leaves our ports is important, inspecting those containers for potential threats before they leave their foreign ports of origin is absolutely critical for the safety of those working and living near our ports.

I am also concerned that a series terrorist incident has the potential to bring global commerce to a virtual standstill, and could force manufacturers and retailers in the Pacific Northwest to cease operations within days of an attack. I am encouraged by the efforts of the Ports of Seattle and Tacoma, along with several east coast ports and ocean carriers, to implement the "Operation Safe Commerce" initiative that is testing concepts and technologies for the pre-inspection and transport of goods, while maintaining the flow of international commerce.

We need clear and aggressive efforts by your administration to prioritize container security at the highest levels and to lead international efforts, in cooperation with the private sector, toward the rapid establishment of international standards for point-of-origin inspections. To reach these objectives, I strongly urge you to take the following steps:

1. Convene a cabinet-level team, including the Secretaries of Commerce, State, and Transportation, to establish detailed plans for point-of-origin container security;

2. Establish a special negotiating team comprised of your trade negotiator, the Commissioner of Customs, and the Commandant of the Coast Guard to negotiate agreements similar to the Singapore accord and the recently enacted Ridge-Manley "Smart Border Declaration" that has been implemented for inspections along the northern border. A similar team should work within international organizations to develop standards and agreements to place customs inspectors in foreign ports and for ensuring secure transport between ports;

3. Submit a budget request to Congress for funds to assist foreign governments' and individual foreign ports in deploying inspection technologies in those ports cooperating with the United States in establishing point-of-origin inspections and evaluating systems integrated cargo security systems;

The development of a comprehensive system for screening cargo while maintaining the flow of commerce requires agreements on a range of complex issues between governments and between individual ports. The intricacy and importance of this issue necessitate the involvement of administration officials at the high-level. I urge you to make cargo security one of your highest priorities in your ongoing efforts to protect the homeland and look forward to working with you to ensure that you have all of the tools and resources necessary to implement these measures immediately.

Sincerely,

MARIA CANTWELL
*United States Senator*

Senator WYDEN. And let us go now to Mr. Browning, and you can take five minutes or so. That will leave some time for questions.

## STATEMENT OF DOUGLAS M. BROWNING, DEPUTY COMMISSIONER, U.S. CUSTOMS SERVICE

Mr. BROWNING. Mr. Chairman, first of all, Mr. Chairman, Senator Wyden, Senator Cantwell and Senator Murray, I want to thank you for the opportunity to appear before you today and testify.

Since September 11th, the U.S. Customs Service's top priority has been responding to the continuing threat as our seaports and land ports, doing everything we responsively and reasonably can to keep terrorists and terrorist weapons from entering the United States. Today, I would like to describe the steps Customs has taken to secure our nation's seaports.

In terms of logistics and economics, all nations should be concerned about the ways global trade would be impacted by a catastrophic event involving sea containers. (1) About 90 percent of world trade moves in containers, much of it carried on ocean-going container ships. The devastation caused by terrorists if they were

to succeed in concealing a weapon of mass destruction (2) is unthinkable, and the impact on our economy would amount to billions in losses. Much of world trade would grind to a halt as we struggled to create a system that would secure against another such attack.

For these reasons U.S. Customs has taken several steps to tighten security at our seaports. (3) Customs officials have been operating at Alert Level 1 since September 11th and will continue to do so. This requires sustained, intensive anti-terrorist questioning, and it includes increased inspections of travelers and goods at every port of entry. Customs has also deployed additional X-ray and gamma ray machines, (4) and other technology that will greatly enhance our security, as well as the flow of commerce through our ports. (5) Customs believes that it must work to push our line of defense outward away from our seaports and towards foreign ports of departure. This will allow Customs more time to react to potential threats, to stop them before they reach us and to expedite the flow of low risk commerce.

(6) Customs builds on past successful security models between Customs and the trade designed to prevent legitimate commercial shipments from being used to smuggle illegal goods. (7) The Container Security Initiative, or CSI, places Customs personnel in the world's major shipping ports, the top 10 of which process about 50 percent of all sea containers imported into the U.S. The Customs officers will identify and pre-screen cargo containers that pose a high risk of containing terrorists or terrorist weapons before they are shipped to the United States. This simple concept represents a major revolution in standard Customs practice.

Currently most customs services around the world including ours target and inspect high risk containers at the port of entry. This system has been adequate to meet the ordinary threats of narcotics smuggling (8), but it is not sufficient to address the danger posed by terrorists (9), the threat presented by weapons of mass destruction. We may be content to seize narcotics at the U.S. port, but if a container were used to smuggle a weapon of mass destruction, finding it at the port may be too late to save American lives and infrastructure.

I am happy to report we have started the process of screening the 500,000 containers. (10) We have also confirmed arrangements to send our inspectors to Rotterdam, Antwerp, and Lettavre, and is in various stages of negotiating CSI partnerships with Singapore and Hong Kong. Technology and information are essential to successful container security strategy and to our counter terrorist mission in general. The more technology and information we have and the earlier in the supply chain we have it, the better.

In addition to the examination and inspection devices already in the Customs' arsenal, we will continue with plans to develop and broadly deploy "smart" containers with electronic seals that will indicate when they have been tampered with. Effective use of technology depends largely on good targeting for which we have require advance information.

Customs examines a small percentage of cargo entering the U.S. but these examinations are not performed randomly. In fact, our decisions are the result of careful screening based on information

culled from a vast database on shipping and trading activities known as the Automated Manifest System. Customs analysts use targeting systems to locate anomalies or manifests that appear unusual, suspect or high risk. This system has served us well, but it can and must serve us better in light of September 11th.

Legislation currently under consideration would make the electronic transmission cargo manifest information in advance of entry mandatory. This would increase the amount of information Customs can input into our targeting systems, thereby enhancing our ability to spot potential risks. This will take us much closer to where we ultimately need to be, and that is to have full information on incoming cargo before it even leaves a foreign port. We appreciate the support the Congress has shown for making the advance electronic transmission cargo manifest information mandatory, and we look forward to providing whatever assistance as may be necessary as you consider these issues.

Today, I have described only a few of customs' efforts that are bolstering our defenses against terrorism. The Customs Service is committed to working closely with our law enforcement counterparts as well as with the international community and the private secter to deter terrorists that would strike America.

Thank you again for the opportunity to testify, and I will be more than willing to take any questions that you have. Senator Wyden: Thank you, Mr. Browning. Very helpful statement.

[The prepared statement of Mr. Browning follows:]

PREPARED STATEMENT OF DOUGLAS M. BROWNING, DEPUTY COMMISSIONER, U.S. CUSTOMS SERVICE

Senator Wyden, Senator Murray, thank you for the opportunity to testify here today.

Since September 11th, Customs' top priority has been responding to the continuing threat at our land borders, seaports and airports. Our highest priority is doing everything we reasonably and responsibly can to keep terrorists and terrorist weapons from entering the United States. Today, I would like to describe for you the steps Customs has taken to secure our nation's seaports.

From both a logistical and economic perspective, all nations should be concerned about the ways global trade would be impacted by a catastrophic event involving sea containers.

Sea containers represent a vital artery of global commerce. The vast majority of world trade—about 90-percent—moves in containers, much of it carried on ocean-going container ships. Nearly half of all incoming trade to the United States by value—about 46-percent—arrives by ship, and most of that is in containers.

Unfortunately, sea containers are susceptible to the terrorist threat.

The devastation caused by terrorists if they were to succeed in concealing a weapon of mass destruction—even a crude nuclear device—among the tens of thousands of containers that enter U.S. ports each day is unthinkable. And the impact on our economy would amount to billions in losses. Much of world trade would simply grind to a halt as we struggled to develop a security system that would provide assurance against another such attack.

For these reasons, Customs has taken several steps to tighten security at our seaports. Across the country, Customs officials have been operating at Level One alert, which requires sustained, intensive anti-terrorist questioning, and includes increased inspections of travelers and goods at every port of entry. Customs has also deployed to its seaports additional x-ray and gamma ray machines, radiation detectors, and other technology that will greatly enhance security as well as our ability to speed the flow of commerce through our ports.

But our efforts to secure America's seaports from the terrorist threat must go beyond fortifying our own ports. Customs believes that it must also do everything possible to push our line of defense outward—away from our seaports and towards foreign points of departure. Pushing our security outward will allow Customs more

time to react to potential threats—to stop them before they reach us—and to expedite the flow of low-risk commerce across our borders.

The Customs-Trade Partnership Against Terrorism, "C–TPAT," builds on past, successful security models between Customs and the trade that were designed to prevent legitimate commercial shipments from being used to smuggle illegal drugs. Trade is now tightening its supply chain security to prevent legitimate commerce from being exploited by terrorists.

As the primary agency for cargo security, U.S. Customs should know everything there is to know about a container headed for this country before it leaves its foreign port for the United States.

The Container Security Initiative, or CSI, places Customs personnel in the world's major shipping ports—the top ten of which process about 50-percent of all sea containers imported into the U.S. The Customs officers will identify and pre-screen high-risk cargo containers that pose a risk of containing terrorists or terrorist weapons *before* they are shipped to the U.S.

This simple concept represents a major revolution in standard practice. Currently, most customs services around the world—including ours—target and inspect high-risk containers as they sit in the port of *entry*. Historically, this has been adequate to meet the ordinary threats of narcotics smuggling or evasion of customs duties.

But this system is not sufficient to address the danger posed by terrorists for one simple, yet sobering, reason—the threat presented by weapons of mass destruction. We may be content to seize narcotics at a U.S. port, but if a cargo container were to be used to smuggle a weapon of mass destruction set to detonate upon arrival, finding it at the port may be too late to save American lives and infrastructure.

This is why we must work with our foreign counterparts to screen the cargo at the port of origin, rather than at the port of entry in the U.S.

CSI is well underway. We have started the process of screening the 500,000 containers that come to the US each year from Montreal, Vancouver, and Halifax. Customs has confirmed arrangements that will allow us to send personnel to Rotterdam, Netherlands; Antwerp, Belgium; and LeHavre, France, and we are in various stages of negotiating CSI partnerships with Singapore and Hong Kong.

Technology and information are essential to a successful container security strategy and to our counter-terrorism mission in general. The more technology and information we have, and the earlier in the supply chain we have them, the better.

In addition to the examination and inspection devices already in Customs' arsenal, we should continue with plans to develop and broadly deploy "smart" containers—with electronic seals that will indicate tampering.

The effective use of technology depends largely on good targeting, for which we require *advance* information. Customs examines a small percentage of cargo coming into the U.S. Yet it is important to note that these examinations are not performed randomly. In fact, our decisions are the result of careful screening based on information culled from a vast database on shipping and trading activities known as the Automated Manifest System, or AMS. Customs analysts use targeting systems within AMS to locate anomalies or manifests that appear unusual, suspect, or high-risk. This system has served us well, but it can and must serve us better in light of September 11th.

Legislation under consideration would make the filing of electronic transmission cargo manifest information in advance of entry mandatory. For Customs, this would increase the amount of information we can input into our targeting systems, thereby enhancing our ability to spot potential risks. This bill will take us much closer to where we ultimately need to be—and that is to have full information on incoming cargo before it even leaves the foreign port. But for us to work most effectively, we need legislation to mandate that Customs receives the information, whether for imports or in-bond shipments, even before the container is loaded on board the ship bound for the United States.

We appreciate the support Congress has shown for making the advance filing of electronic transmission cargo manifest information, mandatory. We look forward to continuing to assist Congress in its efforts to enact seaport security legislation.

Today I have described only a few of Customs' efforts that are bolstering our defenses against terrorists. The Customs Service is committed to working closely with our law enforcement counterparts, as well as with members of the international community and the private sector, to deter terrorists who would strike America.

Thank you again, Senator Wyden, Senator Murray, for this opportunity to testify. I would be happy to answer any questions you may have.

Senator WYDEN. Mr. Dinsmore?

**STATEMENT BY MIC DINSMORE, EXECUTIVE DIRECTOR, PORT OF SEATTLE**

Mr. DINSMORE. Thank you very much. What a pleasure to have you here in Seattle and at the Port of Seattle. Today I have the opportunity to talk about a critical issue of port security and specifically answer the question how do we secure our port communities, and in doing that, how do we ensure the movement of commerce through these communities in a fast and efficient manner.

Ever so briefly allow me to give you a little background on the Port of Seattle. We are one of the most diverse ports in this Nation. Yes, we have both an airport and a seaport, and the combination of both impacts economic viability in this State in excess of $34 billion annually. In the container business, combined with Tacoma, as Senator Murray indicated, we are the third largest load center for containers in this Nation, and as of next year, we will have over 400,000 passengers moving through our harbor with the new activities relative to the cruise industry.

What I would like to do is make five points during my presentation. One, making sure ports and the goods shipped through them are secure, and that is absolutely essential if we are to avoid severe economic distress in this country and abroad. Two, we are pleased, very pleased with the help Congress has provided so far, but more is needed, and it must be rapid. Three, in order to achieve the greatest return from our port security effort, we must rely on existing and emerging technology. Four, whatever processes we use to make our facilities more secure ought to allow us to expedite the flow of commerce through our gateways, and lastly, it is important to ensure that foreign goods coming into the U.S. from both Canada and Mexico experience the same inspection rigor that goods coming to the U.S. from other foreign ports experience.

The vast majority of goods consumed by the American people come from some other country, and 90 percent of those goods travel to this Nation by waterborne vessels, because we no longer have huge warehouses and distribution centers solely for the storage of these goods. Instead they use ocean containers to control inventory and a concept we know called "just in time delivery." This means that before the commerce reaches final designation for sale, the inventory will be either in a container or on board a container vessel.

This system makes waterborne commerce even more critical to the Nation's economy, because it is on the water, and it is in most cases in ocean-going containers that much of the inventory for the next few weeks are kept.

If the system through which these goods are delivered is in any way disrupted because of a terrorist act, at the present time, it would call into question the entire system, and the Federal Government would indeed have to shut the system down. In doing so, it would not only stop goods from being delivered to U.S. ports, but would also stop the flow of freight between ports in Asia and Europe and the rest of the world as well as others that rely on a regular and uninterrupted flow of goods in exchange for products their citizens create that will be consumed by Americans.

If the system shuts down for more than a week, the consequences to many businesses that rely almost solely on foreign goods would be devastating, and as we lived through the 9–11 experience, we

had our Nation's airports shut down for four or five days. The impact of shutting down our seaports would be much more challenging to turn over and start up again.

We must find ways to secure port facilities so that it makes it more difficult for a terrorist to cause damage either hurting our people or citizens or facilities. We must make sure that the security of goods coming into this country and going into other nations is absolutely assured. We must be absolutely sure that what was loaded in the container is what is stated on the manifest, and this needs to be verified independently of the shipper or even the shipping line. We need to make sure that the goods during their voyage across the ocean and overland to their final designation does, in fact, remain secure.

Tim Farrell of the Port of Tacoma will speak to the specific effort that the Ports of Seattle and Tacoma have begun to secure our facilities and the goods that flow through them.

I want to thank you, Senator Murray, for the $93 million that was recently distributed to harden our facilities in the supplemental appropriations bill, to continue that wonderful work. There is also funding in the supplemental appropriations bill that will begin addressing what I refer to as point-of-origin container security.

Between the Ports of Seattle and Tacoma more than 3,000 individual ocean-going containers cross our terminal facilities each day and are trucked or taken by rail to points outside our immediate port boundaries. The only evidence we have of what is in these containers comes directly from the manifests which are provided to us, which of late are more specific but still do not come with an absolute guarantee of accuracy.

There is about $28 million in the supplemental appropriations bill devoted to Operation Safe Commerce which is an attempt, and I think a very good attempt, to guarantee the accuracy of the manifest and to track and identify tampering of those containers.

Once again I want to applaud Senator Murray for including these dollars in the supplemental appropriations bill and thank you, Senator Cantwell and Senator Wyden, for your support of this bill. I urge you once the supplemental bill is passed to make sure that any dollars made available for Operation Safe Commerce are distributed as quickly as possible, because we obviously do need them.

Tim will talk again a little later on the Safe Commerce Initiative which is a port and private sector-based initiative that we believe has the best chance of securing goods that come from overseas. There is also funding in the Treasury portion of the supplemental appropriations bill for U.S. Customs Container Security Initiative or CSI as it is affectionately called. These funds should also be made available because Safe Commerce, in conjunction with CSI, will enhance container security at foreign ports.

I want to talk a moment now about how we make both our seaports and goods that come into our areas more secure through technology. We must move rapidly in deploying technology that will create a more secure environment for the international trade arena. There are many, many vendors, some in this hearing, competing for a piece of the security pie. We favor, absolutely favor the

use of tested and proven technologies and extensive involvement of private sector entities and ports in testing and deploying new technology, especially when there is a need to closely work with our foreign partners.

Federal Government agencies must be providing oversight and working closely to ensure that their standards are met, but port districts and many private entities are more nimble than the Federal Government agencies. In addition, we have extensive business relationships with shippers, shipping lines, foreign ports and others in the chain of custody for goods coming into and leaving the country. Our ability to rapidly deploy and test a particular technology and then actually using the technology long term clearly is a plus for all of us. We want to reach a point where a significant number of boxes that come through the Ports of Seattle and Tacoma are guaranteed to have been loaded according to particular standards, that can verify the manifest accurately reflects the goods that are loaded. We also want to make sure that the goods can be tracked from where the box is loaded to where it is unloaded and the goods distributed——

Senator WYDEN. Mr. Dinsmore, I am sorry to have to interrupt. I just want to ask my colleagues for their questions. Are there any other particular points that you would like to make?

Mr. DINSMORE. No, I have made those points.

Senator WYDEN. I just want to go to both of them. They have spent a lot of time on these issues.

[The prepared statement of Mr. Dinsmore follows:]

PREPARED STATEMENT BY MIC DINSMORE, EXECUTIVE DIRECTOR, PORT OF SEATTLE

**Solutions for Secure Commerce**

Good afternoon, Senator Wyden, Senator Murray and Senator Cantwell. Thank you for the chance to speak to you on the critical issue of seaport security and specifically, solutions to the question: How do we secure our port communities and the goods flowing through them?

First, let me give you some background on the Port of Seattle. We are one of the largest and most diverse ports in the nation. We operate Sea-Tac airport and have many other commercial maritime and non-maritime businesses. Our contribution to the state's economy is more than $34 billion annually. In the container business, combined with the Port of Tacoma, we are the third largest container "gateway" in North America. We are also one of the nation's fastest growing cruise ports, and next year, we will see more almost 500,000 people sailing from Seattle.

I want to make five points during my presentation: 1) Making sure that ports and the goods shipped through them are secure is absolutely essential if we are to avoid severe economic distress in this country and abroad; 2) We are pleased with the help Congress has provided so far, but more is needed and it must come rapidly; 3) In order to achieve the greatest return from our port security efforts we must rely on existing and emerging technology; 4) Whatever processes we use to make our facilities more secure ought to also allow us to expedite the flow of goods through them; and 5) It is important to ensure that foreign goods coming into the US through from Canadian or Mexican ports experience the same inspection rigor that goods coming into US ports receive.

While this may sound like a very dramatic and maybe somewhat outlandish statement, it is a very possible scenario if we do not adequately prepare ourselves. A terrorist incident at a major port in this nation right now would produce the biggest economic downturn this nation has experienced since the Great Depression. Let me explain why.

The vast majority of goods consumed by the American people come from some other country and 90 percent of those goods arrive in this nation at US ports on waterborne vessel. Businesses no longer have huge warehouses and distribution centers solely for the storage of these goods. Instead, they use ocean-going containers

to control inventory and a concept called "just in time delivery," which means the goods reach their final destination just before they are placed on the retail shelf.

This system makes waterborne commerce even more critical to the nation's economy because it is on the water, and in most cases in ocean-going containers, that much of the inventory for next weeks goods are kept. If the system through which those goods are delivered is in any way disrupted because of a terrorist act, at the present time, it would call into question the entire system and the federal government would have to shut it down. In doing so, it would not only stop goods from being delivered to US ports, but it would also stop the flow of trade at ports in Europe and Asia, as well as many other places that rely on a regular and uninterrupted flow of our goods in exchange for products their citizens create that will be consumed by Americans. If the system shut down for more than a week, the consequences to our economy would be devastating.

We must find ways to secure port facilities so that it becomes more difficult for a terrorist to cause damage to facilities on injury to people. We must make sure that security of goods coming into this country and going to other nations, is assured. We must be absolutely certain that what was loaded onto the container is what is stated on the manifest, and this needs to be verified independently of the shipper or even the shipping line. We need to make sure that the goods during their voyage across the ocean and overland to their final destination remain secure.

I want to thank you for the $93 million that was recently appropriated to harden our facilities and we applaud the funds included in the supplemental appropriations bill to continue that work. There is also funding in the supplemental appropriations bill that would begin addressing what I refer to as "point of origin" container security. Between the Ports of Seattle and Tacoma more than 3000 individual ocean-going containers cross our terminal facilities each day and are trucked or taken by rail to points outside our immediate port boundaries. The only evidence we have of what is in these containers comes from the manifests that are provided to us, which of late are more specific, but still do not come with a guarantee of accuracy. There is about $28 million in the supplemental appropriations bill devoted to Operation Safe Commerce, which is an attempt to guarantee the accuracy of those manifests and to track and identify tampering of the container if it were to occur. I want to applaud Senator Murray for including these dollars in the supplemental appropriations bill and I want to thank Senators Cantwell and Wyden for their support for that funding. Once the supplemental bill is passed I urge you to make sure that any dollars made available for Operation Safe Commerce are distributed as quickly as possible without the usual wait we see with federal funds. Safe Commerce, which Tim will describe later, is a port and private sector-based initiative that we believe has the best chance of securing goods coming from overseas. There is also funding in the Treasury portion of the supplemental appropriations bill for the US Customs Container Security Initiative or CSI as it is affectionately called. These funds should also be made available because Safe Commerce, in conjunction with CSI, will enhance container security at foreign ports.

I want to talk a moment about how we make both our seaports and the goods that come into them more secure through technology. We must move rapidly in deploying technology that will create a more secure environment for the international trade arena. There are many technology vendors competing for a "piece" of the security pie. We favor the use of tested and proven technologies and extensive involvement of private sector entities and ports in testing and deploying new technology, especially when there is a need to work closely with our foreign partners. The federal government agencies must be providing oversight and working closely to ensure that their standards are met, but port districts and many private entities are more nimble than the federal government agencies. In addition, we have extensive business relationships with shippers, shipping lines, foreign ports and others in the chain of custody for goods coming into and leaving this country. Our ability to rapidly deploy and test a particular technology and then actually use the technology long-term is a real plus.

We want to reach a point where a significant number of "boxes" that come through the ports of Seattle and Tacoma are guaranteed to have been loaded according to particular standards that can verify that the manifest accurately reflects the goods loaded. We also want to make sure that the goods can be tracked from where the box is loaded to where it is unloaded and the goods distributed. In addition, it is important that we try to move goods more quickly using technology and not find ourselves having to slow the process because we need to be overly-cautious about what comes into this country. A slowdown in the process of moving goods through the system will ultimately result in making US ports less competitive, which will have a major impact on US ports and the US economy.

I now want to talk about how we could easily secure our front door and leave other doors open if we are not careful. We need to make sure that the same processes that we send goods through when they enter a US port is duplicated for goods from overseas that are shipped into our country through adjacent borders—Canada or Mexico. We fear that if it becomes more difficult and costly to bring foreign goods into US ports because of security measures, there could be a rush to send those goods through either Canada or Mexico. If this happens, it will totally undermine all our security efforts and put the nation in a vulnerable situation. Overseas goods coming into the US from these adjacent nations should be subjected to the same rigor that goods coming into US facilities must face. It will be critical for the US Congress to make sure that this is the case.

I will end by again thanking you for conducting your seaport security hearing in Seattle and at our facilities. I would like now to turn over the microphone to Tim Farrell, Deputy Executive Director of the Port of Tacoma.

Senator WYDEN. And we will go to Senator Murray.

Senator MURRAY. Thank you very much, Mr. Chairman, and I want to start with Admiral Brown. This Administration has proposed combining over a hundred different Government organizations into a single Homeland Security Agency to protect the United States from internal threats, and as part of that proposal the President has called for the Coast Guard to be moved from the Department of Transportation to the new Department of Homeland Security.

I wanted to find out while you are in front of us today whether you are concerned that that new agency focus on homeland security may diminish your ability to deal with Search and Rescue, Drug Enforcement, Environmental Management, Fisheries Management, that are such important missions of your agency.

Admiral BROWN. Thank you for the question, Senator. As you have indicated in your statement, and as I indicated in my statement, the other things we do as a multimission agency are critically important, Search and Rescue, Drug Law Enforcement, Marine Environmental Protections, just to name a few, and frankly not only are those things important, they are a center of synergistic contribution to homeland security and homeland defense.

So as it relates to your question about diminishing our ability, diminishing our focus, diminishing our capacity on those other elements, the Commandant has been very clear on what he considers to be appropriate criteria which should be considered, and those are threefold.

First and foremost is that the Coast Guard be moved as an entire entity. Second, that we maintain that multimission, maritime, military focus that we have had which gives us those capabilities, and third and final that we continue to have the complete mission set as a multimission agency. We get a lot of synergy from that. So given those, those elements, given a clear mandate and adequate resources, I see us continuing our ability to provide efficient and economic services to our Nation.

Senator MURRAY. Should we be concerned that if you are under an agency whose only focus is homeland security, that we will lose some of our priority in each of Fishery Management, Search and Rescue or other missions?

Admiral BROWN. I think as I indicated, we will respond to the tasking that we are given. Right now we are a multimission agency with a broad range of mandates, and to the extent that we are

transferred, and with singular focuses, the Nation will still have to get those services provided in some form or fashion.

Senator MURRAY. Let me ask you about the 96-hour advance notice of arrival requirement that you have for ships coming in to supply you with names of crewmen. It has been reported that ships have come and gone before that information has been processed and returned. Coast Guard has said that this is a problem because of communications delays between them and Federal agencies with the information. I think the Coast Guard has said that because we do not have them submitted electronically, it is a problem, and we are supposed to have some kind of final rule in June. Can you tell me to your knowledge has the rule to require electronic submission been finalized yet?

Admiral BROWN. I am not personally familiar with the current status of it, but I can say that the ability to transmit those kinds of information electronically is critical to us getting advance notification. Not only is it critical to getting it in a timely fashion to review the content of the information, but also that it be credible. So I do not know the current status of it, but in terms of electronic submission, it is critical for our marine maritime awareness.

Senator MURRAY. Captain Ellis, do you know if the rule has been finalized yet?

Captain ELLIS. Good afternoon, Senator Murray. I still have the route proposal right now. It is not finalized now.

Senator MURRAY. Admiral, one problem with getting good information and intelligence is that the vast majority of the ships entering the United States are foreign flag and operated by foreign crews. So it is really important that we get international support to ensure that our vessels do not present a risk.

One goal that the Coast Guard announced in this area is for an Automated Information System or transponders by 2004. We had a hearing on this in D.C. and the Coast Guard explained that we needed the cooperation of the IMO to implement that requirement and said that they would know more by late spring, a few months ago. Do you know what the, do you know the status of the IMO's position as yet on that proposed requirement?

Admiral BROWN. The proposal has been reviewed, and they are scheduling an intersessional which is a meeting in advance of the normal one. I think that is scheduled for December. Right now, the acceleration of the AIS is being favorably received. I think right now the only major signatory is Russia, but at this point, who is looking more at the original schedule than the accelerated one. So right now the intersessional in December will give us the final answer.

Senator MURRAY. So we will not know until December whether the IMO is——

Admiral BROWN. Until it goes through its final regulations and voting on it, but that is, in fact, an advance over its normal conduct of business, and at this point is being favorably received.

Senator MURRAY. Approximately 1.8 million containers enter Puget Sound ports every year. That is about 5,000 containers every day. Do you know short of opening and inspecting every container there is really no effective way to verify what is in those containers, and right now less than 2 percent of the containers enter-

ing the United States are actually looked at. It is clear if we increase the number of containers we inspect, we will have an impact on the efficient flow of commercial goods through our ports.

I am curious whether our efforts in partnering with foreign ports, improving communications with Federal agencies, clear security standards and better inspection technology, lower the amount of cargo that we need to annually inspect?

Admiral BROWN. Absolutely, and as Mr. Browning said, while it is 2 percent, it is the right 2 percent. Focusing on which ones to look at, not looking at everything is really the right way of going on with business, and I defer to Mr. Browning on that point.

Senator MURRAY. Mr. Browning?

Mr. BROWNING. Actually, Mr. Brown is on point of that. We actually inspect 100 percent of containers that are determined to be high risk. We talked about the fact that we have a, what we refer to as a layered defense to determining what we want to take a look at. Anything short of that would, in fact, negatively impact the flow of legitimate trade. Also, but I think also, there is something that you need to understand about the 2 percent number that we are dealing with, and in that regard, I think a vote of thanks from the U.S. Customs Service due to your support on CSI, because we have recognized that we are probably financing our paradigm now, that the ALGS doing business from the Customs standards have to be reexamined, and that is why we pursued some of the initiatives such as CSI and the CT pack.

When you look at the total volume of the containers that we are looking at, we are actually inspecting somewhere in the neighborhood of about 8 percent of all of the containers that come into the United States, which is somewhere in the neighborhood of 1.5 million containers a year get broken open by the U.S. Customs Service.

But rest assured, that is not random breaking open containers. This is taking information, slamming it against your database, making a determination and giving that container a score, and at each successive step, ratcheting up the process, unless we are satisfied that it does not pose a risk or we are satisfied of the need to open it.

Senator MURRAY. Mr. Browning, do you know that our intelligence agencies currently have adequate information about cargo transportation?

Mr. BROWNING. I think our intelligence agencies have a lot of information. I cannot speak specifically about cargo, but I can, however, say it is one of the things that we are trying to do, and someone asked a question about what post-9–11, where are we going as an organization and as an agency. I think there has been an awful lot of cooperation between the law enforcement agencies, unprecedented, in fact.

Senator MURRAY. Do you share all your information with the Coast Guard?

Mr. BROWNING. We are marching lockstep with the Coast Guard with many things. The manifest system is information that we applied. The point that you raised about the MPR and the 96-hour manifest, we are piggybacking our effort, and they are providing in-

formation to us as part of that process. So there is a great deal of cooperation that is going on between the agencies.

I have the privilege as part of the Homeland Security Deputy Council to work on the Container Working Group, and that group has all of the concerned organizations involved in taking a look at what we do to shore up our defenses in that area.

As to the specific information that the intelligence community has, I cannot speak to that with any level of detail, Senator. Sorry.

Senator MURRAY. Thank you very much, Mr. Chairman.

Senator WYDEN. Thank you. Senator Cantwell?

Senator CANTWELL. Thank you, Mr. Chairman, and I thank the panelists for their valuable testimony.

Like Senator Murray, I have security concerns about the Office of Homeland Security, and maybe commandeering some budgets, and we certainly do not want that to happen, and like Rear Admiral Brown, I did have a chance to ask which has oversight of some of the agencies going in that, specifically about the Coast Guard budget and whether it will be protected for those same things that Senator Murray outlined, and so hopefully, we will have a written answer from him that will help protect us in the future and clarify that as we go through the process of looking at this legislation in the Senate.

I guess I wanted to focus my first question on, with so much public attention and actually probably public experience has been focused on either at the border or at the airports and our individual travel, and we know that the lines are longer and more identification is required, and more specifications about, about travel plans and designations, at least at our border. I am not sure that it is clear what exactly we have deployed since 9–11 as it relates to container cargo, what changes have we made that are different in how we handle cargo, say for example, in the State of Washington.

Mr. BROWNING. Senator Cantwell, let me take a quick stab at the question. From the U.S. Customs Service prospective, we certainly have gone out with what we consider a wide array of nonintrusive inspection technology. In 1991, we had one nonintrusive inspection device which was an X-ray van. Today, we have devices that range the full spectrum of activities, a total of 86 pieces that are on line right now. Another, at the end of the day probably as many as 139 pieces. We have $102 million worth of 0–2 funding including both our appropriations and supplemental that will give us additional equipment. Our goal is to have at every port of entry some form of nonintrusive inspection equipment or system available.

Senator CANTWELL. Just like X-ray or baggage, like the new equipment that will be deployed at the port?

Mr. BROWNING. However, it is X-ray. It is gamma ray, and it is what we refer to as—or vehicle and core—inspection system, and we have taken those systems and modified those systems into every environment in which we work. We do it in rail. We do it in the seaport environment. We have taken them and put them in mobile and relocatable forms. The relocatable form allows us to move it within 8 hours, and the mobile allows it to deploy it within 20 minutes. So we have become very flexible in our ability to use technology.

In addition, we recognize that there are some threat areas for which some of the existing technology has not evolved to the point that it is reliable. So we are working with a number of labs, including the Pacific Northwest labs to develop some of these technologies based on our specifications, so that we can go out to vendors and see if there are vendors that can meet those technology needs. We are looking at the biochem area.

Senator CANTWELL. What would that be specifically, because you are talking high risk cargo. Not every piece of container cargo goes through that system.

Mr. BROWNING. Not every piece goes through.

Senator CANTWELL. The equipment that you have ordered, will it upgrade the number of at-risk containers to a higher percentage?

Mr. BROWNING. What it does is allow us to move more of it through more quickly. So we are spending less time examining. If you break a container down, it can take you anywhere, depending on the nature of the cargo, a few hours to half a day to break that container down and inspect that container. If you have the nonintrusive technology, we can do nonintrusive technology and do a 40-foot container in less than 6 minutes, and in fact, depending on the type of equipment we are using and the type of container we are examining, it can be done very quickly. So the value of that is it allows us to do our job better and quicker, and I think this is the point that was raised earlier about trying to find that balance between security and facilitation, and these are the kind of tools that would help us to do that.

Senator CANTWELL. So primarily it has been the deployment of more nonintrusive equipment, so that investment——

Mr. BROWNING. It has also been, also what has happened that has also made it is easier, we actually have done two additional things that are very, very important. We stood up an office of anti-terrorism within our organization, and that office has been responsible for coordinating our overall response to the counter-terrorism risk efficiency. We, also, to assist our people in the field, stood up an Office of Border Security whose whole mission was to take a look at our database, to take a look at our targeting tools and to refine those very sophisticated rules-based targeting tools to allow us to cull more information, to make a better determination about what level of risk to attach to a particular container. So what we have really done is to take our work product and refine that work product for the new environment, so that we can get information that our people need, get them the tools that they need to do the job quickly, and also so that they can make determinations on what is at risk and what we need to take a look at.

Senator CANTWELL. I want to come back to that, but I want to ask Mr. Dinsmore from the port's overall perspective, what has the port deployed in the container area that is different from what was pre-9–11?

Mr. DINSMORE. Thank you, Senator. To begin with, I agree with what you stated on behalf of U.S. Customs and on behalf of Coast Guard, there is clearly a new awareness on the seaport side subsequent to 9–11, but that being said, there is still a tremendous opportunity for improvement.

What is different? What we see that is different, Senator. We have still the need to make our land-side facilities more safe and secure, and that is an issue that we are talking about ongoing now, to on the water, when we have container ships and/or cruise ship activity in our harbor. We do have much more presence of the U.S. Coast Guard, and so that is visible. We are, on our land side, we have much more participation with our own law enforcement police department on the land side with our facilities.

Senator CANTWELL. Just making sure that there are not suspicious activities.

Mr. DINSMORE. That is correct, and I suggest there is much more ongoing dialogue with both U.S. Customs and the ports, U.S. Coast Guard and INS.

That being said, I say again, there is still tremendous need to expand that so there is additional quantitative outcomes that will benefit all of the ports in this Nation including Seattle and Tacoma.

Senator CANTWELL. Well, the reason, again, I mention because I think we have had so much attention, and obviously personal experience on the movement of people, and we obviously, given the comments that have been made by detained Al-Qaeda members about potential threats to sea or underwater, obviously, that is increasingly important to us knowing that we are a population center close to a border with many access points.

Back to this point of importance of point of origin as a concept, and the CSI system leans more towards that. Now, that is deployed in a limited number of places, correct? Singapore is probably our key spot. Is that correct?

Mr. BROWNING. Actually, Commissioner Bonner was in Europe this past week, and coming out of that was an agreement between Rotterdam, Antwerp, and, Le Havre to also have a similar program in all three of those points. So with Singapore and those three and Canada, we will now have four. I am sorry, five locations where we will have CSI operational. Our intent is to deploy the personnel to support these programs by the end of this fiscal year. It should be fully deployed to all of the locations to support this.

Senator CANTWELL. The ones that you just mentioned?

Mr. BROWNING. Of the five locations that I just mentioned, but we are continuing to have dialogues with several other ports that are on the list of our ports, and we are hopeful that we can have as many as 10 on line by the end of this year that will be commissioned.

Senator CANTWELL. But the Container Security Initiative is focusing at getting people at those points of origin, customs officials instead of doing the job at the point of entry, doing that job at the port of origin, but it seems to me that that is obviously labor-intensive and somewhat, I am not saying limited, but our ability to deploy that obviously is being phased in.

And we definitely found with the Ransom case that people go to the weakest place, that and while we might be building these great infrastructures in the Netherlands or Singapore, somebody is going to pick this route that we are not thinking about. So this issue of getting an international protocol, getting some agreement and coordinator seemed to me to be a critical point in getting those coun-

tries to agree with us that this is the security standard, and then having that deployed so that it did not just depend on how many customs officers we deploy at certainly cities seems to be a critical issue.

Mr. BROWNING. Actually, Senator, that is a very good point. There are actually a couple of issues that intrigue me about this initiative, CSI. I think you need to look at it in partnership with C–TPAT which is our partnership with the private sector, the private sector, people importing into the United States. A company like Microsoft, for example, has an awful lot of clout, leverage with the vendors that it deals with who do their international work, and their customs work, and one of the approaches that Microsoft is going to take as part of their participation in the Customs—Trade Partnership Against Terrorism was to start modeling guidelines for its vendors, and to go to its vendors and say if you are going to deal with us as a company, you have to do X, you have to do Y, you have to do Z, because as part of C–TPAT, we want to make sure that our cargo coming into the United States gets that specialized treatment that C–TPAT members who are agreeing to install these security standards are going to be eligible to receive.

If you take that, and you partner that up with what we are doing in the CSI area, you are now starting to build what we refer to as supply chain security, not just container security, but supply chain security, and I think the point was raised earlier, what we are looking at is to build a system that builds a system from point of vendor to point of consignor is totally security, and that is what we are trying to do is marry up those two pieces, so we can start the concept at supply chain security and get the notion out there that all of us have a vested interest in this.

One final point I will make to you, I had the occasion to speak with a gentleman from the Maersk line about the megaport concept, because we are receiving a great deal of criticism that said we are going to the megaports. You are closing off smaller ports that may not be in the same position as the megaports to have the infrastructure to build the degree of infrastructure, to allow your people to come there. We are never said as part of CSI that you could not import from any port in the world. What we are saying is that by handling the megaports, we give ourselves a level of certainty that the stuff that is coming in from those ports is relatively secure. That allows us to take our limited resources and direct them toward other areas that may pose a risk, and that is those weak points that may be coming in, and you are talking about 60 percent of the universe that we have to look at. If we can deal with that large a share of our work product so that we can refocus our resources, that makes good sense from both a trade facilitation standpoint, a security standpoint and an enforcement standpoint, and that has been the kind of approach we have been trying to build with both CSI, C–TPAT, our use of our resources in the United States.

Senator CANTWELL. I want to turn this over to the Chairman who has been so good to be here in Seattle today, but C–TPAT is, I mean, we are not in total cooperation on that, and that is individual partners?

Mr. BROWNING. We have made it very attractive for them. We have added some incentives to the C–TPAT process. Right now we have over 160, 170 companies that have come forward, and others are coming forward on a daily basis. We have provided some incentives that say if you are part of C–TPAT, you go to the green line, because we have some level of certainty about the movement of your goods, and that is, we have tried to make it attractive, so they will participate.

Senator CANTWELL. I think Rear Admiral Brown in his comment referred to the Manley-Ridge Agreement. The State Department also needs to take the lead in going to these countries and saying are you with us in the war on terrorism? If you are, part of it is helping to establish a security protocol for container cargo and agreeing on what those processes are going to be. Otherwise, we will be deploying Customs people in every port, every port in the world. I mean every exit point, and we need to build on the international cooperation of this. I do not know if you wanted to add anything?

Admiral BROWN. Just one thing to add to what Deputy Commissioner Browning said, and as we look forward to those kind of international agreements, the incentives and also the things that technology will bring us, at this point the Coast Guard is working very closely with a lot of the facility owners, port authorities through these mechanisms we talked about in port security committees. The Pacific Area Commander to Coast Guard has drafted guidelines for—security guidelines for facilities, and while they are not as sophisticated as some of the things that we have talked about for the future, today what we are doing is working with them to insure when we have places on our facilities, that we have security procedures for access control, for internal security. We are training for security members that wear I.D., procedures to make sure that the people that are coming into these facilities are people that are supposed to be there, that they are putting up barriers and those kind of things. So it is the fundamental, day to day, take care of business things that we are working with. We are working with the owners and getting those things in place here in the Port of Seattle, and that has happened since September.

Senator CANTWELL. Thank you, Mr. Chairman.

Senator WYDEN. I thank you, Senator Cantwell.

I only have a couple of other questions, my colleagues said it so well. To pick up on Admiral Brown, on this question of how the Coast Guard is going to work in the new Homeland Security Office, you know, for the life of me, I do not see how this can be done without billions of dollars additional funding, and the issue of just the nuts and bolts of how you would make this, this transfer just seems to be staggering. I mean, any way you look at it, what you all were doing before September 11th did not involve a whole lot on the issue of securing the country's borders. That was not a primary function of the Coast Guard before September 11.

So if you would, tell me, first, you said it would be done through synergies, and I know you have creative people there at the Coast Guard, and I am sure synergies produce some savings, and they will be great to see them at work, but how is this going to be done if you keep everything you have got, plus you are going to get these

new duties, how is this going to be done without billions of dollars of additional money? And take us, if you would, through your sense just operationally how it is going to proceed?

Admiral BROWN. Mr. Chairman, I would probably lose this job if I turned down potentially billions of dollars for our new responsibilities.

Senator WYDEN. How much are the synergies going to cost?

Admiral BROWN. Sir, just a quick historical perspective, and then we will look ahead. As you know, we became part of the Department of Transportation, moving from the Treasury, continuing to do our multimission responsibility, and I kind of see the future the same way, and not to be glib with you, but we have, we, during World War II had a lot of these security responsibilities, but the Coast Guard at that time was a lot larger, and as I have indicated in my opening statement, in response to the first question that Senator Murray asked was that the clear tasking and appropriate resources, and I was not trying to be glib when I said that we get economies and efficiencies through our synergies, but that is at our current level.

I think right now Senator Murray is aware of the support that she has provided, and we have been greatly appreciative of it, but I think the Commandant has been very clear to meet our material traffic, what we call Market One. That is our definition of a "new normalcy," that we see a multiyear budget strategy of growing the Coast Guard. So at this point we are not in the notion where we are able to meet our own internal requirement for the task that we have at hand.

So the short answer to your question is the resources will probably depend upon the requirements. If the requirements we have currently hold, we have a multiyear budget strategy that should get us there in about two to three years.

Senator WYDEN. Again, for me if you keep everything got, you are going to get all this new stuff, and you basically change the very nature of the agency. Even the physical move strikes me that it is going to cost a vast sum to do it. It is not going to come about through synergies, and you are a good man and a creative fellow, but for the life of me, this map does not have——

Admiral BROWN. Sir, I think a large part of what we will have to do or what we are currently doing—I mean one of the differences, for example, while we do search and rescue, SAR, we have a search and rescue posture. It is mainly kind of like the fire house where you are ready to go when you are needed.

For security, it is probably greater emphasis on presence. So that is not constant patrolling. So to the extent that there are enhanced presence requirements, then those numbers grow. So clearly our force structure flows from the strategy, and to date all the strategies we see, we have put together the budget strategies for them.

You talk about the physical movement. Those physical movements to the best of my knowledge and understanding will probably be small ones at the headquarters level. We are in the places where we need to be. We are in the ports that we need to be. We have the relationships that we need to have. So the movements from my perspective as a field commander that delivers a service,

we are in the places that we need to be to deliver the services, that is what need to do.

Senator WYDEN. Gentlemen, every seaport has unique characteristics. There are certainty unique, geographical and operational characteristics with respect to security. What are the unique concerns with respect to this port, this seaport that the Federal Government has?

Admiral BROWN. Sir, I will take a stab at answering that first. We are enormously challenged by geology here. When you look at our ports versus East Coast ports, so when you talk about things, security things like escorts, that those tend to be long escorts. We have challenging weather here. It is very unforgiving. So some of the craft that we have some places may not be suited as well to do those types of duties and responsibilities out here. We have a very challenging mix of strategic assets in terms of the Navy and being able to ensure they have free communications to the sea force protection, and that they also have protection in their home ports which is a new issue, a new issue for our Navy. But it is our responsibility to work with them to ensure that, and while it is large on the one hand, as Senator Murray indicated, we also have a very, very large Washington State ferry system, the largest in the Nation. So you have what we call a triad of, of security, strategic security assets, that we need to be concerned about, one of the highest recreational commuter and also fisherman use of this area, and also recreational.

So we need to tend to all of those, and I would say that when you combine all three of those, we do not have a port anywhere in the Nation—a lot of other ports have focuses like the Gulf is the oil, but here in the Puget Sound, we have as is indicated the third largest container complex, and so we are ranking in the top of all of those areas, and that, that myriad of diverse responsibilities is enormously challenging.

Just for a minute to talk about some of the other business. I hoped my comment talking about security, but at the same time, law enforcement is a layer where if you are there, and you are present, and you knew what the routes are, the same people that are not currently engaged in legitimate business, a lot of the concept we are talking about focuses on legitimate business. The people that are not in legitimate business are going to find the other routes. To the extent that we are there for drugs that are not in legitimate, to the extent that we know their routes and their rationales, these are the type of things that we need to pay attention to.

Senator WYDEN. Just to wrap up, Mr. Dinsmore, the Interagency Commission on Crime and Security in U.S. Seaports has the ports of this country expressing a fair amount of concern with the Federal Government basically kept in the dark. The Government has a specific amount of information, and that did not get to the ports or to people at the local level. Is that a concern that you have now, and if so, what is being done to address it?

Mr. DINSMORE. I would say, Senator, the interaction has improved, but is it still a concern. The answer is no and yes, and just to add to what Admiral Brown said, we also, few ports in the Nation are directly aligned with and contiguous to a downtown metro-

politan area. We have now two strategic centers that are within a stone's throw of one of our large container ports. So we are unique.

Senator WYDEN. The conference bill is going to mandate that every port have a comprehensive security plan. My understanding is that you all do not have one of those today, but that you will support this requirement in the conference legislation. Is that right?

Mr. DINSMORE. That is correct.

Senator WYDEN. Very good, gentlemen. Anybody want to add anything further? We have gone a little bit over on this panel. We appreciate all of you and the good service that you perform. We will excuse you at this time.

Senator WYDEN. Gentlemen, thank you. I am just going to have to be tyrannical in terms of insisting on the five-minute element. I want my colleagues to be able to lead off with their questions, and we will make your remarks as part of the record.

If you would just summarize, Tim Farrell, to begin with. Welcome.

**STATEMENT OF TIMOTHY FARRELL, DEPUTY EXECUTIVE DIRECTOR, PORT OF TACOMA**

Mr. FARRELL. Okay. Thank you. Thank you, Senator Wyden, Senator Murray, Senator Cantwell, for being here and for offering us the opportunity to speak.

I am going to pick up, you know, you cut off Mic. I am going to pick up where he left off, since there are two of us, but I want to give you a little bit of background on the Port of Tacoma. The port sits on 5,000 acres 30 miles from here. We handle about 15 million tons of cargo each year valued at $22 billion, and that is the international portion. That is about 1.3 million containers last year, and on the domestic side, we handle about $3 billion worth of trade, mostly to Alaska. Some 75 percent of the consumer goods bound for Alaska from the lower 48 go through the Port of Tacoma. Geographically speaking, more than 70 percent of the containers go east, most by train to places like the Midwest and the northeastern part of the United States. So the port is certainly a national asset. All told, the port generates over 100,000 jobs in Washington State alone. The Port of Tacoma is also one of the United States Department of Transportation Maritime Administration agency's 13 strategic ports, and that designation is based on the fact that the port provides to nearby military installations.

Since September we have faced the challenge of enhancing our security while maintaining the efficient flow of cargo. This was not the first time we thought of that. The port had invested over a million dollars in the three years prior to September. The port maintains an armed, uniformed security force 24 hours a day, seven days a week.

One of the things I would like to do today is to recognize Congress and the Federal agencies that we work with every day for acknowledging the Government role in supply chain security. Supply chain security is indeed a defense issue. Ports are border crossings, and they do serve multiple inland locations. The Port of Tacoma is working on enhancements in partnership with the Government as we are doing with port security grants recently announced. The

$4.76 million jointly awarded to the ports of Seattle, Tacoma, and Everett will be used to assess our vulnerabilities and to harden our facilities for such things as fencing, lighting, gates and that sort of thing. The $93 million was a great first step. As you know, there are $700 million of requests for that money, so there is a good bit of work yet to be done.

As we improve security at home, obviously the next step is to push back the borders to the point of origin. The next step we feel is to assess vulnerabilities and assess security standards before the cargo reaches our shores. The ports of Seattle and Tacoma are working with 9 private sector partnerships and overseas ports and will be developing best practices for supply chain security including securing cargo at the port of origin and securing that the cargo stays on schedule and on route, and that there is no tampering with the cargo along the way of its distribution, which can be as far away as New England. This effort includes the Port of Tacoma and Port of Seattle contributing to Operation Safe Commerce, the principal objective of which is as its name implies a secure supply chain. Another objective is that there is minimal disruption of the supply chain and to raise enhancement of the supply lane along the way. As you are aware, the port authorities of New York and New Jersey and the Port of Los Angeles are also involved in Operation Safe Commerce. Operation Safe Commerce will be driven by proven and emerging standards and technologies. The standards and technologies will, one, ensure that the containers are securely loaded at the port of origin in secured containers, two, allow continual container monitoring throughout the voyage to the point of distribution in the United States, again ensuring that the cargo stays on route, on schedule and is not tampered with, and three, Operation Safe Commerce will supply a software system that ensures that all the suppliers in the secure supply chain will know the status of a container at any point from its loading to its distribution. Operation Safe Commerce will provide solutions to our security challenges while contributing to free flow of trade through U.S. ports. The program is completely consistent with U.S. Customs and CSI and C–TPAT that you have heard about today. In fact, what we are hoping is that the best practices that we are able to develop with these three load centers will be integrated into these programs. Operation Safe Commerce is a broad-ranging program. It will be supported by many of the existing efforts that are already under way, including those to develop cargo tracking technology and smart boxes. Coordinator of these various efforts under Operation Safe Commerce will be one of the deliverables of the program.

I am going to leave off at that point, because I think it is valuable—you have heard from me, and you have heard from Mic. I think it is valuable that you have the opportunity to ask as many questions as you can. Thank you very much.

Senator WYDEN. Very good. Thank you.

[The prepared statement of Mr. Farrell follows:]

PREPARED STATEMENT OF TIMOTHY FARRELL, DEPUTY EXECUTIVE DIRECTOR, PORT OF TACOMA

Good afternoon Senator Wyden, Senator Murray and Senator Cantwell. My name is Tim Farrell, Deputy Executive Director for the Port of Tacoma. I appreciate the

opportunity you have given me today to discuss some possible positive solutions to the challenge of securing our international trade routes from disruption by terrorism.

Let me first put my comments about maritime security into context by describing our business. Each year, the Port of Tacoma handles more than 15 million tons of cargo, amounting to more than $22 billion in international trade—the vast majority with Asia. The Port of Tacoma moved more than 1.3 million containers across its docks in 2001 and, when combined with the Port of Seattle, Puget Sound represents the nation's third largest intermodal gateway. More than 70 percent of the containerized imports that cross our docks are loaded onto trains and shipped to consumers throughout the Midwest and East Coast.

Additionally, the Port of Tacoma handles $3 billion worth of trade as the Gateway to Alaska, with more than 75 percent of all consumer goods bound for Alaska transported through Tacoma on CSX and TOTE ships. All of this activity contributes to more than 100,000 family wage jobs for the citizens of Washington state.

Another important distinction Tacoma has is serving as one of the U.S. Department of Transportation Maritime Administration's 13 national "strategic ports"—a designation based on the military support capabilities the Port of Tacoma provides to Fort Lewis.

Whether we are importing shoes from Korea, exporting Washington and Oregon agricultural products to China or supporting U.S. military load-outs from Fort Lewis, the fast and efficient flow of freight through our Port is not only a key regional concern, but also a critical national interest.

In the days since September 11th, we have been faced with the challenge of accelerating security improvements while maintaining the efficient flow of cargo. This has been one of my key responsibilities as the Port's Deputy Executive Director. We have long recognized that, due to our key position as one of the nation's largest container ports, security must be a top priority. To that end, the Port of Tacoma invested more than $1 million in facility security enhancements and related security upgrades prior to the terrorist attacks in New York.

This is in addition to ongoing operating expense associated with the Port's proprietary, non-commissioned—but armed—security force of uniformed officers. In 1999, the Port installed an access control system for all facilities. A database of more than 1,500 cardholders includes members of the longshore workforce, Port employees, terminal operators and stevedore employees.

I would like to thank Congress and other governmental agencies for recognizing the federal role in port and supply chain security and their funding assistance that allows us to continue the process of security improvement. The $4.76 million jointly awarded by the Transportation Security Administration to the Ports of Tacoma, Seattle and Everett will be used to assess our vulnerabilities and harden our facilities. The grant funding of $92.3 million was a tremendous first step, but because seaports are, quite literally, the economic borders of our nation, we believe that more must be done. The Ports of Puget Sound, in fact, were among hundreds of ports and maritime organizations nationwide that submitted requests that totaled nearly $700 million.

As we strengthen security at home, the next logical step is to "push back" our economic borders overseas to the point of origin. We must assess vulnerabilities and establish perimeters of security long before cargo reaches our shores. This is an objective of Operation Safe Commerce. The program is designed to develop practical alternatives to traditional security measures. As a key player in this program with the Port of Seattle, the Port of Tacoma is actively developing a solution that substantially increases the security of trans-Pacific containerized cargo, while not impeding the free flow of trade. As one of the nation's three largest load centers, the Ports of Tacoma and Seattle are working with the Ports of Los Angeles and Long Beach and the Ports of New York and New Jersey to establish procedures and technologies to determine "best practices" in supply chain security.

The objective of Operation Safe Commerce is to secure intermodal trade corridors across the Pacific Rim. The program brings ACCOUNTABILITY for cargo security up and down the entire supply chain from the point of loading—whether it's in China, Japan or Korea—through the Puget Sound load centers and by rail on to points of distribution, such as Chicago or New York.

Operation Safe Commerce is a progressive initiative that will be driven by both proven and emerging technologies that will:

- Ensure that containers are securely loaded at the point of product origin and provide 100 percent verification of container contents.

- Employ technology that will be placed in or on the container, continually monitoring container status throughout the voyage overseas to the point of distribution here in the United States.
- Use advanced cargo tracking technology to ensure that federal agencies, shippers, shipping lines and others know the status of a container at any point from loading to distribution.

Senators Wyden, Murray and Cantwell, we believe Operation Safe Commerce is a logical solution to a pressing security challenge. Moreover, it is a solution that will contribute to the efficient flow of trade through U.S. Ports. As you know, the security of the logistics chain is an element of national security, and we appreciate your efforts to bring federal funding to the implementation of these programs.

The major load centers of the nation are not alone in their request for federal funding to extend our economic borders to the point of origin. U.S. Customs has relied on an automated system to collect information on imports that is becoming inadequate and antiquated. We support the funding and maintaining of U.S. Customs' Automated Commercial Environment (ACE). Without this system, imported cargo clearance must be completed manually on paper. The current Automated Commercial System (ACS), to be replaced by ACE, now processes approximately $1 trillion in imported-goods entries each year. ACS is currently operating at a capacity well beyond its design specifications. Without the ACE upgrade, the system is headed for a serious failure, especially with increasing volumes of cargo.

I would also like to take this opportunity to comment on the maritime security authorization bill (S. 1214, H.R. 3983) that originated in your Committee and is currently before a House-Senate conference committee. We appreciate the willingness this Committee has shown to listen to the views of the overall port industry as expressed by the American Association of Port Authorities (AAPA). The Port of Tacoma is working with other large ports on some additional thoughts on conference issues, which we will be sharing with you soon.

One conference issue that our representatives in Washington have already discussed with you is our concern about the diversion of cargo to Canada, especially the diversion of cargo from Puget Sound ports to the Port of Vancouver, British Columbia. We are losing more and more cargo to Vancouver, due in part to federal policies like the U.S. harbor maintenance tax. We are concerned that this maritime security authorization bill might impose burdensome security regimes and fees on cargo transiting U.S. ports that are not imposed at Canadian ports. That would divert even more cargo to Canada, which would not only hurt the Ports of Puget Sound and the U.S. economy, but also undermine the security goals of this legislation.

We are especially concerned about the discussion of a security fee on waterborne cargo. Taxes and fees on cargo tend to distort trade flows by diverting cargo to ports and modes of transportation where the fee is not imposed. They also hurt the competitiveness of U.S. exports. Maritime security is a national security issue; therefore, its costs should be borne by the U.S. Treasury (As a part of the U.S. Treasury, U.S. Customs ranks among the largest revenue source for the federal government).

If a security fee is imposed in this bill, we urge you to craft it very carefully so that it does not cause cargo diversion to Canada—even for a short period. Once cargo is diverted to new routes, it may never come back.

On behalf of the Port of Tacoma and the citizens of Pierce County, I thank you for this opportunity to discuss maritime security today.

Senator WYDEN. Mr. Yap, I join Senator Murray in the welcome that she gave you earlier.

## STATEMENT OF ROBERT YAP, EXECUTIVE VICE-PRESIDENT, PSA CORPORATION

Mr. YAP. Thank you. Senator Wyden, Senator Murray and Senator Cantwell, my name is Robert Yap, and I am the executive vice-president for information technology for PSA. Thank you, indeed, for the opportunity to testify before this Committee today. It is an honor to be here.

Let me by way of introduction introduce the company that I represent this afternoon. PSA operates the world's largest hub at our terminals in Singapore. Our Singapore terminals recorded 1.44 million TEUs in May 2002, and we expect to handle 17 million TEUs

for this year. Together with our overseas terminals, PSA's throughput grew by 24 percent over the past 5 months.

We provide every shipper an unrivaled choice of 250 shipping lines with connections to over 600 ports in 123 countries. We have daily sailings to every major port in the world with an average two daily sailings to U.S. ports, including Seattle and Tacoma. Our partnership with these two ports is important to PSA, and I am honored to be here with my two partners this afternoon as well. We operate technologically advanced container terminals with the comprehensive infrastructure that allows the accurate and timely handling of vessels and containers. This infrastructure includes 37 berths or terminals handling an average of 60 vessels a day, 45,000 Twenty-foot Equivalent Units of containers and in excess of 100,000 TEUs held within PSA's yards on any given day.

Outside of Singapore, PSA also manages 30 ports in 8 countries around the world included Brunei, China, India, Italy, Korea and Portugal. The recent acquisition of two large ports in Belgium, namely Antwerp and Zeebrugge, has given PSA a substantial presence in Europe for the U.S. East Coast trade. Collectively, PSA manages 24 million TEUs amounting to 10 percent of the world's container throughput.

PSA deploys extensive information technology to manage its 24 million containers yearly. PSA has won numerous awards for IT innovation in the ports and logistics industry in the U.S., the most recent being the Smithsonian award for our terminal operating system, and our part man. PSA's comprehensive technology infrastructure in Singapore rides on a 6,000-km fiber optic network, and real time transfer of information between 500 cranes and 700 terminal trucks within the terminals, and ultimately onto our Port Community System called PORTNET®. PORTNET® facilitates the business-to-business transactions among all players in the port and shipping community in a highly secured Internet environment. We deploy multi-tier firewall and data encryption technology, to secure our data communication networks spanning both private and public access.

The Port Community System brings all parties in the port and shipping community to electronically transact through a common Web-based portal. This serves as a common interface and a central system for all parties to obtain and transmit information.

Steamship lines, freight forwarders, port authorities, government agencies, trucking and rail companies input container and shipping information into this system. The Port Community System subsequently connects to the terminal operator's system, enabling the tracking of containers from factory to terminal, onto ships, to the next port of call, and ultimately to its final designation.

For example, in Singapore, PORTNET® electronically captures information of every container entering, leaving or passing through the port. It also captures information related to bulk or loose cargo. The PORTNET® system has been operating in Singapore since 1984 and currently has a foot- print of 7,000 users, generating around 70 million transactions a year. By far this is the world's largest port community system. Besides Singapore, PORTNET® is operational in other ports of the world.

An operating and proven port community system coupled with an established container tracking infrastructure provides that clear information trail. This trail begins with the input of container information into the system, fixing of the electronic seal on the container, enabling real time tracking of containers globally.

Subsequently, the information trail can be expanded to include who owns the cargo, who packed the container, which tracking company handled the container, and the duration from point to point. The information can be cross-referenced with related systems and databases forming an extensive source of information for the U.S.-led Container Security Initiative.

In effect, the container's movements will be tracked from source to designation physically, with hand over between multiple parties, well documented and audited.

As more port community systems are established globally, they collectively and invariably form a container security backbone.

The farsighted decision by the Port of Seattle to implement PORTNET® in Seattle has essentially provided a platform and a unique opportunity for the Port of Seattle to take the lead in the implementation of a PCS in the U.S. This, in essence, could potentially become the U.S. container security information management layer.

Once again, thank you for the opportunity to share my thoughts with you on this critically important issue. I look forward to answering any questions you have.

[The prepared statement of Mr. Yap follows:]

PREPARED STATEMENT OF ROBERT YAP, EXECUTIVE VICE-PRESIDENT, PSA CORPORATION

Senator Wyden,
Chairman Murray,
Senator Cantwell,

Thank you for the opportunity to testify before this Committee today. It is an honour to be here.

PSA operates the world's largest container transhipment hub at our terminals in Singapore. Our Singapore terminals recorded 1.44 million TEUs in May 2002, and we expect to handle 17 million TEUs for this year. Together with our overseas terminals, PSA's throughput grew by 24-percent year-on-year over the past 5 months.

We provide every shipper an unrivalled choice of 250 shipping lines with connections to over 600 ports in 123 countries. We have daily sailings to every major port in the world, with an average 2 daily sailings to US ports, including Seattle and Tacoma. Our partnership with these two ports is important to PSA and I am honoured to be here with my two partners this afternoon.

We operate the most technogically advanced container terminals, with a comprehensive infrastructure that allows the accurate and timely handling of vessels and containers. This infrastructure includes 37 berths, handling an average of 60 vessels, 45,000 Twenty-foot Equivalent Units (TEUs) of containers and in excess of 100,000 TEUs held within PSA's yards, on any given day.

Outside of Singapore, PSA also manages 13 ports in 8 countries around the world. These include Brunei, China, India, Italy, Korea and Portugal. The recent acquisition of 2 large ports in Belgium, namely Antwerp and Zeebrugge which entails 22 terminals, has given PSA a substantial presence in Europe for the US East Coast trade. Collectively, PSA manages 24 million TEUs amounting to 10-percent of the world's container throughput.

PSA deploys extensive Information Technology to manage this 24 million containers. PSA has won numerous awards and accolades for IT innovation in the Ports and Logistics industry. The most recent being the Smithsonian award for our terminal operating system and the Computerworld Honors Laureate for PORTNET®.

PSA's comprehensive technology infrastructure in Singapore rides on a 6,000 km fibre optic network, enabling the real time transfer of information between 500

cranes and 700 terminal trucks within the terminals, and ultimately on to our Port Community System called PORTNET®.

PORTNET® facilitates the business-to-business transactions amongst all players in the port and shipping community in a highly-secured Internet environment. We deploy multi-tier firewall and data encryption technology to secure our data communication networks spanning both private and public access.

The Port Community System brings all parties in the port and shipping community to electronically transact through a common web-based portal. This serves as a common interface and a central system for all parties to obtain and transmit information.

Steamship lines, freight forwarders, port authorities, government agencies, trucking and rail companies input container and shipping information into this system. The Port Community System subsequently connects to the terminal operator's system—enabling the tracking of containers from **factory to terminal, onto ships, to the next port of call and ultimately to its final destination.**

For example in Singapore, PORTNET® electronically captures information of every container entering, leaving or passing through the port. It also captures information related to bulk or loose cargo. The PORTNET® system has been operating in Singapore since 1984 and currently has a foot-print 7,000 users, generating around 70 million transactions per year. By far this is the world's largest Port Community System. Besides Singapore, PORTNET® is operational in other parts of the world.

An operational and proven Port Community System coupled with an established container tracking infrastructure provides a clear information trail. This trail begins with the input of container information into the system, fixing of the electronic seal on the container, enabling real time tracking of the container globally.

Subsequently the information trail can be expanded to include, who owns cargo, who packed the container, which trucking company handled the container, and the duration from point to point. The information can be cross referenced with related systems and databases forming an extensive source of information for the US led container security initiative.

In effect, the container's movements will be tracked from source to destination physically, with hand-over between multiple parties well documented and audited.

As more Port Community Systems are established globally, they collectively and invariably form a **container security backbone.**

The farsighted decision by the Port of Seattle to implement PORTNET® in Seattle has essentially provided a platform and a unique opportunity for the Port of Seattle to take the lead in the implementation of a PCS in the USA. This, in essence, could potentially become the US container security information management layer.

Once again, thank you for the opportunity to share my thoughts with you on this critically important issue. I look forward to answering any questions you may have.

Senator WYDEN. Very good statement, Mr. Yap, and we thank you. Captain Marcus?

## STATEMENT OF CAPTAIN DON MARCUS, VICE-PRESIDENT, PACIFIC INTERNATIONAL ORGANIZATION OF MASTERS, MATES AND PILOTS

Mr. MARCUS. Good afternoon, Senators Murray, Wyden and Cantwell. I am testifying on behalf of the Puget Sound Ports Council of the Maritime Trades Department of the AFL–CIO. On a national level, the organizations that make up the Maritime Trades Department represent the vast majority of mariners operating United States flagged vessels in the international and domestic trade.

It is gratifying and only right that seafaring labor has a place at this forum. We thank you and your staffs.

Our perspective is somewhat different as seagoing labor protecting our trade routes starts overseas and on the high seas.

Since ancient times every great trading nation has thrived only to the extent that it has been able to maintain and protect its ocean trade routes. 9–11 has demonstrated that commerce can be

brought to a stop. What we do now to reduce our vulnerabilities will have lasting impacts.

The overwhelming proportion of our imports and exports are carried by sea. Sadly, there are now only 102 U.S. flag vessels engaged in international trade, a pitiful 2.6 percent of our foreign commerce. It is difficult to think of any great trading nation that allowed itself to become as dependent on foreign shipping as the United States currently is. Our economic and military security, not to mention our port security, are now largely at the mercy of foreign flag ocean carriers, foreign shippers and foreign seafarers.

Billions of dollars are being made transporting goods and materials to and from our shores. That immense power must not inhibit the changes that are necessary to protect our trade routes.

Worse than the decline in the numbers of U.S. flag vessels is the loss of skilled mariners. Experienced seafarers are abandoning their careers in record numbers. Young Americans are not committing themselves to an industry that has no apparent future.

We must not forget the lessons we learned in the Persian Gulf War, Vietnam, Korea and two world wars. The next terrorist attack will likely involve our brothers and sisters working on the high seas, in our harbors or on our docks. We will be the first responders. If our troops need supplies overseas or if foreign cartels decide to strangle or blackmail our economy, it will not be to the global village that our Nation will turn to for help. It will be to our citizens. We will be called upon to make the sacrifice. Without some forward thinking and action, we will not be able to rise to the task.

9–11 has not changed the historical proof that a viable United States flag merchant marine plus the United States Navy are what is needed to secure our trade routes. We must establish a vigorous national maritime policy. Consider the following steps to increase our maritime security. At this time there are 47 ships in our Maritime Security Program. We urge you to expand and extend this program. A minimum of 100 militarily useful vessels, and a 20-year program are needed to maintain the U.S. flag fleet in international trade. Maritime tax reform is essential to encourage investment in United States flag shipping.

The proposed Merchant Marine Cost Parity Act, H.R. 3262, could provide the sort of tax and investment incentives enjoyed by our foreign flag competitors. We must continue to support the Jones Act and cargo preference laws. Our domestic trade must remain in United States control. Our cargo preference laws must be rigidly enforced. Title XI loan guarantees must remain available if our obsolescent domestic fleet is to be rebuilt. Investment in domestic shipping needs to be fostered, to improve our national transportation network, to protect our environment and to sustain our seagoing labor pool.

Legislation such as the United States Cruise Vessel Act, S.127, should be enacted to ensure that some of the billions of dollars going virtually tax-free to foreign cruise ship owners gets redirected into the United States economy and tax base. The palatial foreign flag cruise ships that we see in U.S. harbors employ hundreds of low wage, poorly documented Third World seamen. These floating cash cows enhance neither our maritime capability nor our port security.

The security of our trade routes is similarly not enhanced by certain misguided actions of the U.S. Customs Service and the U.S. Coast Guard. Last year the Customs Service extended the scope of the already disadvantageous 50 percent ad valorem duty on repairs to U.S. vessels. Customs regulations now subject maintenance and repairs performed by American crew members while underway on the high seas to the ad valorem duty. Owners of foreign flag vessels pay no such duty. This is absurd and must be stopped.

The USCG subjects American mariners engaged in foreign trade to the latest requirements of the International Convention on Standards of Training, Certification and Watchkeeping, known as STCW 95. At the same time, the U.S. Coast Guard has delayed implementing these requirements for foreign seafarers. Foreign seamen are given a free pass into the United States disregarding one of the most effective means of differentiating between bona fide, properly trained seafarers and possible impostors, or at best, inadequately trained seamen. The U.S. Coast Guard must be instructed to vigorously enforce these standards aboard all flag of convenience vessels entering U.S. ports.

U.S. citizen mariners are among the most highly regulated workers in this country. We do not expect that to change. However, since 9–11, there has been an irrational and unwarranted urgency to regulate U.S. citizen shore-side workers, yet no urgency to extend equivalent requirements to foreign seafarers. For example, while American seamen can be legally arrested, detained, fined, and deported by Canadian authorities upon evidence of past misdemeanor convictions, foreign seamen enter U.S. ports without effective scrutiny.

American maritime workers and United States flag employers must not be burdened with more regulations, while the rest of the industry carries on with business as usual. This can only drive U.S. flag ship owners away from our flag and U.S. citizen mariners out of the industry.

A New York Times article noted that the Al Queda owned a fleet of merchant vessels hidden under various flags of convenience. Every day, flag of convenience vessels whose owners are virtually anonymous enter our ports.

Starting at foreign points of origin, shippers and ocean carriers need to be examined to ascertain responsible parties. Cargo profiles must be established to identify suspicious shipments. Vessel ownership, the identity of shippers and cargo manifest information must be transparent. There is absolutely no legitimate reason not to require all parties in the transportation chain to be gradually certified in order to continue doing business in this country.

We in the maritime trades are calling for background checks and certification for the shippers and ocean carriers who bring their business into our ports. We support the proposed Port Threat and Security Act, S. 1587, and the Ship, Seafarer and Container Security Act, which reflect these interests.

In summary, maritime security demands a viable United States merchant marine. Maritime security demands accountability for all participants in the transportation chain. In order to protect our trade routes, we must have a United States flag, citizen-crewed merchant fleet capable of carrying a reasonable proportion of U.S.

foreign trade. Self-reliance is the best guarantee of economic and national independence.

Thank you for your attention, and I look forward to your questions.

Senator WYDEN. Thank you. Very helpful.

[The prepared statement of Mr. Marcus follows:]

STATEMENT BY CAPTAIN DON MARCUS, VICE-PRESIDENT, PACIFIC INTERNATIONAL ORGANIZATION OF MASTERS, MATES AND PILOTS

Good afternoon Senator Wyden and Members of the Subcommittee. I am testifying on behalf of the Puget Sound Ports Council of the Maritime Trades Department, AFL–CIO. On a national level, the organizations that make up the Maritime Trades Department represent the vast majority of mariners operating United States flag merchant vessels in international and domestic trade.

It is gratifying and only right that seafaring labor has a place at this forum. We thank you and your staff.

Every great trading nation since ancient times has thrived only to the extent that it has been able to maintain and protect its maritime trade routes. 9–11 has demonstrated that commerce can be brought to a halt. What we do now to reduce our vulnerabilities will have lasting repercussions.

The overwhelming proportion of our imports and exports are carried by sea. Sadly, there are now only 102 United States flag vessels engaged in international trade. These vessels carry a pitiful 2.6-percent of our foreign commerce. It is difficult to think of any great trading nation that allowed itself to become as dependent on foreign shipping as the United States currently is. Our economic and military security, not to mention our port security, are now largely at the mercy of foreign-flag ocean carriers, foreign shippers and foreign seafarers.

Billions of dollars are being made transporting goods and materials to and from our shores under foreign flags. The immense power of this money must not inhibit the changes that are necessary to protect our trade routes.

Worse than the decline in the numbers of United States flag vessels is the loss of skilled mariners. Experienced seafarers are abandoning their careers in record numbers. Young Americans are not committing themselves to an industry that has no apparent future.

We must not forget the lessons of the Persian Gulf War, Viet Nam, Korea and two world wars. The next terrorist attack will likely involve our brothers and sisters working on the high seas, in our harbors or on our docks. WE will be the first responders. If our troops need supplies overseas or if foreign cartels decide to strangle or blackmail our economy, it won't be to the Global Village that our nation will turn to for help, it will be to our citizens. We will be called upon to make the sacrifice. Without some forward thinking and action, we will not be able to rise to the task.

9–11 hasn't changed the historical proof that a viable United States flag merchant marine plus the United States Navy are the essential requirements to secure our trade routes. We must establish a vigorous, national maritime policy. Consider the following steps to increase our maritime security:

- At this time there are 47 ships in our Maritime Security Program. We urge you to expand and extend this program. A minimum of one hundred militarily useful vessels and a twenty-year program are needed to sustain a U.S.-flag fleet in international trade.
- Maritime tax reform is essential to encourage investment in United States-flag shipping. The proposed Merchant Marine Cost Parity Act, H.R. 3262 introduced by Representatives Oberstar and Young could provide the sort of tax and investment incentives enjoyed by our foreign-flag competitors. This bill would go a long way to reduce the high tax, insurance and inspection costs that disadvantage United States ship owners.
- We must continue to support of the Jones Act and Cargo Preference Laws. Our domestic trade must remain in United States control. Our cargo preference laws should be rigidly enforced. The current leakage of military cargoes to foreign-flag carriers needs to be stopped.
- Title XI Loan Guarantees must remain available if our obsolescent domestic fleet is to be rebuilt. Investment in domestic shipping needs to be fostered, to improve our national transportation network, protect our environment and to sustain our seagoing labor pool.
- Legislation such as the United States Cruise Vessel Act, S. 127 should be enacted to ensure that some of the billions of dollars going virtually tax-free to

foreign cruise ship owners gets re-directed into the U.S. economy and tax base. The palatial foreign-flag cruise ships that we see in U.S. harbors employ hundreds of low wage, poorly documented third-world seamen. These floating cash cows enhance neither our maritime capability nor our port security.

The security of our trade routes is similarly not enhanced by certain misguided actions the United States Customs Service and United States Coast Guard:

- Last year the Customs Service extended the scope of the already disadvantageous 50-percent ad valorem duty on repairs to U.S. vessels. Customs regulations now subject maintenance and repairs performed by American crew members while underway on the high seas to the ad valorem duty. Owners of foreign-flag vessels pay no such duty. This is absurd and must be stopped.
- The USCG subjects American mariners engaged in foreign trade to the latest requirements of the International Convention on Standards of Training, Certification and Watchkeeping (known as STCW 95). At the same time, the U.S. Coast Guard has delayed implementing these requirements for foreign seafarers. Foreign seamen are given a free pass into the United States disregarding one of the most effective means of differentiating between bona fide, properly trained seafarers and possible imposters or, at best, inadequately trained seamen. The U.S. Coast Guard must be instructed to vigorously enforce these standards aboard all flag of convenience vessels entering U.S. ports.
- United States citizen mariners are among the most highly regulated workers in this country. We don't expect that to change. However, since 9–11 there has been an irrational and unwarranted urgency to regulate U.S.-citizen shore-side workers, yet no urgency to extend equivalent requirements to foreign seafarers. For example, while American seamen can be legally arrested, detained, fined and deported by Canadian authorities upon evidence of past misdemeanor convictions, foreign seamen enter U.S. ports without effective scrutiny.

American maritime workers and United States flag employers must not be burdened with more regulations, while the rest of the industry carries on with business as usual. This can only drive U.S.-flag ship owners away from our flag and U.S. citizen mariners out of the industry.

A New York Times article (October 8, 2001) noted that the Al-Qaeda owned a fleet of merchant vessels hidden under various flags of convenience. Every day, flag of convenience vessels, whose owners are virtually anonymous, enter our ports.

- Starting at foreign POINTS of origin, shippers and ocean carriers need to be examined to ascertain responsible parties. Cargo profiles must be established to identify suspicious shipments. Vessel ownership, the identity of shippers, and cargo manifest information must be transparent. There is absolutely no legitimate reason not to require all parties in the transportation chain to be gradually certified in order to continue doing business in this country.
- We in the Maritime Trades are calling for background checks and certification for the shippers and ocean carriers who bring their business into our ports. We support the proposed Port Threat and Security Act, S. 1587 and the Ship, Seafarer and Container Security Act S. 2329 which reflect these interests.

In summary:

- Maritime security demands a viable United States merchant marine.
- Maritime Security demands accountability for all participants in the transportation chain.
- In order to protect our trade routes we must have a United States-flag, citizen-crewed merchant fleet capable of carrying a reasonable proportion of U.S. foreign trade.
- Self-reliance is the best guarantee of economic and national independence.

Thank you for your attention.

Senator WYDEN. Mr. Bates?

## STATEMENT OF DEL BATES, VICE-PRESIDENT, LOCAL 19, INTERNATIONAL LONGSHORE AND WAREHOUSE UNION

Mr. BATES. Yes, I want to thank you, Senator Wyden, Senator Cantwell and Senator Murray for having me testify today.

As vice-president of the International Longshore and Warehouse Union, Local 19, representing working men and women in the Port

of Seattle, I am pleased to submit these comments regarding the security of our port.

The members of the ILWU are committed to making our port and surrounding areas safe, and secure and free of criminal or terrorist activities. Just as important, we are absolutely committed to insuring the security of our work force as well as the community where we live and interact. This is especially so since ILWU members face direct risk to their personal safety and livelihood from such criminal terrorist acts simply by virtue of the jobs we do and the areas where we work.

Following the horrendous terrorist attacks of September 11, our port went on immediate security alert. The Longshoreman's Union has held joint meetings with the Coast Guard and all of our maritime employers to discuss the threats we now face and the actions we must now take. The U.S. Coast Guard has basically been our waterside enforcement agency within the Federal Government.

To be perfectly clear, understand that land side enforcement is a different matter altogether. In Seattle, as in other major American ports, including those with ILWU jurisdiction, land side security enforcement has been a function of the local port and terminal operators.

Land side security issues, container security seals, like luggage on airplanes, the containers on vessels and in port facilities need to be subjected to security screening to protect the U.S. seaports and international maritime commerce. Obviously, it is both impractical and cost prohibitive to inspect every one of the tens of thousands of containers that flow in and out of our ports each day. Proposed legislation should at least mandate that port workers who receive containers inspect the integrity of the outside seal on each container. Seal inspection must be done to ensure that the seal number matches up with the consignee who was the last person who sealed that container up and is responsible for the cargo therein. To ensure port security, this is one of the primary actions that must be undertaken. This act must mandate that the integrity of the seals be checked and rechecked against terminal documentation to ensure the origins of that cargo.

A broken seal would alert port security that the container has been tampered with, and that it needs to be carefully inspected before entering a port facility or being placed on a vessel, and it should be immediately earmarked to Customs for inspection. A systematic check of container seals provides authorities with a record as to the parties responsible for placing the seal on any container that may be the means of a terrorist act.

Empty containers, one of the most overlooked of potential security risks at the terminals, ships and port infrastructure is the proper handling of empty containers. On any given day as much as 40 percent of cargo delivered into any facility is comprised of empty containers. A physical inspection of these containers is vital for a number of reasons for terminal safety. Knowing that in almost all port facilities, empty containers are very rarely inspected, the potential for placement of some kind of explosive device is something that must be considered and planned for.

Vessel Safety or remote site endangerment, the concept where an uninspected empty container containing an explosive device would

be loaded onto a vessel for detonation. In many ports throughout the world, the inspection of empty containers is a requirement, for exactly many of the reasons that were outlined. What would happen if a terrorist cell in a foreign country were to take an empty container and place an explosive device inside and load it on a ship for detonation elsewhere? For years, inspection of empty containers was regularly done in America's largest seaports. However, this procedure was abandoned years ago. Once again, if we truly are desirous of creating safe and secure seaports, then the return to these inspections is a must. Thank you.

Senator WYDEN. Thank you very much.

[The prepared statement of Mr. Bates follows:]

PREPARED STATEMENT OF DEL BATES, VICE-PRESIDENT, LOCAL 19, INTERNATIONAL LONGSHORE AND WAREHOUSE UNION

As Vice President of the International Longshore and Warehouse Union, Local #19, representing working men and women in the Port of Seattle, I am pleased to submit these comments regarding the security of our Port.

The members of the ILWU are committed to making our port and surrounding areas safe, secure and free of criminal or terrorist activities. Just as important, we are absolutely committed to insulating the security of our workforce as well as the community where we live and interact. This is especially so since ILWU members face direct risk to their personal safety and livelihood from such criminal and terrorist acts simply by virtue of the jobs we do and the areas where we work.

Following the horrendous terrorist attacks of September 11, our port went on immediate security alert. The Longshore Union has held joint meetings with the Coast Guard and all of our maritime employers to discuss the threats we now face and the actions we must take. The Port and Maritime Security Act (S.1214) initially focused on criminal activities rather than national security and terrorism. The need to secure our port from the threats of international terrorism now is at the top of our security agenda. There are substantial areas of omission in S.1214 that need to be rectified to truly enhance our nation's seaport security. The U.S. Coast Guard has basically been a waterside enforcement agency within the federal government. To be perfectly clear, understand that landside enforcement is a different matter altogether. In Seattle, as in other major American ports, including those with ILWU jurisdiction, landside security enforcement has been a function of the local port and terminal operators.

In the goal of maintaining secure seaports, to treat a longshore worker as security risks is both contrary to the facts and detrimental to the goal. Longshore workers are not the problem but rather are a critical part of the solution for keeping our ports safe and secure from crime and terrorism. It is the well-established longshore workforce that knows how things work best in the ports and, perhaps most importantly, knows who belongs where in the marine terminals. It is ILWU members who are best able to and often detect and report suspicious and unusual activity in the ports. The government should, therefore, enlist us as partners rather than as suspects in the effort to secure our ports.

The ILWU opposes background checks on our workers. During the investigation of the Interagency Commission on Seaport Security (the Graham Commission) the ILWU challenged the Commission to prove their assertion that internal conspiracies are a problem at many of our nation's ports. They were asked for an example of an internal conspiracy to commit crimes involving ILWU longshore workers. They could not produce one example of ILWU workers at our nation's ports involved in criminal conspiracies. Not one. In fact, the only involvement our members have with serious criminal activity is reporting to authorities suspicious activities and cargo. In testimony before the Senate Commerce, Science, and Transportation Committee, the ILWU pointed out that the actions of one longshore worker at the Port of Tacoma led to the largest cocaine seizure in that Port's history. In times of war, the ILWU members have delivered on their promise to load military cargo in the safest, most efficient way possible.

It is also critical that the government in response the new terrorism threats against our country, does not set policy which harms the productivity of our commercial seaports. Excessive or imprudent regulations that fail to account for the true realities of port operations will only result in further damage to the national and world economies. We must not, through rash government regulations, accom-

plish the very result our enemies seek and we are trying to avoid—the disabling of waterfront commerce.

Accompanying this statement is a detailed proposal from the ILWU International Officers designed to pinpoint critical security—sensitive areas with specific delineations between landslide and waterside operations. The proposals are designed to increase and improve port security protections in an economically feasible way.

## WATERSIDE SECURITY ISSUES

***MATCH PERSONNEL WITH PROVIDED DOCUMENTS—**

Legislation should require crew and passenger lists including names, addresses, passports, and mariner documents be matched up in person with the documents submitted. When the Immigration Naturalization Service (INS) is given the documentation, they merely go through the documents without requiring the individual's presence to insure he or she is who the documents say they are.

***IMPLEMENTATION OF INTEGRATED SYSTEMS—**

Implementation of integrated systems allowing Customs to inspect and/or review manifests containing identification of shipper, port of origin, and cargo shipped prior to vessel entering American waters.

***ADVANCE SECURITY CLEARANCES OF VESSELS—**

The legislation should require advance security clearance requirements for all vessels, their owners, operators and crew before entering a U.S. port. Presently, these vessels operate under secrecy and without regulations by the scheme of flying the flag of a country (flag of convenience) that lacks any meaningful regulations and scrutiny. The London Times reported that the terrorist group Al Qaida operates flags of convenience vessels.

***CONTAINER SECURITY SEALS—**

Like luggage on airplanes, the containers on vessels and in port facilities need to be subjected to security screening to protect U.S. seaports and international maritime commerce. Obviously, it is both impractical and cost prohibitive to inspect every one of tens of thousands of containers that flow in and out of our ports each day. Proposed legislation should at least mandate that port workers who receive containers **inspect the integrity of the outside seal** on each container. Seal inspection must be done to insure that the seal number matches up with the consignee who was the last person who sealed that container up and is responsible for the cargo therein. To insure port security, this is one the "primary" actions that must be undertaken. *This act must mandate that the integrity of the seals be checked and rechecked against terminal documentation to insure the origins of that cargo.* A broken seal would alert the port facility that the container has been tampered with and that it needs to be carefully inspected before entering a facility or being placed on a vessel, and should be immediately earmarked to Customs for inspection. A systematic check of container seals provides authorities with a record as to the parties responsible for placing the seal on any container that may be the means of terrorist act.

***EMPTY CONTAINERS—**

One of the most overlooked of potential security risks to terminals, ships, and port infrastructure is the proper handling of empty containers. On any given day as much as forty percent of cargo delivered into any facility is comprised of empty containers. A physical inspection of these containers is vital for a number of reasons; 1) Terminal safety—knowing that in almost all port facilities empty containers are very rarely inspected, the potential for placement for some kind of explosive device is something that must be considered and planned for, 2) Vessel Safety or remote site endangerment—the concept where an uninspected empty container containing an explosive device would be loaded onto a vessel for detonation. In many ports throughout the world the inspection of empty containers is a requirement, for exactly many of reasons that were outlined! What would happen if a terrorist cell in a foreign country for example were to take an empty container, place an explosive device inside, then load it up and ship it for detonation elsewhere? For years, inspection of empty containers was regularly done in America's largest seaports; however this procedure was abandoned some years ago. Once again, if we truly are desirous of creating safe and secure seaports then the return to these inspections is a must.

***NON-INSPECTION OF TRUCKERS—**

The primary threat to American seaports is the ability of truckers gain access to dockside marine containers terminals with "carte blanche" accessibility. **THE MAJORITY OF ALL TRUCKERS ENTERING MARINE FACILITIES IN AMERICA'S LARGEST PORTS DO SO WITHOUT HAVING TO EXHIBIT ANY KIND OF IDENTIFICATION WHATSOEVER.** Prior to the terrorist attacks in New York and Washington D.C., there was no requirement for truckers to produce any identification upon entrance to marine terminal facilities. However, even following the attack, only two marine container facilities now demand I.D. upon entrance through marine terminal gates, but there is still no match-up of photo I.D. with the truckers themselves because they only have to produce the driver's license number for entrance. The truckers entering these marine facilities have virtually unobstructed access to the entire facility, enabling them to place anything, anywhere, at anytime.

***THE FAILURE TO PROVIDE SECURE CARGO HANDLING AREAS—**

In many ports throughout the world, the local workforces take the cargo (now in steel cargo shipping containers almost all the time) and place them in secured "holding" areas, many times located next to marine facility entrance gates, awaiting truckers who are allowed only in these secured areas to pick upon containers, usually on an appointment basis. This is an excellent concept that has resulted from years of experience realizing that he best way to secure your facility is only allow those on the terminal that have immediate business needs. They then realized that to allow trucker's unlimited "carte blanche" access to all areas of the facilities was a dramatic error as it compounded the problems of security and congestion. What followed was the establishment of secure "holding" for cargo retrieval.

***UTILIZATION OF EXISTING SECURITY PERSONNEL—**

Minimum manning standards and uniform training procedures must be adopted for the existing professional security personnel to meet the growing security needs of our ports.

The above outlined points are a collection of the most critical procedures that must take place if we are to safeguard our American seaports. We have worked within these ports every day for many years and our experience enables us the opportunity to share with you, some of the protocols and procedures in a marine environment.

I appreciate the opportunity to submit comments for the record on behalf of the International Longshore and Warehouse Union Local #19 and I am prepared to answer any questions. I look forward to the opportunity to work with you as we solve the problems of reviewing security issues so that commerce within our nation's seaports may continue uninterrupted in a manner prosperous, safe and secure for many years to come.

Thank you.

DEL BATES
*Vice President, ILWU Local #19*

Senator WYDEN. Let us go to Senator Murray for her questions.

Senator MURRAY. Thank you, Mr. Chairman. Thank all of you for excellent input as we explore where we need to go. As I mentioned earlier, Puget Sound, and these grants are supposed to work us towards some sort of regional solution. In looking at them so far, they have mostly been awarded for preliminary work and access systems. So we have a long ways to go before we get, and probably a lot of significant resources before we get to the solution.

Mr. Farrell, you have been working with local, state and government entities. Have they been willing partners in exploring innovative efforts to address seaport security?

Mr. FARRELL. We have, and first, let me start at the port level. You know that we worked very closely together with the ports of Seattle and the port of Everett, and that effort is based on the premise that you are only as secure as your neighbors are. The work that we have done with the U.S. Coast Guard in the establishment of the interim guidelines for the West Coast has been a

good example of working closely together in an agency that is focused on making sure whatever regulations or guidelines come into place are attainable, and that the industry has a chance to look at them before they have put in place, and on the side of customs, and these are the two major players that we deal with on the Federal level, the cooperation has been quite good as well.

We spent some time in D.C. and here on the local level talking to them to find out what with we can do to play a part in the CSI and the C–TPAT, and we feel that our involvement in Operation Safe Commerce is a successful program. So the cooperation has been, has been good to date on security issues.

Senator MURRAY. Thank you. Mr. Yap, our security is only as good as our information, and I am curious what sort of enforcement mechanisms you envision that could be put in place to give our Federal agencies comfort about what is reported to be in any foreign containers?

Mr. YAP. I can only speak from experience, what we do in Singapore, Senator Murray. More, what we do in Singapore, we have an extensive system. The information that we have contains purchase information, cargo manifests, shipper information, and everything else that goes together with the information.

My take on this is basically that the information management layer becomes a critical success factor when it comes in terms of actually attaching relevant information to the box, and that actually comes in two forms. One is actually the box that leaves a particular port, and one as it comes to the port itself. My take on this is that as we basically move towards container security issues, one of the key things is application and databases, and it is got to be put in place to actually capture information. That actually then allows cargo systems as you draw on that information specifically to look for data of concern.

Senator MURRAY. What do we do about countries that known terrorists operate in, like Malaysia?

Mr. YAP. My sense, Senator Murray, is a lot of waiting for clarity to come from the U.S. government pertaining to, I think this has been alluded earlier on by one of the earlier speakers in terms of our body of information and I think by and large we are still waiting for some kind of mandate, if you like, in terms of that kind of information to be made clear, in terms of what specifically are we looking for in terms of the information that would really tie on top of the container security issues.

Senator MURRAY. Well, one of the things that I think is important to understand is that this has to be economically feasible.

Mr. YAP. Absolutely.

Senator MURRAY. We have a plan we put together, and there have to be incentives for private businesses to get involved in this, and it seems to me that part of that is standards for all the players that we all know are usable and can be enforced, and if you could comment on that, Mr. Yap, I would appreciate it.

Mr. YAP. I think that a couple of players that should be involved is the shippers community. These will be the manufacturers, if basically today in terms of the added layer of security comes into play would involve shippers having to induce a kind of a payment to really look at technology today, that would tie on top of those boxes

that would be something that would have to be considered very seriously. We are waiting for clarity to come from the Container Security Initiative, whether it is sealed technology, whether it is information management on top of it, whether there is some kind of device that can be attached, proven concepts that are currently being conducted now.

I would also like to inform Senator Murray that at this point in time, PSA Singapore is involved in a proof of concept as such. This proof of concept involves electronic sealing system. In terms of what they are doing as a proof concept, we are participating at that level as well, and this is in combination together with funding at the Singapore Government, how to tie in very closely with the needs of U.S. insofar as CSI are required.

Senator MURRAY. Sounds like, and Mr. Farrell, maybe if you could comment on the willingness of our merchants and shippers in ports to share information that they have not been so willing to share in the past. Is that going to be problem?

Mr. FARRELL. Yes, it has been a problem in the past, because trade information obviously is commercially valuable to the various entities that are involved in trade. We have seen more of a willingness of our customers and our partners to become involved in these efforts, and we have not gotten to the point where we said, okay, we need this piece of information and this and this and this, and I think when we get to that point, when these projects get to this point, that is when we are going to find out just how willing these entities are, and I think Mr. Yap makes a very good point, and that is what are we exactly going to require, and if we can get, in the way that the Coast Guard has done with it, in terms of making sure that the industry is involved, I think operational carriers will hopefully get with us on that.

Senator MURRAY. Just one final question. I would like to ask Mr. Bates, in our developing comprehensive solutions, have you been involved in the collaborative efforts in putting some of these issues forward?

Mr. BATES. In putting which forward?

Senator MURRAY. Any of the comprehensive solutions that we are looking at? If the port grants that have been funded or the comprehensive——

Mr. BATES. No, we have not been in the Port of Seattle implementing these plans. We now inspect some of the containers that are, or the containers that are coming into the port, but we have not been involved in the, in the facility, itself, as far as what we are going to do with the facility. If that answers that.

Senator MURRAY. It does. Captain Marcus?

Mr. MARCUS. Yes, I would concur with that. Basically we get directives, our people aboard ship, for example, the 96 hour notice requirement. As far as input into the process, I am very happy to say that we are getting more of an opportunity to come to the table. For example, we are here today, but it has been a difficult road to get input up to this point.

Senator MURRAY. Thank you very much. Thank you, Mr. Chairman.

Senator WYDEN. Senator Cantwell?

Senator CANTWELL. Thank you, Mr. Chairman. If I could, I would like to follow up just a little, and Captain Marcus, thank you for that outline and specifically about various maritime issues. One day they will wonder why we do not have a merchant marine, and they will all wonder exactly how are we guaranteeing that security in time of war. So thank you for reminding us of that.

Senator Murray hit on an important point which is how you are inputting into the process, and Mr. Bates, I think you are in the middle of a contract negotiations, are you not?

Mr. BATES. Yes, we are.

Senator CANTWELL. And hopefully those will be resolved in a positive way, but are there issues that are part of that discussion that are part of the security issue about how you participate in the design of implementation of what your day to day work force is going to be required to do?

Mr. BATES. In our contract talks?

Senator CANTWELL. Yes.

Mr. BATES. Yes, there are. There is technology and jurisdictional issues that we are discussing that are not unlike what we dealt with with mechanization and monitorization in 1960 and 1961, and the technology, well, one of the issues, they would like to use that to get rid of some of the work force that is already is in place that is doing a lot of these jobs that we are doing right now. One of those is inspection, the inspection of the containers, the containers' seals, the empties, opening the doors, checking the empties and following through with that, possibly check them again when they go on the ship or vice versa when they come back from overseas.

Senator CANTWELL. I am not sure I understand. Who would check a container seal, whether it had been broken or not, if it was not a human being?

Mr. BATES. I hear that electronically, they want to have some electronic seals. I just heard it today again. So we would have to check those seals. That is what I am saying. They want to get by with not checking the empty containers, for instance, coming in, not opening the doors and looking at every empty container and specifically talking about that. We check the seals of the empty or the loaded containers that come across.

Senator CANTWELL. Mr. Yap, does your system deal with empty containers?

Mr. YAP. My system actually deals with the information that sits on top of, basically what we call track and trace information that is pushed into the system. We are really the front end system that sits on top in the front of the system.

In terms of answering the question, I think the seal technology entails two things, one is the physical checking of the seal, itself, and the other has to do with the procurement of the information that attaches itself to the seal. So as I see it, both as information that attaches to the seal which needs to be computed as well as the physical checking of the seal, itself, which comes into the port

Senator CANTWELL. Mr. Bates is talking about checking empty containers, and obviously they are empty, but maybe somebody has infiltrated the system and added something to that container.

Mr. YAP. Perhaps I could paraphrase. What you are saying in terms of information that attached to the seal, it actually has been tampered with. Is that the question?

Senator CANTWELL. I am not sure. I am not sure there is a seal. It is empty.

Mr. BATES. No, excuse me, Senator Cantwell——

Senator CANTWELL. They are all sealed?

Mr. BATES. No, they are not all sealed. The empties are not sealed.

Mr. YAP. My sense basically is that when a container is actually taken together, one of two things actually happens here. First, there is a physical seal that attaches itself to the carrier, that has got to be basically physically watched in terms of tampering, in terms of any intrusion if you like, but I think what we are talking about is in terms of the information that attaches itself to the seal. We are talking about for example——

Senator CANTWELL. I want to get to that in a minute. I am asking that about your technology, but I think Mr. Bates is bringing up a good point, but maybe it is just an interesting thing to have it resolved as they work through their process, but there may be elements of the security system that is not about manifests, because there are no manifests, not about security seals, because there are no security seals, but they are about the infrastructure of the whole shipment and other opportunities that—that if somebody wanted to infiltrate the system, they might be able to do that, because it is not in a container that has a seal or a manifest.

Mr. YAP. I think in terms of the seal technology, we are the layer that actually sits on top of the——

Senator CANTWELL. Captain Marcus?

Mr. MARCUS. Actually, if I might jump in on that, that is a concern that we see on board ship. An empty container is frequently undocumented. It is loaded aboard the ship as an empty. It is never inspected at either the loading terminal or the discharge terminal, so you have a empty container aboard the ship, but in reality, anything could be in that container. It is not manifested. It is listed as empty. It is not sealed. It is not locked. Frequently, it is loaded aboard ship, and you cannot get access though this container. For example, you may have a container that is buried in the hold. You may have it four or five tiers high, and that empty container is unaccessible. So it is a concern both aboard ship and ashore.

Senator CANTWELL. Mr. Yap, thank you for being here, and I understand you are the CIO of the organization. So maybe you could answer, the deployment of this is through the Port of Singapore, soon to be here in Seattle?

Mr. YAP. That is correct.

Senator CANTWELL. Or the Port of Seattle. Are there any other parties that have deployed your system?

Mr. YAP. We have introduced this technology essentially in China. That is going on now. The other is in Italy. That is in Genoa.

Senator CANTWELL. As you describe your system, it is an information database system, a layer, an information layer that sits on top of the security system?

Mr. YAP. That is correct. So what we are doing here is basically just to keep you a line of information pertaining to the container, information pertaining to the shippers, pertaining to cargo, bill of lading, all the information that we have today, but that is actually the shippers' information that they declare. The shipping line information that we, that we are implementing. This is absolutely necessary when you have contracted cargo to sell. I think the question here in play is then information versus——

Senator CANTWELL. No, I am assuming, you are probably a closed platform or open platform?

Mr. YAP. We are an open platform.

Senator CANTWELL. Could not, so other people can build on your architecture and build on it, and so on, and that is a positive thing in many ways, but I am assuming that the security of that system is guarded, I do not know, with some sort of security encryption technology?

Mr. YAP. Yes, yes.

Senator CANTWELL. And you have had no problems with vulnerability of your system?

Mr. YAP. None whatsoever. Coming from a nation such as Singapore, we have strict firewall technology. It is a three-tier firewall technology, and also because it is data encryption to ensure data is actually being entered into the system, and actually being pushed, processed and also be mandated to have the highest level of integrity and correctness.

Senator CANTWELL. So your system deals with security, and it deals with security of information once it is compiled. You do not really focus on the security of the seal, per se, other than making sure that that information is transmitted?

Mr. YAP. That is correct.

Senator CANTWELL. So do you have opinions about the security, in the sense of an optimal security solution being, as a CIO of a related technology, do you have any opinions on what kind of technology solution should be deployed for container cargoes in the current sealed process or other technology that some people have indicated that they have capability of actually attaching, you know, a device to, you know, wireless communication to every single piece of cargo and having that tracked and having that ping a mother ship every time there is a change in that? So then if something has been moved or changed, do you have input on that?

Mr. YAP. My opinion in terms of the technology that stands today is that in terms of where we are, the technology enablement, the features are there. The ability for a company to pick up such a technology and deploy it exists. We see basically that there is a strong indication today that electronic seals which become such a deterrent in terms of looking, of absolutely foolproof in terms of its ability to prevent any box basically from being compromised. I do not think I have the answer at this point in time.

Senator CANTWELL. Well, I think something could be inside with the product, right inside the box. So if you ever have a sealed box, and you know the seal has not been broken, but guess whatever, inside there is——

Mr. YAP. Absolutely, I think what price you are willing to pay, I think you put in the most advanced technology today, and you

can basically look in terms of intrusion detection to the ninth degree, but if the costs are absolutely high and are prohibitive, then it becomes a deterrent, itself.

Senator CANTWELL. One more question, and then I want to turn it over. Is your company participating in any international organizations like TIET or the other organizations that build on standard for your kind of security, information security systems, so that we can either have compatible platforms, either compatible systems to your platform, but standardized on one platform for information sharing? Is that happening?

Mr. YAP. Yes.

Senator CANTWELL. So that we do not—we like your success with Genoa and China and Seattle, but is there a way to get this standard to be more rapidly deployed with many more ports in the world?

Mr. YAP. I think you alluded to the first point whether our system remains open. That is absolutely correct. You have an entire system that you can plug, and you can play, and you can play all the major data systems that are available globally, but most of them are still fairly much archaic, because it is built on legacy system. We are the only one that is international engaged.

Secondly, from PSA's perspective, we are also represented in some of the international bodies like IMO for example, which takes this end and some of the data sources that is actually good to be procured.

Senator CANTWELL. I think that is an important point for the Commerce Committee and Chairman Hollings' interest in the port security issue, if there is a way that the Committee could encourage such an international cooperation, encouraging the participation of people coming together and standardizing, Mr. Yap's technology being open, lots of people, you know, you could have a somewhat like the fingerprint system that the FBI and other countries use. We need a similar——

Senator WYDEN. That is an excellent point. We will follow it up. I think we have seen again and again on these technology issues, and you have pointed out that we can huff and puff and do all kind of useful things in this country, and then what happens in other parts of the world?

Senator Cantwell, thank you very much. Any other questions?

Senator CANTWELL. No.

Senator WYDEN. Just one question, Mr. Bates. How often do you find an unsealed container?

Mr. BATES. Daily. The empties are unsealed that come into this port.

Senator WYDEN. To most folks, this is an issue that is like my kids say, this is a "hello" kind of issue. I mean if you have unsealed containers, it seems to me they are just potential magnets for terrorists, because they are not subject to any of the rules. They are just sort of out there. Am I missing something?

Mr. BATES. No, I believe that is, it is very true. In fact, I know that, and coupled with the fact that our proximity to Canada and the truck deliveries that come in that do not have empties checked when they are carrying an empty container. You know, it just to seems to me that that is mind boggling that that happens.

Senator WYDEN. We are going to work with all of you. This is something that we can take up in the conference committee. You all have already indicated you are going to support that requirement as well, and in the legislation, but my colleagues asked a number of questions with respect to this containerization, you know, questions which just seem to me to state the obvious. If you have got unsealed containers floating around, this is a clear, unquestioned security problem, and we will work with you to get it taken care of.

You all have been great.

I have some other questions that I would ask Captain Marcus. I was particularly exasperated as I heard about some of the issues relating, you know, to the Coast Guard and the certification requirements. Some of them apply to U.S. flag vessels, and then do not apply to overseas, and our Government basically let those other people off the hook, and that just does not seem to be right either, and I know this is something that is probably of concern to you, and I want you to know that this is an area that I am going to follow up on.

Gentlemen, we have got another long panel ahead. So we will excuse you at this time. Thank you for all the excellent input.

As I said, I do pledge to put all of your remarks into the record. If you could just summarize your principle concerns in your five minutes, that would be great.

**STATEMENT OF VIKRAM VERMA, CEO, SAVI TECHNOLOGY**

Mr. VERMA. Chairman Wyden, Senators Cantwell and Murray. To begin, I would like to take a moment to thank you, all of you, for the leadership you have demonstrated on the issue of the vulnerability of the global supply chain to terrorism. I would also like to commend Mic Dinsmore and the Port of Seattle for hosting this event. Since September 11, Mic has been a vocal and tireless advocate of moving quickly to address the vulnerability of our ports and the global supply chain to terrorist actions while at the time ensuring the free flow of goods into the United States.

I have two comments on the nature of the threats we are facing. First, the container security threat is real. With the expectation that we will be attacked, we must look at what is most likely to be the next target. Candidly, I believe the global supply chain is the prime target and in its present state is especially vulnerable to terrorist attack.

Second, the threat is systemic. Simple solutions designed to prevent point attacks only or to provide 100 percent inspection at designation ports will not work for the entire supply chain. Though extremely complex, we must look at the problem holistically, and as Senator Murray and Senator Cantwell said earlier, we need to put in place a security system preventing the threat at the point of origin before it hits our ports in the United States.

In terms of the policy response, we believe Congress is moving in the right direction. The Senate Commerce Committee's legislation on maritime security passed in December of last year and currently in conference negotiations with the House is thoughtful and measured. We especially view the considered policy of a "cargo grading" system based on secure supply chain systems to be an im-

portant policy, since it will not only enable secure and fast trade lanes, it also enables a system with a "reset" button, so to speak, in other words, control/alt/delete. So should any terrorist incident occur, the system would come back on in reverse order to which it was shut down. We strongly support this measure and encourage its rapid passage.

Also, Chairman Murray's Transportation Subcommittee's legislation on the implementation of an Operation Safe Commerce program is extremely positive in my view.

All of these are vital requirements that not only add security to the system but will also result in efficiency benefits with better tracking, monitoring and visibility capabilities.

However, it has been almost 10 months since the horrific terrorist attack on our country, and in my view there has been too much discussion and not enough action coming out of Washington. This is a very complex issue, and we recognize the importance of taking the time to develop thoughtful public policy, but we do not believe that equates to conducting lengthy science experiments on process and technology. In short, as Mic said, we need to get moving using proven, reliable immediately available technology and best practices to address these threats now. Fortunately, there are technology and best practices available today that can immediately be put to use to ensure the safety and security of our supply chain.

You heard a little bit about PORTNET®. You will hear about eModal. One model that I want to share is the Department of Defense's Total Asset Visibility network.

After the Gulf War, the U.S. Department of Defense began testing and implementing innovative track and trace technologies to gain comprehensive visibility of the supply chain as well as acquire "in-the-box" visibility. This led to the development of the radio frequency identification network, spanning 36 countries, 350 nodes at seaports, airports, rail terminals, military bases, tracking 250,000 conveyances as they move around the world.

The Department of Defense has named this global logistics infrastructure the Total Asset Visibility network. This network is comprised of active RFID tags that support full electronic container manifests, and the ability to seal and secure intermodal containers from the loading point at manufacture, through truck, train, and ship transport. Once these radio tags are affixed to containers, essentially making these containers "smart," wireless readers deployed at strategic points feed real-time information on the status, location and other events into a global asset management software application. The Total Asset Visibility Network enables the DOD to track, locate and secure all en-route containers.

Over the last seven years, the system has been battle-tested across over 5 continents and has been used to track all military deployments from weapons to boots to foodstuffs to toilet paper.

Why do I know so much about this system and the benefits? Because my company, Savi Technology, developed and implemented the TAV network for the Department of Defense. Based on agreement with the Department of Defense, this global infrastructure can readily be made available for commercial security use.

In short, the U.S. Department of Defense, one of the largest shippers in the world, has invested over $200 million to build a visible

and secure global supply chain network. In addition, in the last three to four years, industry has spent over $100 million on research and development to enhance this technology and make it more cost effective for commercial use. We feel this provides a rapid deployment capability to address the principles of Operation Safe Commerce, a grading system for secure cargo, and the Customs Container Security Initiative.

In summation, the supply chain is vulnerable. The threats are real and immediate. There are best practices and systems already in place based on proven, reliable technologies that can be immediately leveraged. These include PSA's PORTNET®, eModal, and L–3 Communication to enhance legacy systems that are already in place. I urge the Members of this Subcommittee to move quickly and expediently to make these systems available for implementing maritime and port security.

Once again, I appreciate the opportunity to address the Committee.

Senator WYDEN. Thank you, very much.

[The prepared statement of Mr. Verma follows:]

PREPARED STATEMENT OF VIKRAM VERMA, CEO, SAVI TECHNOLOGY

**Senator Wyden, Members, and Distinguished Guests,**

I want to thank you for giving me the opportunity to provide testimony to the Committee on what I believe is one of the most important national security issues facing the United States.

To begin, I have three comments on the nature of the threats we are facing.

First, the container security threat is real. Although it is virtually impossible to predict the precise target or method that terrorists may deploy in their war on the civilized world, we can with confidence predict that, in all likelihood, the U.S. and other developed nations will continue to be the target of further terrorist activities.

With the expectation that that we will be attacked, we must look at the world through the eyes of a terrorist in order to determine what is likely to be the next target. What is both accessible and can be destroyed or leveraged to create maximum societal and economic disruption and damage? The global supply chain is one such target and it is especially vulnerable to terrorist attack.

The characteristics of an efficient, lean, high-velocity global supply chain—openness, ubiquity, diversity, agility—are also why it is an extremely attractive target for terrorists. The global supply chain is an accessible and tremendously efficient delivery system whose reach can allow a terrorist to strike virtually anywhere in the world—with potentially catastrophic results.

In addition—the supply chain is the foundation of the economy. The health and well being of our economy is directly tied to the continuous availability of efficient freight transportation. It has been estimated that a disruption that shuts down the global supply chain will cost the world economy $1 Trillion dollars per week. Sinister elements wanting to destabilize the economies of the US and other industrial nations are certainly aware of this direct linkage.

Secondly, the threat is systemic. The vulnerability of the supply chain must be viewed from two perspectives; point attacks against a single element and systemic attacks against the infrastructure as a whole. Because of the decentralized and redundant character of the freight system, many believed that systemic vulnerability was low. September 11 showed that terrorists could carry out operations that are more complex. This made us more aware of systemic risks via indirect attack upon the overarching interconnected, interdependent transportation infrastructure.

With over 300,000 miles of freight rail networks, 45,000 miles of interstate freeway, 600,000 bridges, 500 commercial airports, and several hundred of ocean freight terminals handling 16 million containers every year—the physical infrastructure supporting freight transportation is vast and poses a tremendous challenge to effectively monitor, safeguard and control.

Solutions designed to prevent point attacks will not work for the supply chain. Though extremely complex, we must look at the problem holistically—and put in place a security system that is capable of being as ubiquitous and flexible as the supply chain itself. This system must leverage best-of-breed technologies and proven

processes to integrate the various components of the transportation system into a single command and control infrastructure that deters and prevents terrorists from using the supply chain for their activities, and also provides authorities the means by which to continuously monitor the supply chain and intelligently respond to security threats as they occur.

Thirdly, the threat is asymmetric. As has been widely discussed, full frontal conflicts—much like the Gulf War—are probably a thing of the past. Terrorist organizations will leverage their strengths of radically decentralized organizations with fervent followers employing low tech means to attack the U.S. We cannot respond on the same terms.

Now, what is to be our response to the ongoing asymmetric, systemic, real threats in port and maritime security?

First, as many of you have said, there is no single solution. We need effective intelligence, deterrence, monitoring and tracking, and response capabilities to secure the global supply chain. These capabilities however must be delivered through an integrated, comprehensive, systems-based approach that spans policy, security procedures, business practices and technology. With respect to technology, given the asymmetrical nature of the conflict, we need to employ high-tech means to prevent low-tech attacks. Equally as important, all participants in the global supply chain from port operators to port workers to global importers and exporters to shipping lines to technology companies need to work together.

Secondly, in terms of the policy response, we believe Congress is moving in the right direction. The Committee's legislation on maritime security is thoughtful and measured. We especially view the considered policy of a "cargo grading system based on secure supply chain systems" to be an important policy since it will not only enable secure *and fast* tradelanes, it also enables a system with a 'reset' button (so to speak) should any terrorist incident occur. This is a vital point: if we shut down the nation's ports indefinitely or even for several days in the event of an incident, we will hand the terrorists a multi-trillion dollar win. We simply must keep the supply chain running securely and smoothly.

The Senate Subcommittee's legislation on the implementing of an "Operation Safe Commerce" program is also very positive in my view. The concepts of Operation Safe Commerce get to the physical nature of a complex problem, specifically:

- The development of auditable security standards for maintaining secure loading docks and ports
- The outfitting of containers with mechanical and/or electronic seals and devices intended to identify containers whose security has been compromised
- The establishment of integrated communication systems to track containers throughout the entirety of their journey through the global supply chain
- The transmission of that tracking data in accessible format to appropriate Federal agencies
- The demonstration of secure trading lanes that ensure maritime and container security from point of origin to point of destination
- The establishment of new requirements which will pertain to all participants in the supply chain to allow Federal agencies sufficient information on the contents of each container and its expected journey.

All of these are vital requirements that not only add security to the system but will also result in efficiency benefits with better tracking, monitoring, and visibility capabilities. Further, ports and global importers and exporters are the key strategic control points in implementing these standards.

Finally, US Agencies are also taking positive proactive measures to secure the nation's transportation network and supply chain. Admiral Loy and the Coast Guard were especially admirable the day of and immediately after 9–11. They have taken that momentum and have instituted new security policies and procedures as well as have recruited a volunteer network to help monitor our nation's ports.

US Customs and Commissioner Bonner have been actively pursuing raising the security of the global supply chain through:

1. The Customs Trade Partnership Against Terrorism (CTPAT) Program
2. Customs' Container Security Initiative (CSI)
3. Bilateral agreements with our top trading partners

A third point, I would like to strongly emphasize is that this is no time for science experiments in process or technology. In a conversation I had both in April and just last week with the CEO of one of the largest port operators in the world, he is convinced there will be an incident in the global supply chain. We must use proven, reliable immediately available technology to address these threats now. We must leverage existing best practices currently in use.

Pilots and "proof of concept" projects are being proposed that will take years to complete. Then—and only then—can you begin the time consuming task of actually implementing the tools, technologies, and processes that will address the problem.

Fortunately—there are technologies and best practices available today that are proven, reliable, and can immediately be put to use to ensure the safety and security of our supply chain. One model I want to share with you is the Department of Defense's Total Asset Visibility Network.

After the Gulf War, the U.S. Department of Defense began testing and implementing innovative track and trace technologies to gain comprehensive visibility of the supply chain as well as acquire "in the box" visibility. This led to the development of the world's largest active radio frequency identification (RFID) network, spanning 36 countries, 350 nodes at seaports, airports, rail terminals, and military bases, tracking 250,000 conveyances as they move around the world. The DOD has named this global logistics infrastructure the Total Asset Visibility network.

The Total Asset Visibility network is comprised of active RFID tags that support full electronic container manifests and the ability to seal and secure intermodal containers from the loading point at manufacture through truck, train and ship transport. Once these seal tags are a affixed to containers—essentially making these containers "smart"—wireless readers deployed at strategic checkpoints worldwide, most prominently in ports, feeds real-time information on the status, location, and other events into a into a global asset management software application. The Total Asset Visibility Network enables the DoD to track, locate, and secure all enroute containers.

Over the last seven years the system has been battle tested across over 5 continents, runs at 99.999-percent uptime, and has been used to track all military deployments from weapons to boots to foodstuffs. While the system was designed and the infrastructure was deployed to track all Department of Defense supplies leaving the country and landing in foreign ports, it can be used just as efficiently to track all goods entering the country with active RFID seal tags being applied at foreign port of origin by certified parties.

Total Asset Visibility could enable U.S. authorities—US Customs, the U.S. Department of Transportation (DOT) Transportation Security Agency (TSA), and the Office of Homeland Security—to physically track and trace containers' physical movements from the manufacturer's dock to the U.S. port of discharge and beyond. Electronic active RFID seal tags on containers enable a security layer to detect potential intrusions and tampers. Alerts and exceptions can be programmed into the Total Asset Visibility network to automatically alert authorities of suspect container movements and to locate questionable containers quickly. Further, hazardous materials shipment information can be encrypted and tracked on electronic manifests affixed to containers to increase security and safety.

Why do I know so much about this system and its benefits? Because my company, Savi Technology, developed and implemented the TAV network for the Department of Defense and we are continuing to operate and extend the system for commercial applications. Based on agreement with the Dept. of Defense, this global infrastructure can readily be made available for commercial security use. In short, the US DOD, one of the largest shippers in the world, has invested over $200M of the public's money to build a visible and secure global shipping network for their supply chain. To the extent that best practices and available technologies are considered, we feel this provides a rapid capability to address the principles of Operation Safe Commerce and Customs Container Security Initiative.

In summation, the supply chain is vulnerable; the threats are real and immediate. The problem is complex—and no simple, point solution will be adequate to address the problem. There are systems already in place based on proven, reliable technologies and processes that can be immediately leveraged to create a comprehensive system that will deter and prevent security breaches and will enable authorities to efficiently monitor and immediately respond to events that occur in the supply chain. I urge the Members of this Subcommittee to move quickly and expediently to make these systems available for the sake of the continued safety and security of our economy, our country, and most importantly our people.

Once again, I appreciate the opportunity to address the Committee and further welcome any questions.

Senator WYDEN. Mr. Cushing?

**STATEMENT OF JOHN CUSHING, PRESIDENT, eMODAL.COM**

Mr. CUSHING. Thank you. Good afternoon, Senator Wyden, Senator Murray, Senator Cantwell. I am going to take you up on your

suggestion and leave my submitted comments, and I would like to take my five minutes——

Senator WYDEN. Bless you.

Mr. CUSHING. I am still going to take my five minutes, and I thought I would tell a quick story, and the story is about solutions. That is what we are looking for today is security solutions, and since September 11, we have all geared up and taken further action, but in the United States, there has been a lot underway leading up to that, and it goes back a few years to November of 1994, and in the Nation's busiest port complex, L.A.-Long Beach, drivers boycotted work, and they said we are not going to work anymore, because the queues are too long, and a number of other issues, and we brought the truckers to the table, the terminal operators to the table. We all sat down, and we said we have got to come up with a system between trucking companies and terminal operation. What we did was we built the Nation's first port community system, and since that day, we now have that port community system in 14 ports around the United States. We also have it in Central America and Europe. It has been a very collaborative effort. It has involved marine terminal operators, steamship lines, port authorities, trucking companies. We have got over 3,000 registered companies as part of eModal. It is a Web-based system. It is a single portal working system in the United States for importers, exporters. We have got from mom and pop importers to Wal-Mart, K-Mart, Target are all part of this system. Registered users include Customs, the Coast Guard, include port authorities. In fact, most of the terminals and trucking companies here in the ports of Seattle and Tacoma are already on board with this port security system actively working to address some of the issues.

What are some of the issues we have worked on since? One of the big ones is security. We had a system where we got together with the truckers and the terminals and said, How can we deal with trucker identification? There is no simple solution for that, so we put together what we call Trucker Check, a Web-based system.

To date right now over 12,000 drivers' status is being checked while we sit here. They are in the database trying to get in and out of terminals. That system is being expanded to other terminals and other ports. The system we use as I mention is Web-based, but for the identifying card, credentialing, we went with the driver's license for a number of reasons. Number one, if you are driving, you must legally have a driver's license with you.

If you are running a terminal, you want to be sure that for risk management purposes, those coming onto the terminal have a driver's license. There is a standard set up. Driver's licenses now have barcoding and swipe capabilities. We were able to put all 50 states plus Canada and Mexico into the system. So we work on logical, everyday use that the industry is comfortable with, but take it up a notch by introducing technology to those methods.

We also have what is called eModal Scheduler. It is an appointment system. While it provides efficiency at the terminals, what it also does is it allows the terminal operators to verify purpose. It is one thing to say I can come onto your terminal because I can verify who I am with whatever trucking company, but this asks

what are you doing here on this day, this time block? We put purpose on it.

Other things, we talk about documentation being a lot of loose paperwork floating around. Right now if we have our customs brokers, they will go in their file with customs cargo cleared, and then what they do is they give an order to a trucker to go deliver the goods.

Well, it is a paper order. They have couriers running around with this information. This is oftentimes in technology, traditional—this is archaic to have people running around with hazardous cargo information, destination, things like that. We sat down with the customs brokers and terminal operators and truckers and said what do we have to do to make this thing work? It is a closed system with digital certificates downloaded, but it works. So it is approaching things from a logical approach.

We have got the community working behind it, which is key, because this is a very, very fragmented industry we are in, the transportation industry, many different carrier modes. We have many different carrier facilities, many different systems. So what we have done is brought them all together and by working with them to create this Port Community System.

Senator WYDEN. Very excellent presentation. Thank you very much.

[The prepared statement of Mr. Cushing follows:]

PREPARED STATEMENT BY JOHN CUSHING, PRESIDENT, EMODAL.COM

I would like to thank the Subcommittee on Surface Transportation and Merchant Marine of the Committee on Commerce, Science, and Transportation for having this hearing to address these very important and critical issues. My name is John Cushing. I am the president of eModal.com, a Web-based Port Community System. eModal's Port Community System is currently in place at terminals in 14 major Port complexes around the United States. At this very moment, eModal has more than 400,000 containers and 12,000 truck drivers' information in our database that is being applied to various working applications. More than 3,000 transportation and transportation-related companies, including the United States Customs Service, the United States Coast Guard, Port Authorities, marine terminals, trucking companies, railroads, importers, exporters, Customs brokers and others are registered and participating at various levels within the eModal Port Community System. I am happy and encouraged to report that terminals and the trucking community right here in the Ports of Seattle and Tacoma are actively engaged in the eModal Port Community System.

As a very brief background to what eModal is all about, it is fair to say that we were born out of a need to address disarray and fragmentation in the Ports. In November of 1994, truck drivers boycotted work in our nation's busiest Port complex in Southern California. While there were many issues that were on the table, including queuing at terminal gates, it became obvious that the various transportation carrier modes and the terminals needed to improve the level of communication and coordination. eModal's solution brings the various industry participants to the table on a common platform—a single portal.

Although eModal's Port Community System addresses many of the needs of the transportation industry to operate efficiently in both a safe and secure manner, there is clearly more that needs to be done. The single portal Community-based concept allows all users to work together to ensure that this be accomplished.

Prior to the September 11th attacks, eModal was already working with marine terminals to provide security at the terminal gates. A leading cause of crime at a terminal occurs when a bad truck driver misrepresents them self at the terminal gate as a truck driver for the company that was supposed to be on the premises to pick up or deliver cargo. To address this, eModal developed and has implemented the eModal Trucker Check™. Participating marine terminals require that trucking companies and truckers wanting access to their terminal register with eModal. The process requires that the trucking company register with eModal and be assigned

a unique User Name and Password. Registering trucking companies are required to fill an application, identify their Standard Carrier Alpha Code, and enter verifiable information about truckers employed or contracted with them wanting access to terminals. The information about each trucker includes: first name, last name, driver's license number, state of issue (50 states, Canada and Mexico), driver's license expiration date, contract period if under contract, a unique Personal Identification number (PIN) that uses the National Motor Freight Traffic Association's Standard Carrier Alpha Code (SCAC) prefix for the trucking company along with a computer-generated four-digit random number, and the tractor plate(s) for that trucker. The trucking company also attests that the trucker's driver's license is current and that the trucker has agreed and signed allowing their information to be viewed for verification purposes.

The process begins as the identity of a trucker is verified before the trucker enters the terminal. The terminal's trucker verification then includes a match of the driver's license picture, a match of the data input to verify the driver's license, verification that the tractor being used matches the trucking company and the trucker in the data base, and confirmation with the trucker entering their PIN. The eModal Trucker Check™ has been designed to receive biometric files for match and can query other government databases in an ongoing basis as well.

The eModal Trucker Check™ uses the state-issued driver's license for many reasons. eModal's Trucker Check™ database can query DMV databases for ongoing updates. As most driver's licenses issued now have magnetic reader strip or bar coding, fraud detection is readily available. The eModal/DMV connections also allow for immediate address with any outstanding police issues that are questionable with third party cards.

As indicative of the Port Community System, participants in the transportation industry are looking for greater interface, not less. Unique Port-wide cards restrict truckers' abilities to free flow between various Port complexes—a traditional trait of cargo flow. Truckers are legally required to carry their driver's license. This also provides terminal risk managers assurances when allowing truckers onto their terminals. There is also the ongoing issue that the introduction of another card only increases the opportunity for loss. State-issued driver's licenses are already in place and can more easily be standardized than "reinventing the wheel."

The eModal Trucker Check™ system provides security verification without impacting terminal operations. Terminal gates can be secure and maintain their efficiency. It is imperative that we maintain our position as a productive nation as we address our security needs.

Just as important as important as verifying the person(s) wanting access to Ports' terminal facilities is to verify the purpose for those wanting access. While it is important to be able to match a person with a company, it is also important to verify their purpose for wanting access to a facility.

Originally designed to provide a tool for terminals to set appointments for truckers delivering or picking up cargo, the eModal Scheduler™ provides terminal operators with a tool to determine the purpose of a truck coming onto their terminal. In addition to the requirements placed on the trucker to prove verification for terminal access, the eModal Scheduler™ requires the trucker to have a transaction number associated with the date and time they want access. While a trucker can be verified in a system as driving for a particular company as an employee or as an independent contractor, terminals need verification that the trucker has a purpose for coming on to their terminal. The eModal Scheduler™ provides a single platform for all of the terminals to post their time options for when truckers can select to come to the terminal. The truckers select the time option that works operationally for them. Both parties are then provided the matching transaction number with the cargo being delivered or pick-up. Secure access to providing the transaction number is limited.

Using a unique User Name and Password, a marine terminal's Administrator accesses the required tool sets within eModal. At that point, the Administrator sets up the criteria for posting available time options, based on how they lay-out their terminal as well as how many trucks they can handle at a given time. With criteria in place, the trucking company's Administrator logs on to eModal using their unique User Name and Password and selects the options that work. The transaction number that the trucking company receives at this point is then assigned to the trucker calling at the terminal where it will be matched against the container to be picked or delivered to the date and time slot appointed.

In addition to providing another access requirement, the eModal Scheduler™ provides yet another operational tool for the terminals to use to maintain efficient productivity.

While the eModal Trucker Check™ and the eModal Scheduler™ assure that the trucker is verified with a company and that their purpose is confirmed for wanting access to a Port terminal, it is important to look at other exposed areas. While the cargo flow is often addressed as the area to be monitored, it is equally important that the documentation attached to cargo is securely managed.

The United States Customs Service requires Customs brokers to file documentation electronically with them. Once U.S. Customs has cleared an entry, the Broker can begin the process of notifying a trucking company to send a trucker to pick up the cargo; advise the marine terminal of which trucking company will be coming down for the cargo; and post the same information to the steamship line that delivered the cargo to the terminal. The process, commonly known as a Delivery Order (DO), is either sent by fax and/or via a courier. Some terminals require a signed copy. The DO contains vital information that identifies the commodity, where the cargo is destined, hazardous IMO information, name of trucking company, and in the absence of eModal's Trucker Check™ and Scheduler™, the container and bill of lading number—two numbers that some terminals still use to release cargo.

eModal has worked with the Customs brokers to develop an electronic Delivery Order. After the broker receives clearance from the United States Customs Service that the cargo may be picked -up, the Customs broker now has the ability to continue with a paperless process. The eModal electronic Delivery Order (eDO™) sends this vital information through eModal electronically. As with the other applications, access is limited to those registered with their own User Name and Password. Due to the sensitivity of the eDO™, the companies designated by the Customs broker to receive the eDO™ must also download a secure digital certificate. This adds a further level of identification and verification as to who is in the secure loop to receive these electronic documents.

In essence, once cargo is cleared with the United States Customs Service, it can have its documentation transmitted in a secure, digitally certificated manner to a select group of recipients—a truck company being one. At that point, while still logged in with the same User Name and Password, and with the Administrative rights assigned, the trucking company can select a date and time to dispatch for cargo delivery and/or pick up and be assigned an identifying transaction number to substantiate the purpose for the trucker arriving at a terminal at that time frame. In the sequential order, the trucker is then verified at the terminal gate with the many required criteria on file. These steps provide technological solutions but still more needs to be done.

The eModal applications need to be expanded to address any and all person(s) wanting access on to a terminal. Vendors, maintenance, contractors, administrators and others need to verify whom they work for against a database as well as identify purpose for wanting access to a Port terminal. A match in a database can include files that contain pictures, Personal Identification Numbers, background clearance levels, biometrics and other. eModal has been accepted by 46 terminals in 14 Ports around the United States to provide a community-based system. The current applications will require expanded areas of input to add uniformity and standards to this endeavor.

eModal's functional products also have application for importers and exporters of hazardous and dangerous cargoes. eModal is currently testing existing features for these uses. Further testing needs to be done to ensure complete use of verification and purpose of truckers at chemical, petroleum and other such related facilities.

The use of technology will be required to meet the challenges that lie ahead. While eModal already has a proven use and success record within the Port Communities, it is evident that further expansion and development will be required for current products as well as new products to maintain an ongoing read of trucks, their drivers, their origins and destinations, accompanying and related documentation and the methods for input and retrieval to the eModal database.

In closing, I would like to reiterate eModal's commitment to our nation's Port communities. As the largest Port Community System provider in the United States, we have taken a leadership role that ensures that the products that we deliver meet the rigid standards set by Ports and terminal operators. We have developed these applications to address security with a practical understanding and functional respect for needed productivity. As a result, we have contributed solutions to-date for the transportation industry and we look forward to working towards possible solutions to further our nation's security.

Thank you

Senator WYDEN. Mr. Koch?

**STATEMENT OF CHRISTOPHER KOCH, PRESIDENT AND CEO, WORLD SHIPPING COUNCIL**

Mr. KOCH. Thank you, Mr. Chairman, Senator Murray, Senator Cantwell. Thanks for the opportunity to be here today. I will also put my written comments in the record with your permission and simply summarize.

I think what we are dealing with here as we think through the liner shipping and the container portion of these security issues, is the $1.3 billion of commerce that is going through our ports every single day. How do we continue to have the efficiency of that system that benefits American commerce, and at the same time make it more secure? The observation that I would make is that security is not a single issue. There are multiple layers to this.

I think you heard today, the first layer is the ship where the Coast Guard has jurisdiction. Basically, securing the ship is fairly straightforward. Then you then have the marine terminal, which is obviously a major interest to the ports of Seattle and Tacoma. We support the Senate legislation on this and believe that is a good start.

Now you get into more interesting issues, such as personnel security. Do we do background security checks, and, if so, how and for whom? We are very supportive of the legislation that would establish such a system and think it is a good step forward.

But the point I would like to make is about cargo security, which is probably the most difficult issue and will be certainly one of the challenges that the House and Senate Conference Committee on maritime security will have to deal with. The change here is really less about how transportation is conducted than it is about how trade is conducted, and let me make a couple of points.

Before I do though, I would like to commend Customs Commissioner Bonner on the C–TPAT program where customs is working in partnership with the private sector, and the CSI (Container Security Initiative where they are working with foreign governments to establish protocols around the world to inspect and secure cargo before it is loaded on ships. Frankly CSI is a central beginning component of moving forward to build an infrastructure that will work.

Senator Cantwell, your comment of an international protocol to do that is an excellent comment. Until that international struction is in place, I would suggest that CSI and custom's efforts be supported.

Maritime security legislation is needed, and the House and Senate conferees have a big task ahead of them.

Let me make a couple of points. The first is, hopefully out of this process, we will get clarity regarding Government organization and responsibilites. Regardless of whether you are talking about a Department of Homeland Security or not, we need clarity about who owns these issues and how they get dealt with.

The Coast Guard has responsibility for the ships. It seems to have responsibility for U.S. ports. Customs has container security, usually, although the Transportation Security Administration's role is somewhat ambiguous in all that. But, I think we also need to consider who responds if we have an incident. At the present time, it is probably the Department of Transportation. There is a serious

goverance problem if the people who are responsible for response are not the same people responsible for developing prevention protocols.

Senator Murray, you were talking about crew manifests and how those issues are dealt with. To show you an example, an ocean carrier coming to the U.S. electronically files 96 hours ahead of time a crew manifest with the Coast Guard. It gives the paperwork to the Customs Service when it arrives. It gives the paperwork to the INS when it arrives, and the House version of the legislation would have carriers also give it to the TSA in advance. That is three existing, potentially four agencies. The industry has offered to submit it all 96 hours in advance to one place. We think a little coordinator in this effort——

Senator MURRAY. Should that be, which agency?

Mr. KOCH. I believe the Customs Service system is the easiest to get it up and running. They have got it in place for the aviation industry and for use on cruise ships. It ought to be easy to get together for this industry as well.

Then you get to the trade implications of enhancing security, and I would submit that this legislation also has to deal with these issues, namely what information importers and exporters have to provide, when do they have to provide it, and how accurate does it have to be. We have a number of holes in the system at the present time.

Today, the way the information is transmitted by the ocean carriers is via cargo manifests. First, there is no agreement on what level of detail the cargo descriptions have to be from the shipper of the cargo. Second, to the extent accuracy is required, one must recognize that it is the ocean carriers who must rely on the shipper's description: all they are or can be doing is providing the information that is given to them by the shippers.

As you can see from our testimony, we have indicated that we would be willing to accept a requirement from the Customs Service to provide cargo manifests before loading in a foreign load port, but that requirement has to be applicable to every carrier, including the non-vessel operating common carriers that handle over 30 percent of the inbound cargo.

So in conclusion, what we would like to see is that the Government be organized clearly, that clear rules be established so that every party in the supply chain knows exactly what is expected of them, there is no ambiguity about who has to do what, and that we establish these rules—as all of you have said—in a way that still allows an efficient flow of trade, that does not choke trade.

Take, for example, the seal technology that has been discussed. If we have one seal standard in the U.S. but the seal readers at the gates in the U.S. have a different technology or different system than those in Rotherdam, Singapore or other places, we have just created a big mess. So international standards are really going to be essential for this. The U.S. has been responding pretty well in supporting international initiatives in this regard. I think we just need to urge the continuation of that.

Senator WYDEN. Sounds too logical to me. Thank you. Very helpful.

[The prepared statement of Mr. Koch follows:]

PREPARED STATEMENT OF CHRISTOPHER KOCH, PRESIDENT AND CEO, WORLD SHIPPING COUNCIL

The government and all segments of the maritime industry, including liner shipping[1], have spent considerable effort since last September to determine what new programs and rules should be developed to protect international trade from the risk of terrorism. Now that the Senate and House of Representatives have both passed versions of maritime security legislation and announced the formation of a conference committee to produce a final bill, we enter the most important stage of this legislative process. It is important because the Executive Branch agencies need additional authority to address the challenge. It is important because the agencies need to have their roles and missions more clearly defined and coordinated. It is important because the private sector needs to know what will be required of it. And it is important because what is required will not only affect enhanced security, but how efficiently and reliably, and at what cost, America's international trade will continue to flow.

**I. Containerization and Liner Shipping**

Containerization was developed for the purpose of providing a more efficient, less expensive way to move goods, and its success surely exceeds what Malcom McLean hoped for when he began this revolution in the mid- 1950's. Last year, the United States moved roughly 7.8 million containers of import cargo and 4.8 million containers of export cargo through its ports. That is roughly $1.3 billion worth of containerized goods moving through U.S. ports every day. Seattle and Tacoma are major national gateways for the nation's international trade, as well as efficiently serving the import and export needs of Washington State. The movement of sealed containers has greatly reduced damage and pilferage of goods. It has facilitated intermodal door-to-door supply chains. And it has done so with remarkable efficiency—making ocean transportation a huge bargain for importers, exporters and consumers. Last year, for example, the cost of transporting all of America's liner imports, including all consumer, commercial and industrial goods, was only $133 per household.

This remarkable system operates by carriers—truckers, railroads and ocean carriers—transporting sealed containers, like the postal service transports sealed letters and packages. The challenge we now face is how to ensure the continuation of this system's benefits and efficiencies that knit the world's economies together, while at the same time instituting new initiatives and rules that can enhance security.

The international liner shipping industry has taken this challenge seriously. On January 17 of this year, the World Shipping Council issued a White Paper[2] that made a series of recommendations on how the government should address the issue of maritime security. It was and is, not a solution to every possible concern, but a good-faith effort to propose meaningful improvements to the supply chain.

The immediate challenges are (1) to design the security process and deploy the capabilities necessary to minimize, detect and intercept security risks as early as possible—before they are loaded aboard a ship for delivery to their destination, and (2) to have the systems and international protocols in place to ensure the efficient flow of international commerce during all possible security conditions. We must protect the system that facilitates world trade, and prevent transportation assets from becoming means of delivering destruction. We must protect the lives of people who make the international trade system operate and who work and reside in areas through which trade flows. We must protect nations' ability to continue their trading relations in the event terrorists do attack. And, we must recognize that this terrorist threat is not going to go away, but only become more challenging as world trade volumes grow.

For that reason, what is at issue is not just maritime security, or even the global, intermodal transportation system, but the flow of international trade and the world's economic health. The stakes are high. Consequently, the United States is focused on implementing security measures that begin as early in the transportation supply chain as possible.

---

[1] The World Shipping Council is a nonprofit trade association representing the international liner shipping industry. Its members carry roughly 90 percent of America's international liner cargoes, which represents two-thirds of the value of the country's ocean-borne international trade. A list of the member companies of the Council is attached at Appendix A.

[2] The paper, entitled "Improving Security for International Liner Shipping", can be found on the Council's website at www.worldshipping.org.

The World Shipping Council has provided this Committee with its White Paper recommendations and has previously testified about specific aspects of security regarding vessels, marine terminals and ports, personnel, and cargo documentation. I will not repeat that testimony today, but will instead offer some suggestions as the Committee enters into the final phase of writing maritime security legislation

**II. The Government Organization Challenge**

Designing and implementing an effective maritime security program will require cooperation, information sharing, and coordination between government and industry, and because this is an international business, it will also require international cooperation between governments.

A unified, coordinated U.S. government strategy must be designed not only to detect and prevent terrorist attacks on the international cargo transportation system, but also to provide adequate contingency planning for the management of the consequences should a significant attack occur, and—by all means not to be forgotten—to ensure the continuation of efficient, reliable, low cost transportation of America's commerce.

The government organizational challenge is substantial. The Department of Transportation oversees transportation, and, in the immediate aftermath of September 11, the Congress created the new Transportation Security Administration (TSA) within DOT with very broad authority for transportation security in all modes, including maritime. Also within DOT is the Coast Guard with broad authority to address large segments of the maritime security issues involved, but not all. The Customs Service oversees trade, and has taken the commendable initiative to develop two programs to reduce the risk of terrorism, namely Customs' Trade Partnership Against Terrorism (C–TPAT) and the Container Security Initiative (CSI). C–TPAT is a voluntary program between Customs and industry to develop a more secure supply chain. CSI is a program pursuant to which Customs has begun establishing agreements with other nations' Customs organizations for the purpose of information collection, pre-screening, and cargo inspection. The Immigration and Naturalization Service and the Department of State are responsible for crew visas and entry into the United States.

Improving the security of international commerce requires a tightly integrated, common approach and clear responsibilities. It also requires government agencies to effectively share the information that they require. President Bush's proposal to reorganize the government and create a Department of Homeland Security should help achieve this. In many respects, maritime trade is a "poster child" for this initiative. In fact, the maritime transportation industry was the first example used in the President's explanation of the new Department.[3] The fact that there are numerous federal agencies, each with a portion of responsibility—often overlapping other agencies'—has not only caused confusion in the industry and within government, but it has delayed the development and implementation of problem solutions.

Let me provide some examples, both because they are illustrative of the problem and because we request that the maritime security legislation clearly address them. First, consider personnel security aboard vessels. Ocean carriers must file their crew manifests with three different federal agencies (the Coast Guard, the INS and the Customs Service) in different format at different times. The House-passed maritime security legislation would add a fourth agency, TSA, to that list. Instead of having one agency responsible for checking crew members, or even having one system that all agencies can share, each agency has its own system and procedures. The three agencies are now working on plans to automate these systems for electronic advance filing of the information. But, each agency—motivated by recently enacted or envisaged legislation—is planning on having its own system, rather than a single system that all agencies could share. The present system is uncoordinated, confusing and inefficient. We strongly recommend that the final legislation require the establishment of a single system for the receipt of crew manifest information, and that agency responsibility for crew issues be clearly defined.

The Coast Guard estimates that roughly 200,000 seafarers call at U.S. ports per year. It is entirely appropriate that security procedures for seafarers be in place. At the same time, it must be recognized that seafarers are, in many respects, the first line of defense to ensure that vessels are secure when they arrive in a U.S. port, and they should be treated fairly with clear, predictable, and uniformly applied rules.

Let me provide another example of the need for clear government organization and role definition. The U.S. Customs Service appears to have the "lead" on con-

[3] "The Department of Homeland Security"—President George W. Bush (June 2002)

tainer security issues, as both the C–TPAT and the CSI initiatives would indicate. Customs is awaiting enactment of the pending maritime security legislation by Congress which will authorize it to issue regulations changing the requirements applicable to cargo documentation for imports and exports and conduct better cargo security screening earlier in the transportation process. But the bills in conference do not agree on what Customs' role will be, as the House version of the legislation provides that, while Customs may collect cargo manifests from carriers to use for security screening purposes, TSA shall "develop and maintain a antiterrorism cargo identification, tracking, and screening system for containerized cargo shipped to or from the United States".

This presents fundamental governance issues that must be resolved. First, which agency is responsible for the analysis and risk assessment of the acquired information, and, if that agency is not Customs, can it analyze and act on the information and communicate to Customs in time to identify cargo that requires further attention before loading aboard a vessel?

Second, if Customs is responsible for screening and inspecting cargo and detecting security threats, but another agency is responsible for managing how and whether ports and vessels and trade would operate if there were a terrorist incident, there is a risk of an uncoordinated or inconsistent view of what needs to be done, when coordination and consistency will be most needed.

It is essential that the enhanced security, screening and prevention programs be in precise alignment with the incident planning, management and response programs. If they are not, many billions of dollars worth of trade and millions of jobs in America and around the world could be adversely affected. The agency responsible for answering to the President for how the United States government would keep international trade flowing in the event of a terrorist event, must have complete understanding and confidence in the programs being put in place to address these risks on a preventive basis. Stated differently, the regime being designed for addressing the risk on a preventative basis also must be capable of addressing how trade would continue to flow efficiently if it had to respond to an incident.

A Department of Homeland Security should help accomplish this. Already since the announcement of the President's proposal, we see some positive signs of closer agency cooperation. If there is one overarching concern over the initiative, it is that such a department would become so focused on the security of the transportation system that it would not properly consider the costs, delays, inefficiencies and complexities that new requirements could impose on America's international trade.

## III. Supply Chain Security Analysis

Defining what constitutes a secure shipment is relatively straightforward: a container should be stuffed in a secure facility, by approved people, sealed immediately upon stuffing, transported from that location to the ocean carrier in a timely manner that ensures the container is not compromised, stored in a secure facility where it is not compromised, and then loaded aboard a secure ship for transit. And if there is a security question about a container, it should be inspected by appropriate authorities before it is loaded aboard a ship.

Implementing that vision is enormously difficult (1) because of the number of different entities in different jurisdictions involved in a shipment—those involved in loading and sealing the container, documentation of the shipment, storage, trucking, railroads, inland terminals, marine terminals, and the ocean carrier, (2) because of the current lack of a clearly defined and coordinated information system to receive, analyze and act on all the shipment data relevant to pre-screening containerized shipments before they are loaded aboard a ship, (3) because of the limitations and expense of technologies that might be developed, and (4) because of the lack of an established or coordinated global capability to inspect containers, when warranted, before they are loaded aboard ships.

### *C–TPAT and CSI*

The good news is that the government is taking positive steps in tackling this challenge. The Customs Service has undertaken two important initiatives: Customs' Trade Partnership Against Terrorism (C–TPAT), and the Container Security Initiative (CSI).

C–TPAT is a voluntary program focusing on U.S. importers. The theory is that if they undertake certain actions to improve the security of their supply chain, they will get preferential treatment of their cargo by Customs. C–TPAT importers will also be required to use ocean carriers that have C–TPAT agreements with Customs, to use C–TPAT brokers, C–TPAT NVOCCs etc, etc. While there are limits to how far C–TPAT can go as a voluntary program without binding requirements, it is a

good first step. C–TPAT recognizes that true security requires that the entire supply chain and all its component pieces be considered. For example, a seal on a container by itself is meaningless; it is an indicator of security only if it is part of a supply chain that is secure from the stuffing of the container through its final delivery.

The World Shipping Council has been engaged in detailed discussions with the Customs Service about the C–TPAT program, and while there is no ocean carrier component of the program yet in place, our members are hopeful of accomplishing that with Commissioner Bonner in the very near future.

Customs' CSI initiative is another very important initiative to address supply chain security, pursuant to which the Customs Service is seeking to enter into agreements with foreign governments and port authorities:

- establishing security criteria for identifying high-risk containers
- developing and implementing a pre-screening process to target containers before they are loaded aboard a vessel, and
- developing and deploying technology to screen and inspect identified containers prior to loading, including the stationing of Customs officials overseas in accordance with the principle of reciprocity.

Customs has entered into such agreements with Canada, Mexico, Singapore, the Netherlands, and Belgium, and is in the process of entering into agreements with several other European governments. Such arrangements provide a level of security capability and communication not otherwise easily achieved. The competencies and protocols that can emerge from CSI are essential to screen cargo before it is loaded aboard a vessel. This is especially important because secure intermodal supply chains will take considerable time to develop, and even then, the capability to check and inspect containers will be essential.

The CSI complements, but does not compete with, the international efforts being undertaken at the International Maritime Organization. The IMO is working to amend the existing international convention regulating ships in order to institute new vessel security requirements, and to develop a new international agreement to address physical security standards and requirements for port facilities. But by sharing cargo information and developing negotiated agreements for how cargo security can be monitored and verified, the CSI agreements fill a hole in current international cargo security capabilities.

Another aspect of such CSI agreements is that they are important to manage the continuation of trade if the industry is ever beset by a terrorist attack. Without such agreements and without the technology in place to inspect containers in ports of origin, what system would provide sufficient security confidence to keep international trade flowing following an incident? It would be difficult to over-emphasize the importance of this initiative and its urgency. Similarly, it must be recognized that CSI must not focus on just the largest ports around the world, otherwise terrorists would simply know that there is less risk of detection by using ports which are not among the largest.

*Cargo Documentation Requirements*

Beyond these Customs' initiatives, enhanced container security requires a clearly defined and coordinated government information system capable of receiving, analyzing and acting on data determined by the government to be necessary to screen shipments. Such data should be transmitted electronically and early enough to meet the government's needs. This requires enactment of the pending legislation and some clear direction to be provided. Because this remains one of the more complex and unresolved areas of the legislation, I would like to take a moment to address some of the questions involved, specifically:

- What information must be filed with the government?
- When must the information be filed?
- Who must file the information?
- What level of detail and accuracy is required?
- Who will analyze and act on the information?

*What information?*

We fully support the provisions of S.1214, which set forth thirteen specific items of information must be included on a cargo manifest, and urge that section 115(a)(2) of the Senate bill be retained in conference. Its clear enumeration of what is required will provide necessary clarity and uniformity.

The cargo manifest filed by a carrier was never designed to provide all the information that might be relevant to a security analysis, and it is not likely to ever do so, because that would require information beyond the knowledge of the carrier and

involve commercially sensitive information that shippers may not want to share with a carrier. We recognize, however, that until a new system is developed, cargo manifests will be the interim means to gather relevant information. We request, however, that cargo manifests not be perceived as the means to gather any and all information of interest, and that Customs be instructed not to require "additional" information on cargo manifests unless it is appropriate information to be provided to and by a carrier and is essential for security screening.

*When must the information be filed?*

Today, cargo manifests are not required to be filed until the vessel arrives in port, although for those carriers that file manifests electronically via Customs' Automated Manifest System, they file 48 hours before the vessel arrives. Both the House and Senate bills require that cargo manifests will be filed electronically in advance of arrival in such manner, time and form as the Customs Service requires. Customs officials have indicated that, when this bill is enacted, they intend to require carriers to file import cargo manifests 24 hours before loading in a foreign port. The logic of this is clear. If you want to perform a security screening of a container before it sails for the United States, you need the shipment information before loading.

This will be a substantial change for carriers and shippers, and it will affect how a lot of cargo is transported. Ocean carriers can accept such a requirement, but *only* if the requirement is applicable to *all* carriers equally, including non-vessel operating carriers. If this information serves a sufficiently important security function so as to be required earlier than today, then all carriers and all shipments must be required to comply with the same rules, or else the system will be both unfair and will provide inconsistent levels of security.

*Who must file?*

Ocean carriers are required by law to file cargo manifests for all cargo they transport. Nonvessel operating common carriers (NVOs), however,—which carry between 30–40-percent of the containerized cargo moving in U.S. foreign trades—are not currently required to file cargo manifests for the shipments for which they are responsible. NVOs are common carriers that purchase space from ocean carriers on a "wholesale" basis and then resell it to shippers on a "retail" basis. They issue the bills of lading to the shipper; they know the cargo descriptions; and they know the identity of the shipper and the consignee. Today, the only manifested information required for NVO-controlled containers is from the ocean carrier's manifest, which typically provides only a very limited cargo description (e.g., "freight all kinds" or FAK), and contains *no* information about the actual shippers or consignees of the cargo. Thus, the government has no advance visibility of cargo descriptions or, more importantly, the identity of the shippers or recipients of a huge percentage of our trade. A recent estimate, for example, was that from Hong Kong alone, over a quarter of a million "FAK" containers were sent to the U.S. last year.[4]

The House bill does not specifically require NVOs to file cargo manifests, whereas Section 115 (a) (3) in S. 1214 requires Customs to issue regulations requiring NVOs to meet the same cargo manifesting requirements as ocean carriers.

It is essential that the final legislation either require NVOs to file cargo manifests with the Customs Service for shipments for which they are responsible in the same time, manner and form as ocean carriers, or give this information to the ocean carrier to file with its manifest (an option that neither the NVOs nor the ocean carriers want). Without such a requirement, the government will have insufficient cargo descriptions and will have no advance information about the shippers or consignees of 30–40-percent of our imported ocean borne cargo. Without such a requirement, a shipper or consignee could conceal its identity from advance disclosure to the government by using an NVO rather than an ocean carrier to transport its goods. Furthermore, without such a requirement, the same shipment would be subject to less onerous security requirements if handled by an NVO than if handled by an ocean carrier. That would make no sense.

*What level of detail and accuracy?*

In modern ocean-borne transportation, the shipper is the party that provides the bill of lading information to the carrier. The carrier essentially transcribes the information into its system and issues a bill of lading on the carrier's form. Consequently, cargo documentation information is actually provided by the shipper.

Regarding the required level of detail of cargo manifest information, there is presently no common, agreed standard for what level of cargo description detail is need-

[4] Lloyd's List, June 21, 2002.

ed on the cargo manifest for security screening. Clear and uniform rules are needed to inform shippers what is required in the way of cargo descriptions. Recognizing that this early manifest filing is not needed or used for Customs entry or trade compliance purposes, such cargo description requirements should require only information that is needed for security purposes, and should not be so detailed as to impede the efficient flow of commerce.

Regarding the accuracy of the cargo description, the ocean carrier by necessity must rely on the shipper's declaration to the carrier of the cargo, because the carrier can't open and verify the contents of sealed containers or crates. While shippers are subject to penalties for inaccurate information filed for customs *entry* purposes—a process that is not required until after the goods arrive in the United States, existing customs law (Section 431 of the Tariff Act) does not clearly require the shipper of the cargo, who has the necessary cargo information, to provide complete and accurate cargo descriptions for the carrier's *cargo manifest*. In addition, the law's current penalty provisions (Section 436 of the Tariff Act) authorize penalties only on the *ocean carrier* in cases where the cargo description on the manifest is incomplete or inaccurate. This may have made sense in the pre-containerization days when the law was written and when carriers physically handled all the loaded cargo, but it is anachronistic and inappropriate when applied to cargo in sealed containers. With sealed containers, the ocean carrier by necessity must rely on the shipper's declaration to the carrier of the cargo because the carrier does not—and cannot—open and verify the contents of the sealed container.

In addition to being unfair, the current absence of clear statutory obligations fro shippers fails to ensure that the cargo interests, who possess the cargo information, have the proper incentives to provide accurate information that the government requires on the cargo manifest. We recommend that, if penalties are going to arise from inadequate cargo descriptions of cargo in sealed containers, then those penalties should be imposed on the cargo interests, not the ocean carrier which is simply transmitting what it has been told is in the container. The Tariff Act should be amended to make such penalty authority clear.

*Who will analyze and act on the information?*

The House bill (Section 101) would require the Under Secretary of Transportation Security to develop and maintain, by June 30, 2003, "a[n] antiterrorism cargo identification, tracking, and screening system for containerized cargo shipped to and from the United States either directly or via a foreign port".

The Senate bill appears to assume that cargo identification, tracking and screening for containerized shipments would continue to be the responsibility of the Customs Service. However, Section 207 of the bill also requires the Secretaries of Transportation and Treasury to "establish a joint task force to work with ocean shippers and ocean carriers in the development of systems to track data for shipments, containers and contents".

The lack of clarity over which agency is responsible for cargo security analysis should be clearly addressed by the conferees. It is essential that Congress: 1) clearly establish which agency is responsible for what portion of this security challenge, and 2) ensure that, if Customs is not the agency responsible for security analysis, then the lines of communications guarantee that identification of what cargo requires further review or inspection be communicated to the Customs Service in a timely manner. If the new regime is going to require substantial changes, such as filing import cargo manifests 24 hours before loading, then the security screening system must be able to analyze and act on the information before the cargo is loaded, or it will not accomplish its objective.

*Export Cargo Documentation*

Section 115(b) of the S.1214 would require shippers to "properly document" all export cargo, meaning submit a "complete set of shipping documents" "no later than 24 hours after the cargo is delivered to the marine terminal operator". The bill provides that carriers cannot load cargo aboard a ship unless it has been "properly documented". The House bill does not specifically address export cargo.

As you consider what requirements may be made applicable to export cargo, we request that you consider the following:

- The National Customs Brokers and Freight Forwarders Association has recommended that filing with the Automated Export System (AES) be made mandatory for all export shipments. We believe that this would facilitate government acquisition of export shipment data and simplify export procedures.
- Carriers should not be made responsible for whether a shipper has properly interpreted and applied export rules applicable to its cargo. For example, today

an export declaration may be required for a particular type of cargo, but not another.[5] The determination of whether a particular cargo requires an export declaration is an obligation of, and should be the sole responsibility of, the shipper.

- When complete documentation is required can significantly affect the flow and timeliness of commerce. For example, S.2534 would require exporters to provide a complete set of shipping documents 72 hours prior to departure of the vessel. That would require a large amount of cargo to just sit in a marine terminal for several days before loading. Such a requirement could cause delays to a significant amount of export trade and create congestion in marine terminals. S.1214 would allow shipments to be loaded for export if tendered just before loading so long as the documents were complete.[6]

IV. *The Role of Technology Improvements in Meeting the Security Challenge*

There is no question that technology can help address the security challenges. There is also no question that one must be careful not to assume technology can solve every security problem in a short time frame. The role of technology should be analyzed in the context of specific security challenges.

*Seals*

Today, there is no government standard for seals. A standard should be established promptly, which is internationally acceptable. We believe that in the immediate future, the standard should be for a hardened bolt-type seal. In the future, electronic seals may be required, but seal standards should not wait for the development, testing, and standard setting for electronic seals. Depending on the specific technology, electronic seals will also require different kinds of supporting infrastructure to be installed, such as readers at gates.

*Sensors*

There is interest in sensors that could be installed in containers to detect entry, and depending on the technology, perhaps even notify somebody of that entry. There are no commercially accepted or internationally accepted standards for such devices. Such devices also may require sophisticated supporting infrastructure depending on the type of sensor, such as satellite coverage. Finally, a requirement of such sensors is that they not be so costly as to be commercially impractical.

*Transponders on Ships*

The House bill (Section 107) would require the installation of Automated Identification System (AIS) transponders on any vessel built after December 31, 2002, on any vessel operating within a Vessel Traffic Service by that date, and on all other vessels, by December 31, 2004.

S.1214 does not have a comparable provision. However, S. 2329, which has been approved by the Senate Commerce Committee, would impose a requirement that AIS be installed by December 31, 2004, independently of when the vessel was built, or whether it was in a geography with a VTS system.

The IMO is presently addressing this issue, and we agree with the G8 Transportation Security Summit conclusion of last week that the IMO is the most appropriate forum to accelerate implementation of AIS equipment requirements. If accelerated installation of AIS equipment is nevertheless required by Congress, we believe the S.2329 approach and timeframe is preferable, as it coincides with the G8 agreement. In addition, the following clarifications are requested if this requirement is included in the final security legislation: 1) The AIS transponders are short-range (approximately 30 miles) transponders—as there are no standards for long-range equipment. 2) There is some uncertainty as to adequate availability of these transponders by the proposed date. It would therefore be appropriate to link the implementation of the installation requirement to a positive determination by the Secretary of Transportation that the AIS equipment will be reasonably available to install on all ships in international commerce. 3) Shore-based radio facilities, manned and operated by the Coast Guard, do not currently have the necessary equipment to receive AIS signals, obviously diminishing the value of AIS for enhanced maritime security. It would seem appropriate, therefore, to include in the legislation a

[5] This would not be the case if export declarations were required of all shipments.

[6] S.1214 requires for export shipments that all documents be submitted to the vessel common carrier or its agent "no later than 24 hours after the cargo is delivered to the marine terminal operator", and that no export container be loaded aboard a vessel unless this has been done. Thus a container could be delivered to the marine terminal the day the vessel sails and still be loaded aboard. (Section 115(b)).

requirement that the Secretary of Transportation provide regular progress reports to the relevant Congressional Committees on the planned installation of the necessary equipment on shore-based radio stations for receiving short-range AIS communication signals.

*Personnel Credentialing*

The issue of credentialing and checking transport workers in security sensitive positions requires resolution. The industry has expressed its support for the House and Senate legislative efforts to establish a national credentialing program, with uniform, minimum federal standards, with a federal background check process using criminal history and national security data, and with "smart card" technology for the credentialing of appropriate transportation workers. The credentialing system adopted should cover people with access to restricted marine terminal areas and to vessels, the truckers hauling the containers, and other security sensitive positions. America's seaports, like America's airports, should have systems to ensure and record that only approved people who are supposed to be there are there, and only when they are supposed to be there.

Regarding seafarers' documents, we were pleased to see the G8 Transport Security Summit agreement agree to seek by June 2003 minimum standards for issuance of seafarer identity documents at the International Labor Organization, and minimum standards for the application of biometrics in procedures and documents by the spring of 2003

*Cargo Inspection Technology*

The Customs Service is acquiring non-intrusive container inspection equipment for use at seaports around the country. These technologies are as important and useful as any in ensuring a secure supply chain, and such equipment should be installed at ports in other countries that load containers destined for the United States. This is an objective of the Customs Container Security Initiative.

We understand that other inspection and detection equipment is being deployed to check for certain risks, such as radioactive materials. These kinds of technologies should be among the highest priority acquisitions.

* * * * *

The challenges in developing and applying such technologies are many, but certainly include the following considerations. The first is internal to the government—clearly assigning organizational responsibility for developing and managing the process of reviewing all available technologies, setting criteria and standards for testing, judging the test results, and developing standards and requirements. A second challenge will be finding the right technologies for security at a reasonable cost. A third challenge will be making sure the standards and requirements are internationally accepted—an essential task when regulating international commerce, because the consequences of security requirements can affect equipment, systems, business practices and operating procedures around the world. Differing standards or disagreements could impede international commerce and cause substantial confusion.

*V. International Commerce Needs International Security Solutions*

A final point to consider is that ensuring higher security standards for international commerce requires international cooperation. Certain aspects of a security solution are beyond the direct reach of United States legislation. However, Congressional recognition and support of ongoing international efforts at the IMO, the ILO, the World Customs Organization and the G8 Summit is helpful.

First, S.1214 calls on the Secretary of Transportation, in consultation with the foreign governments concerned, to assess the effectiveness of the security measures maintained at foreign ports, by determining the extent to which a foreign port effectively maintains and implements internationally recognized security measures. This approach is consistent with and supportive of the U.S. government's international initiative to develop such standards at the International Maritime Organization, and with the G8 Transport Security summit agreement. We support this approach in the Senate bill, and believe that it should help further promote international cooperation in this area.

Second, the bilateral negotiations that are part of the Customs Service's Container Security Initiative are a critically important part of any security regime addressing the security of international cargo transportation. It will help detect and inspect security questions earlier, and will help governments manage the continuation of commerce under a wide range of security scenarios.

Finally, it is obvious, but worth repeating, that the hundreds of ships and millions of containers serving America's trade travel to and between all nations. This transportation network, that allows American exporters and importers to move their goods to and from any location in the world, must operate under rules that are internationally acceptable.

*VIII. Moving Forward*

I would like to close my remarks by thanking the Committee for its leadership in addressing this issue. S.1214 was conceived before September 11. The Senate passed it during the last session. The Committee's continued perseverance on the issue is instrumental in making progress on an exceptionally difficult challenge. Your efforts are one of the reasons to be encouraged, if not by the present state of success, at least by the efforts and positive direction things are moving.

I would also be remiss if I did not express thanks to the Committee for listening to all parts of the industry so that you understand and appreciate the consequences of the actions being considered. It is essential that maritime security legislation be enacted this year. It is also critical that the legislation and its implementation not unduly handicap commerce. International liner shipping is remarkably successful in providing America's international trade with efficient, reliable and low cost service. Great care should be taken to preserve those attributes at the same time that we improve security measures against the risk of terrorism.

We can't always choose the circumstances in which we find ourselves, but we can choose how we respond to those circumstances. Governments are now engaged in an exceptionally difficult endeavor, namely to institute safeguards against the risk of terrorism while protecting the benefits of free trade. It is essential that governments succeed. It is incumbent on all the participants in this international transportation process to help governments succeed. The World Shipping Council is committed to helping the Congress and the Executive Branch agencies succeed in these efforts, and we commend those in industry and in public service who are doing their best to address this new and complex set of challenges.

---

*Attachment A*

## Member Companies of the World Shipping Council

APL
A.P. Moller-Maersk Sealand—(including Safmarine)
Atlantic Container Line (ACL)
CP Ships—(including Canada Maritime, CAST, Lykes Lines, Contship Containerlines, TMM Lines, and ANZDL)
China Ocean Shipping Company (COSCO)
China Shipping Group
CMA–CGM Group
Compania Sud-Americana de Vapores (CSAV)
Crowley Maritime Corporation
Evergreen Marine Corporation—(including Lloyd Triestino)
Gearbulk Ltd.
Great White Fleet
Hamburg Sud—(including Columbus Line and Alianca)
Hanjin Shipping Company
Hapag-Lloyd Container Line
HUAL
Hyundai Merchant Marine Company
Italia Line
Kawasaki Kisen Kaisha Ltd. (K Line)
Malaysia International Shipping Corporation (MISC)
Mediterranean Shipping Company
Mitsui O.S.K. Lines
NYK Line
Orient Overseas Container Line, Ltd. (OOCL)
P&O Nedlloyd Limited—(including Farrell Lines)
Torm Lines
United Arab Shipping Company
Wan Hai Lines Ltd.
Wallenius Wilhelmsen Lines
Yangming Marine Transport Corporation

Zim Israel Navigation Company

Senator WYDEN. Mr. Schorer?

**STATEMENT OF STEVEN SCHORER, PRESIDENT, L–3 COMMUNICATIONS, OCEAN SYSTEMS DIVISION**

Mr. SCHORER. It is always great to be last. Chairman Wyden, Senator Murray and Senator Cantwell, it is a pleasure to be here. I am Steve Schorer of L–3 Communications, Ocean Systems Division.

While a lot of the time today has been spent on cargo vessels and containers tracking and tags, I would argue that the threat today includes everything from huge container ships to small pleasure boats. Thousands of water craft operate in our Nation's inland waterways as well as in our traditional ocean side harbors, making cities like Minneapolis and St. Louis as vulnerable to attack as New York and Seattle.

The sheer number of vessels involved makes it almost impossible for the Coast Guard or the port authority to reasonably be expected to stop all potential terrorist activities using conventional methods. There have been recent reports in the press indicating Al-Qaeda are training in underwater operations, which lends an even greater sense of urgency to resolving this complicated issue.

Much of the current discussion today centers around the threat of a terrorist organization smuggling in weapons or detonating explosives, conventional or unconventional in cargo containers, cargo vessels. A much more practical or realistic threat involves the threat posed by underwater mines or explosives placed at the access to a harbor, a choke point, on a pier's pilings, or on a pipeline running across the sea floor. Virtually any vessel, not just a cargo vessel, operating in our waters can covertly deploy mines. An enemy might not deploy his mines or explosives from a submarine or an aircraft, but instead could simply push them off the back of a pleasure craft or a freighter in the dark of the night.

Mines are easy to build, inexpensive and readily available worldwide. A typical mine, like the widely exported Italian Manta is a anti-ship mine, commercially available, easy to deploy and very difficult to detect. The Manta comes with a 290-pound warhead that could easily sink any of today's commercial cargo ships. Furthermore, the appearance of a mine in one harbor not only shuts down commercial activity in the affected port like Seattle, but could require examination of all other U.S. ports like L.A., New York, et cetera, and waterways to ensure that they are mine-free before normal activity reassumes.

Mine clearance becomes a particularly onerous problem when you consider the vast majority of the U.S. Navy's mine warfare equipment is located in Ingleside, Texas. The transit time alone which could be on the order of two weeks from Texas to Seattle would result in an unacceptable delay in reopening the port for commerce. Once on station, some estimates indicate it could take as long as 3 weeks to conduct mine hunting operations in New York harbor alone. In comparison, it seems a much more complex problem. A 2 to 5 week shutdown with any of our major ports would have a devastating economic impact.

The key to isolating newly planted objects in a harbor or waterway is knowing what is already there. Most harbor bottoms contain large amounts of junk, debris, trucks, cars, things you would not imagine are in the bottom of this harbor, and the clutter rates are excessive. This might include tires, making the job of locating newly implanted objects like mines extremely difficult.

Traditionally, our Navy, the U.S. Navy has conducted Q-Route surveys in military ports to locate and map objects on the bottom of a channel or operating area in peace time, so that in a heightened alert or wartime, they can go back and look at the same area and note the differences between the two surveys. Hence, focus on the new information, something that is newly implanted. In the presence of a threat, this enables them to quickly eliminate known objects and focus their attention on new mine-like contacts for neutralization. This an exceptional capability. However, is it extremely limited due to the size of the U.S. Navy's mine countermeasure force, their geographic location, as I said in Ingleside, Texas, and the fact that many of the assets are forward deployed for identification overseas in areas of conflict.

To effectively counter the threat posed by an underwater attack to our ports and infrastructure requires dedicated assets and an ongoing, nearly continuous survey effort. In my view, the United States must intensify and broaden its conduct of what I will call civilian Q-Route surveys in our major ports and waterways to enable us to quickly recover from the mining of any port or harbor.

I would offer the following as one possible concept of operations employing of use of sidescan sonar to conduct Q-route surveys in our ports and waterways. I believe every major port authority in the U.S. should conduct a detailed initial survey to actually locate and plot bottoms, to locate and plot objects on the harbor approaches, shipping lanes and channel bottoms. The result of this survey should be stored in the national computer database which all future surveys could be compared to, thereby enabling port authorities to determine the appearance of new and potentially hostile objects.

The survey system must be able to provide sufficient resolution to eliminate having to investigate every oil drum, debris, car, whatever piece of junk lies on the bottom today during a survey. The number of surveys conducted is largely dependent on the size of the search area and the number of the search assets available. While a harbor the size of Seattle seems formidable, the search area is actually somewhat more manageable since you are primarily concerned with the shipping lanes and choke points. Once a suspicious object is located, the port authority could isolate the affected area until it was cleared.

This problem of searching a large volume of water in the ocean as a medium is much more different than in air. To search that volume of water in a very short period of time requires an extremely sophisticated underwater surveying equipment. The system must possess the ability to resolve very small targets in the ocean and accurately identify those with almost photographic image quality.

Today, L–3 Ocean Systems produces such a high-resolution sidescan sonar. The system is presently in use with the Canadian Navy and was successfully used to locate SwissAir Flight 111, and

this was, this was a crash site that no one else could find the aircraft. The U.S. Navy had assets on station. The Canada Navy had assets on station. No one could find that plane.

So in summary, our Nation's ports are vulnerable to terrorist activity, and my opinion it is just a matter of time before a terrorist brings the war on terror to our shoreline. A single mine in a U.S. harbor could have a devastating social and economic effect. The approach I have proposed today is not a panacea for the defense of our harbors, but only serves as one strand in an overarching security net we must construct to counter the threat posed by an enemy waging an unconventional war against us. I have provided written testimony which further expands on this, and I thank you for the opportunity to be here.

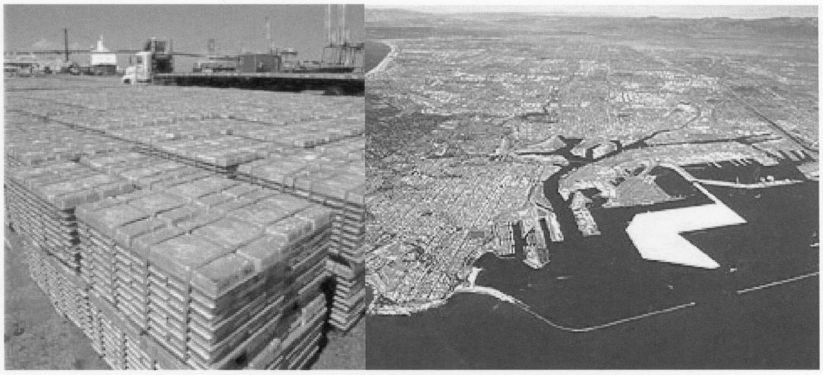
[The prepared statement of Mr. Schorer follows:]

PREPARED STATEMENT OF STEVEN SCHORER, PRESIDENT, L–3 COMMUNICATIONS, OCEAN SYSTEMS DIVISION

Good afternoon Senator Wyden, Senator Murray, Senator Cantwell and members of the Port Authority. I am Steven Schorer, President of L–3 Communications, Ocean Systems Division. Ocean Systems is a world leader in underwater detection technologies both domestically and internationally.

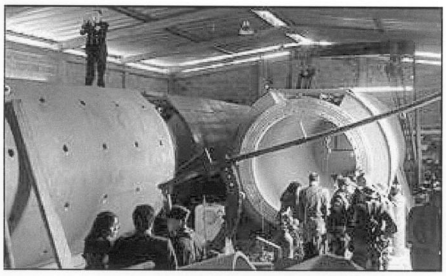
The tragic events of 9–11 serve to illustrate the unconventional nature of the war we now find ourselves fighting and the pressing need to examine other potential vulnerabilities inherent in a free and open society. I applaud the Committee's and the Port Authority's actions today to bring into open discussion a critical element in any Homeland Defense strategy. While significant attention is now being focused on making the Nation's skyways safe, too little attention has been given to our relatively unprotected and open ports and harbors. Commerce is the lifeblood of our Nation and economy, but just as the terrorists used our own aircraft against us, they have the capability to exploit commercial shipping in similar and unimaginable ways.

The threat today includes everything from huge container ships to small sailboats. Thousands of watercraft operate in our Nation's inland waterways, as well as in our traditional ocean side harbors, making cities like Minneapolis and St. Louis as vulnerable to attack as New York and Seattle. A major port like the Port of Los Angeles handles over 110 million metric revenue tons a year with cargo value exceeding $120 billion. Yesterday alone, over 100 container ships entered Los Angeles Harbor.



$120 Billion of Cargo flows through Los Angeles Port Alone

The sheer numbers of vessels involved makes its almost impossible for the Coast Guard or Port Authority to reasonably be expected to stop all potential terrorist activities using conventional methods. There have been recent reports in the press indicating the Al-Qaeda terrorists are training in underwater operations, which lends an even greater sense of urgency to resolving this complicated issue. Small diesel submarines are widely available for purchase in the international marketplace and, as recently demonstrated in Columbia, submarines can be constructed by virtually any industrial facility for non-military uses.



Confiscated Columbian Drug Submarine

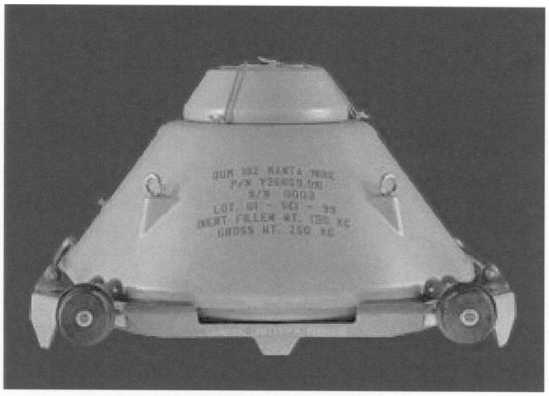
Used Russian Submarine

Merchant Vessels

Pleasure Craft

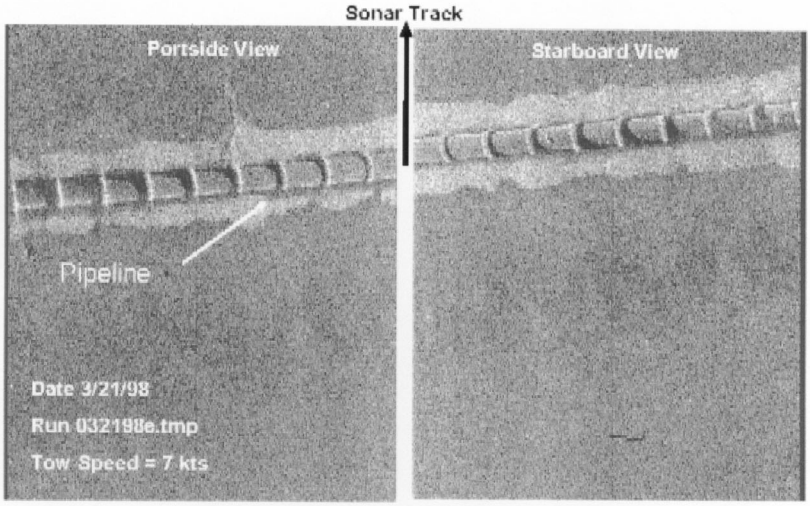
Much of the current discussion in the press centers around the threat of a terrorist organization smuggling in weapons or detonating explosives, conventional or unconventional, in a major city's port. The ensuing loss of life and disruption in commerce would have far reaching and possibly long lasting implications for our

country. However this discussion seems to ignore other, equally devastating, scenarios. One example of this would involve the threat posed by underwater mines or explosives placed at the access to a harbor, in a choke point, on a pier's pilings or on a pipeline or cableway running across the sea floor. Virtually any vessel operating in our waters can covertly deploy mines. They are easy to build, inexpensive and readily available worldwide. A typical mine like the widely exported Italian Manta is a lethal anti-ship mine which is widely available, easy to deploy very difficult to detect.



**Manta Mine**

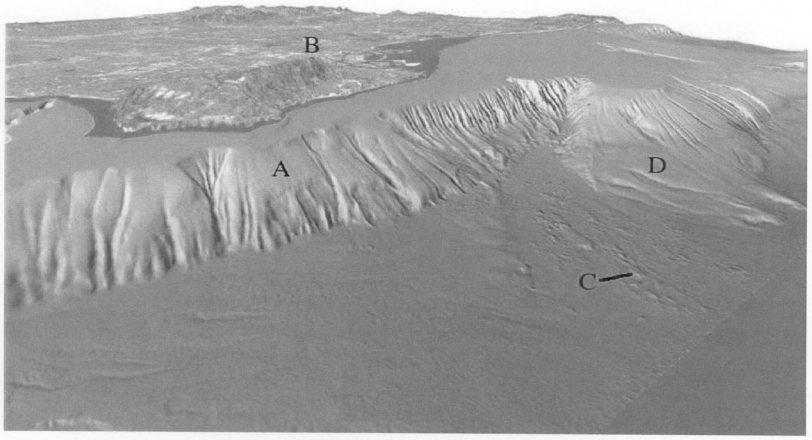
The Manta is a shallow water mine with a 290 lb warhead that could easily sink any of today's commercial cargo ships. The appearance of a mine in one harbor not only shuts down commercial activities in the affected port, but it requires an examination of all other ports and waterways to ensure they are mine-free before normal activities can resume. Communication and electrical cables, sewage lines, oil pipelines and bridge pilings are all possible targets for attack.




**Pipeline on bottom of Los Angeles Harbor**

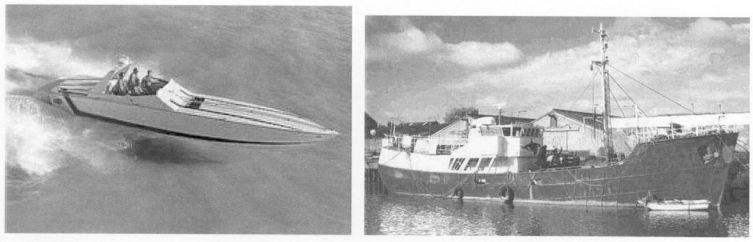
Mine clearance becomes a particularly onerous problem when you consider the vast majority of the US Navy's mine warfare equipment is located in Ingleside, Texas. The transit time alone (2 weeks) from Texas to Seattle would result in an

unacceptable delay in re-opening the port for commerce. Once on station, some estimates indicate it could take as long as three weeks to conduct mine-hunting operations in New York Harbor alone. To complicate matters further, the undersea environment poses some unique challenges not encountered in surface based surveillance methods. Detection and detection ranges are affected by numerous, constantly changing, variables such as bottom type and contour, salinity, temperature gradients, water depth and ambient noise levels.



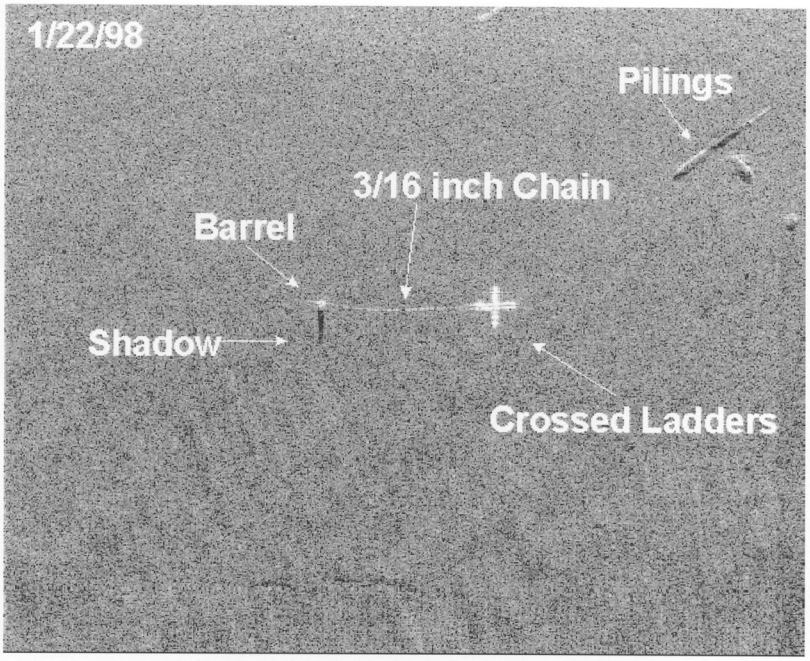

**Los Angeles Harbor Approach Presents a Difficult Set of Terrain and Oceanographic Complexities**

Historically, the perceived mining threat was from an enemy intent on bottling up the US Navy or merchant Fleets in time of war—today's threat is no different. What is different is that the enemy might not deploy his mines or explosives from a submarine or aircraft, but instead could simply push them off the back of a pleasure craft or freighter in the dark of night. It is reasonable to expect that an enemy intent on disrupting port operations could attach an explosive device to the bottom of an oil tanker or large merchant ship as well.

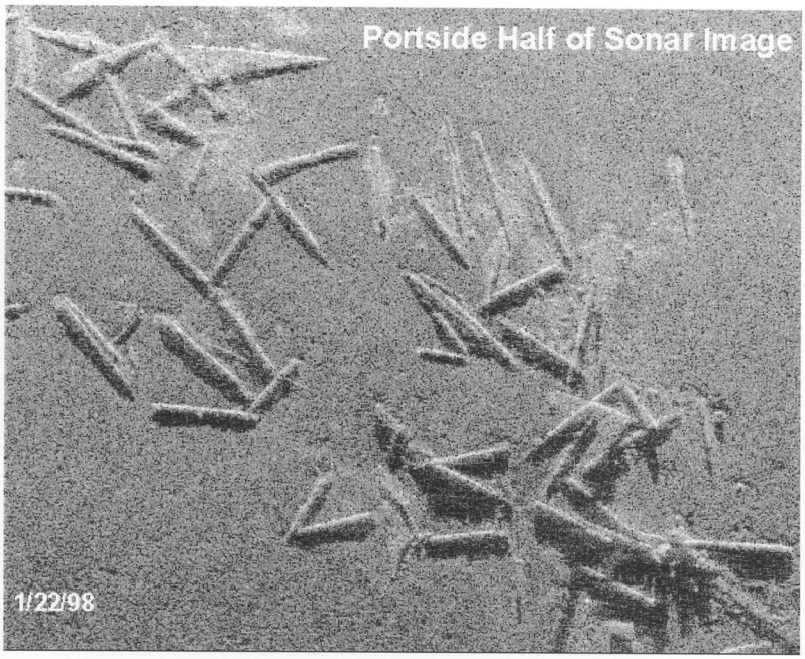


**Commercially Available Cigarette Boats and Small Merchant Ships Could Provide a Covert Means of Mining Ports**

The key to isolating newly planted objects in a harbor or waterway is knowing what is already there. Most harbor bottoms contain a fair amount of existing debris; things like cars, refrigerators, 55-gallon drums and the like, all appear on a sonar operator's screen and make the job of locating new objects more difficult.



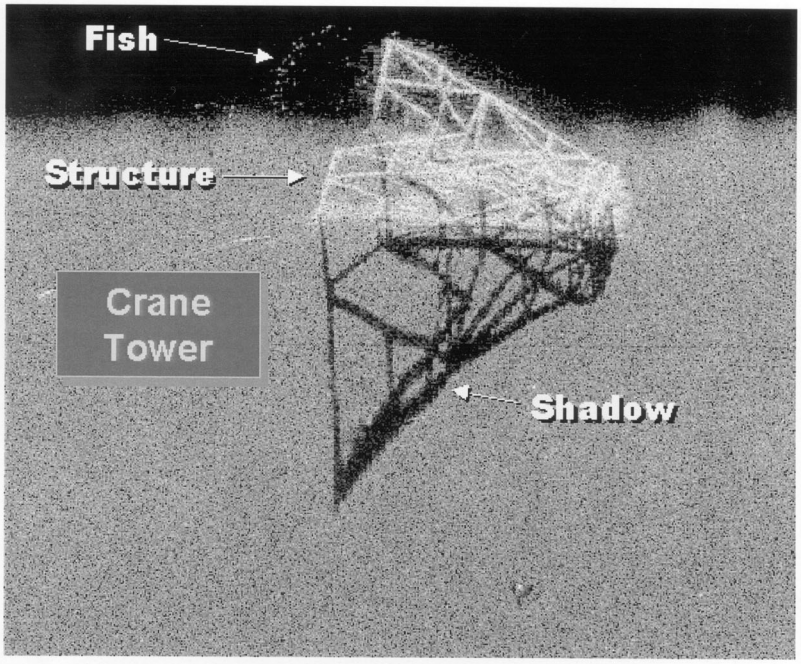

Typical Debris on Harbor Bottom




**Pilings Scattered on Harbor Bottom**

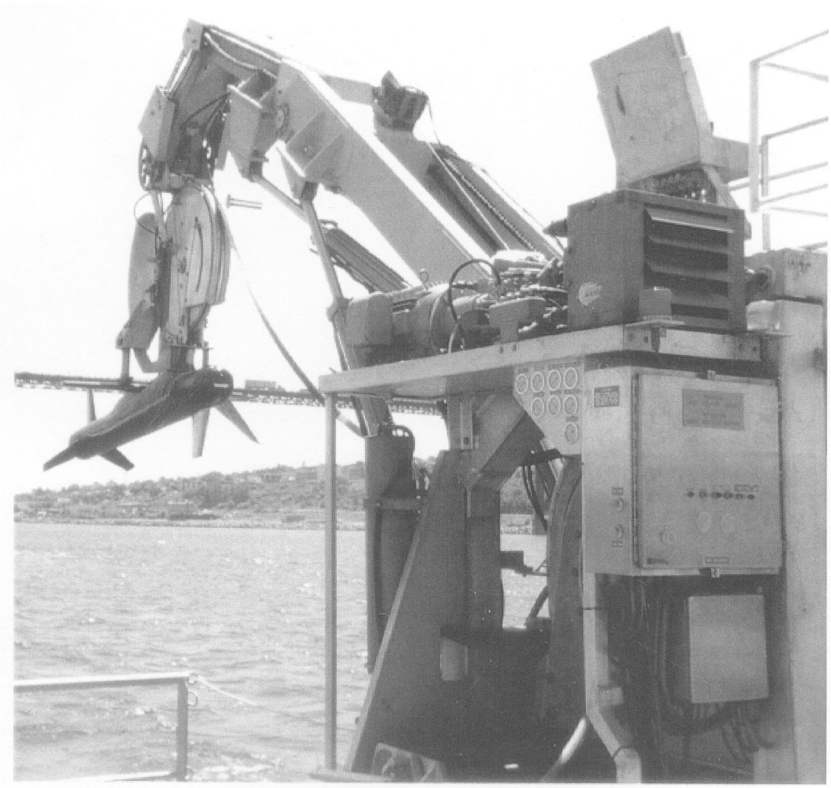
Traditionally, the US Navy has conducted Q-Route surveys in military ports to locate and map objects on the bottom of a channel or operating area (OPAREA) in peacetime, so that in wartime they can look at the same area and note the differences between the two surveys. In the presence of a threat, this enables them to quickly eliminate known objects and to focus their attention on new mine-like contacts for further investigation and neutralization. This is an exceptional capability, however it is extremely limited due to the size of our mine countermeasures force, their geographic location, and that many of the assets are forward deployed supporting international operations. The Navy uses specially designed and equipped ships of the MCM and MHC classes to conduct these surveys, in addition to limited helicopter borne search assets. While the sonars used aboard these ships and aircraft are good, they do not provide the kind of photographic resolutions necessary for use in harbor defense. To effectively counter the threat posed by an underwater attack to our ports and infrastructure requires dedicated assets and an on-going, nearly continuous, survey effort. Furthermore, this survey must encompass more than just shipping channels, but must also look at other potential underwater targets. In my view, the United States must intensify and broaden its conduct of civilian q-route surveys in our major ports and waterways to enable us to quickly recover from the mining of a harbor. Since 9–11, the Canadian Navy has plans to conduct this type of survey of the Saint Lawrence River and most, if not all, Canadian ports.

The problem of searching a large volume of water in a short period of time requires the use of extremely sophisticated underwater surveying equipment. The system must possess exceptional resolution under a variety of water conditions, depths and sea states for the accurate identification of targets. Resolution must be such that a detected object's geographic location is accurately plotted on a chart to facilitate removal or further investigation by other assets—this degree of accuracy is not typically available in commercial sonars. Additionally, the equipment operator must be able visually identify the detected object to eliminate false targets and to effectively coordinate removal activities.




**Clearly Identifiable Tower Structure on the Bottom**

The system must be user friendly enough to require minimal operator training, and should be easily deployable from existing vessels rather than requiring the construction of a dedicated search platform. Given the large size of many of our harbors, the system must also provide the user with a high rate of search coverage.



**Side Scan Sonar Installed**

I would offer the following as one possible concept of operations employing the use of a sidescan sonar to conduct commercial Q-Route surveys and to perform periodic surveillance to detect mines or other suspicious devices in our waterways. Upon acquisition of a suitable system, the port authority would conduct a detailed initial survey to accurately locate and plot objects on the harbor or channel bottom. The results of this survey are then stored in a national computer database to which all other surveys will be compared to, thereby enabling port authority officials to determine the appearance of new, potentially hostile, objects. As I previously stated, the system used must be able to provide sufficient resolution to eliminate having to investigate every coffee can or car detected during the survey. Additional surveys can be then conducted to rapidly identify objects requiring further investigation. The number of surveys conducted is largely dependent on the size of the search area and the number of search assets available. While a harbor the size of Los Angeles, New York, or Seattle seems formidable, the search area is actually somewhat more manageable since you are primarily concerned with the shipping lanes, choke points, cable and pipeline crossings and waterfront approaches. Additionally, survey assets can be deployed to specific locations in response to a treat or to reports from surface based observers. Once a suspicious object is located, the port authority can isolate the affected area until the object can be visually identified, removed or neutralized.

L–3 Ocean Systems currently produces a high-resolution sidescan sonar system with the ability to locate and display objects as small as a piece of 3/16's inch chain with nearly photographic imagery. All of the sonar images in this presentation are taken from unretouched raw sonar output. The system is presently in use by the Canadian Navy and was successfully used in locating and mapping the wreckage of SwissAir flight 111 that crashed off the coast of Halifax on September 2, 1998. The L–3 sidescan sonar system provides a credible, near-term, solution to closing one area of port vulnerability in our Homeland Defense strategy.

Since most modern sea mines are designed specifically to reduce sonar reflectivity, the L–3OS side scan sonar system possesses a high shadow contrast ratio allowing the operator to determine the shape, size, and orientation of underwater objects. Positional accuracy of plotted contacts is approximately three meters RMS, which enables rapid reacquisition of the contact for further investigation or removal. The system is easily installed on the stern of virtually any surface ship, but for port operations it would ideally be placed on a harbor craft of 100 tons or greater. The system is capable of search speeds of up to 10 knots and, due to its superior detection ability, resolution, increased range and accuracy, its search area coverage is equivalent to that of many airborne sonar systems towed at 25 knots. It uses an automatically stabilized towed body with motion compensated beam steering coupled with a motion compensated handling system. This design results in a system capable of effective operations in up to Sea State 4, which translates into wave heights of approximately 6 to 7.5 feet.

The threat to our Nation's ports is real. In my opinion it is just a matter of time before a terrorist group exploits this vulnerability and once again brings the war on terror to our shoreline. We must act proactively to avoid another 9–11 style attack on America. The approach I have proposed today is not a panacea for the defense of our harbors, but only serves as one strand in the overarching security net we must construct to counter the threat posed by an enemy waging an unconventional war against us. I have provided the Committee with a copy of the detailed performance specifications and capabilities of the L–3 sidescan sonar system. I thank the Committee for giving me the opportunity to address this important issue.

Senator WYDEN. Senator Murray?

Senator MURRAY. Mr. Chairman, I think this panel has really shown us why the complex problem of seaport security has been one the TSA has sort of hunted on and focused on, and this is a very complex and challenging problem, and each one of you focused on a different area, and I am just curious, Mr. Verma and Mr. Cushing, you both talked about technology, truckers and the information. How do you talk to each other? Is this information compatible? Mr. Schorer?

Mr. VERMA. I think we just started. I think eModal is an information layer. We are much more at the data gathering. I think Senator Cantwell asked the question how do you make sure whether the containers have been opened. We will have the manifest of

the carrier, and then, you know, push that information either into eModal or PORTNET®, which basically does the information layer on top of that. Robert talked about this layer. We are the background layer which is just the container security layer.

Mr. CUSHING. By trade, I am not a techie, but since getting involved in this, I can tell you ever since I have got involved in it, there is talk about standards, and every time someone comes up with a standard, somebody else comes up with a new standard. Right now we are working with 46 marine terminals. They are all sending us their data, and what we do is provide them a map and say this is how we need to receive it. They talk to each other. They do. You know, will we ever get another standard, you know, spend a billion dollars? This is going to do an XML.

We are in an industry that is not that advanced. Admittedly, the transportation industry is not the most technically savvy group, and we admit it, and that is, my background is transportation, and we are not all that technical, but we can make these things work, and these two do talk to each other.

Senator MURRAY. And I am assuming that you are also saying that, does the United States need to move forward with that standard first, or should we wait for the IMO, and if the U.S. comes forward with one, will the rest of the international community come forward?

Mr. CUSHING. As soon as my mike is on, I will go. By standards, yeah, the procedural, I think we just need to get going in the United States. For example, in the various ports, people are submitting their security plans by terminal, and they are wondering what will be acceptable and what will not. Just set up some standards.

Senator MURRAY. Will the rest of the international——

Mr. VERMA. It is a combination of things. You have to do standards in conjunction with everything else, but industry if it starts moving, de facto standards are a whole lot more effective than in facto. Seventy percent of ocean cargo is in the hands of a limited number, three, four port operators, and so if you get those guys, three, four, five critical major port operators, you get started and make sure that you keep working with the IMO.

But we are finding that there is a lot of incentive to move forward, because these port operators are concerned, because if what happened to the airport network (Network) ever happened to the ports, you are talking significant losses to all these people. That is why the grading system is a good idea, so they get differentian, and by the way, what we are finding is that several of them have started talking to each other. It is not about technology, really. I think somebody, Chris, I think, talked about it.

A reader in Rotterdam has to be able to be the same; or the reader in Singapore has to be the same as the reader in Seattle. If you get that, and if you find that the majority of the ports are in the hands of four or five or six people that start working together to make it happen.

Senator MURRAY. Thank you very much to all of you. Thank you, Mr. Chairman.

Senator WYDEN. Senator Cantwell?

Senator CANTWELL. Thank you, Mr. Chairman.

Mr. Verma, I think your testimony must have had one of the most significant lines of anything that we have heard this afternoon, and I think summarizes the challenge that we are facing in Washington, D.C., when you say that with respect to technology given the asymmetrical nature of conflict, we need to employ technology that is a high-tech means to prevent low-tech attacks.

Mr. VERMA. Correct.

Senator CANTWELL. How do we get that understanding into the decision making process of Washington, D.C.? For agencies who are multilayered, may not have the same kind of CEOs on board within the various agencies that understand those choices?

Mr. VERMA. That is a great question. It is a standard technology adoption problem that I think you face in the high-tech industry all the time. I think candidly Washington is no different.

Senator CANTWELL. A slow adapter is what you are saying?

Mr. VERMA. Exactly. They tend to be the laggeres in technology, but I think this is one of those things where there has to be a large degree of business process plus technology to come up with a complete, comprehensive solution, and we need a critical mass of people to go in there and say here is the way that we are going to proceed. We will start this thing. We will start moving. We will assure these certain requirements that you have, and we want to help you observe it, and we want to help grow it, but we want your support. I think one of the things that Chris faces, once some of these systems start to be deployed, you want to make sure that the guys who are the entrepreneurs are not punished, and if you start to get a much better security coming out of certain ports or certain shippers, you need to make sure that there is some benefits to these guys, whether it be a grading system——

Senator CANTWELL. Let us try to categorize it, then, because you are saying, you know, high-tech means for low-tech attacks, which I think certainly crystallizes the challenge given that you know so much of what our organizations were as far as information processing, focused on a superpower and analyzing what that superpower might do, and now we are talking about lots of networks all over the world, and so we have to get the FBI to get rid of seven layers and all of that, but in the system, you were critical, now then go to this approach that this is the problem, the thing that we know best. Go out and do some pilot programs and tell us in two years.

Mr. VERMA. Three years and 5 billion dollars later, I am sure we will have a system.

Senator CANTWELL. But no attacks during that period?

Mr. VERMA. That is my point. My point is I think to some extent what you have to do is use existing technology. It may not be a hundred percent——

Senator CANTWELL. My question then is this, from what perspective, what do you think the timeline of deployment of an international system should be? What do you think, knowing what we know today, what do you think the real timeline is if bureaucracy was not the issue? What really could we guarantee to the American people would be the timeline for the deployment of this system?

Mr. VERMA. Six to 9 months.

Senator CANTWELL. How do we get there then?

Mr. VERMA. We will talk to you in about a week and a half, if you have got a critical mass of players, we are going to start putting our own nickel in and start building a system, and we will work with a lot of you folks and get moving on it, work with all of you to make sure that this is consistent with what we are trying to achieve, we will build more on that.

Senator CANTWELL. Mr. Koch, what do you think of that? Given that your, obviously, council members are people like United Arab Shipping Company, and Italia Line and all over, all over the world? Do you think that they would participate in that process, be behind the deployment of these international standards, working with their governments? Do you think that they are the vehicle or do you think it is more us putting on pressure to go and negotiate these agreements with these various companies?

Mr. KOCH. I think the industry is already participating and will continue to participate in these ventures, including Operation Safe Commerce, and I think what the industry really is looking for is an answer to the problem. Nobody wants to figure out how to deal with this more than our industry, because we do not want to be the conduit or the vehicle by which terrorists attack the United States or any of the economies in the world right now.

I think the difficulty for the industry is as was stated earlier. Unless everybody has to do it, there is really no way to ensure security. Unless there are requirements that are understood and enforced. If we want to make progress on this, if you want to change people's commercial behaviors, it has got to be by requirements that are internationally understood.

And the other point I would make is that the technology solutions always tends to sound simple but be the most confusing, the most difficult to get resolution on.

We should not lose sight of the fact there are technologies that can be and are being deployed, such as Customs container inspection technology. Those are critical technologies. He said we have a plan to have 139 pieces of equipment in U.S. ports, but for the CSI initiative which is being rolled out to be in foreign ports, where is the equipment in the foreign port? We need to make sure that we are applying these technologies in the places that they need to be. We also need a process to develop, test and gain agreed standards for new technologies and seal standards. The industry is perfectly willing to support such efforts, with the obvious caveat that we want to know what it is going to cost. If sensors and seals end up costing as much as a container, it is going to be a big problem.

Senator CANTWELL. We will, but I think our interrogation of Al-Qaeda prisoners, and their revelation about possible underwater attacks on ports is no different than the Special Agent Crowley memo or the Phoenix memo. It is a piece of information talking about intent, and so we need to change the 3 to 5 years to the 6 to 9 months.

Mr. VERMA. Absolutely.

Senator CANTWELL. And standardization seems to be the key in doing that, and so we are just going to have to figure, I applaud the business community if they will stand up and help drive that, because they obviously can move faster. They helped make that standardization happen. We push the governments to agree, but

you know, we are not going to stop at government level in pushing it as well, but to me that seems to be the critical challenge that we are facing.

Thank you, Mr. Chairman.

Senator WYDEN. Thank you, Senator Cantwell, and your expertise on all these technology issues is enormously helpful.

I think, gentlemen, you all have been far too diplomatic in terms of characterizing Government's approach on this. I am chair for the Merchant Marine Subcommittee today, but I chair the Technology Subcommittee of the Commerce Committee, and I was struck in particular after 9–11, thousands of ideas were sent by technology companies to Washington, D.C. for products in this area, security, underwater technology and the like, and the Federal Government was simply unable to even consider them. I mean simply unable to even have any sort of process for a test bed or any kind of analytical capability. It really is a disgrace.

I think you all have been very diplomatic, and I am going to be less so, and I have said as Chairman of the Technology Subcommittee, we are going to set up a one-stop process so that when technology leaders and entrepreneurs and companies have promising ideas, you will be able to go to one place in the Federal Government, and they will tell you, look, it is Commerce that needs your ideas. It is Customs that needs your idea, and I just want to restate the pledge, if I have an ounce of breath in my body at the time we consider that legislation, we are going to make that possible.

Now, I think the other troubling thing about this is not only does the Federal Government not have a way to evaluate what you all bring them, they are really dawdling in terms of going out to you, and this seems to me to be pretty baffling as well. You have the law enforcement and the intelligence agencies, NSA, for example, talk about candor, last week said we are just light years behind the private sector.

This a dramatic change from the Cold War and others where Government would lead, and now the Government is just admitting that they are sort of Luddites. They are just sort of behind the times and cannot keep up, and to me your point, Mr. Cushing, with respect to the amount of paper that flows in the customs field strikes me as sort of a classic case of instead of you having to come to your Government in order to put in place this new kind of system, your Government ought to be coming to you and saying, Look, we want to figure out a way to promote security while at the same time not having people traipse all over the countryside trying to get things processed and having paper and the like.

And I would just be kind of curious whether you all can give us some instances where the Government was presently proactive instead of you having to come and, you know, pull them kicking and screaming to go along with any of these ideas. Are there any ideas where the Government——

Mr. VERMA. Can I take the Fifth? Not that we know of.

Senator WYDEN. Again, we are going to try, and Senator Murray with her influence in the Appropriations Committee and Senator Murray with all of her years in the technology field, we are going to try to make the Government, we are going to try to make a 180

degree about-face on this issue, try an approach in technology where they are proactive, where people who admit that they are light years behind are actually proactive and coming to you on things like digital certificates and some of your proposals, and I gather that again, Mr. Verma, you take the Fifth Amendment on that question. Are there any kind of instances where the Government has been proactive in coming to you?

Mr. SCHORER. You know, I will add the system that I talked about, we developed for the Canadian Navy. The Canadian Navy has this capability and has this ability on the St. Lawrence River and all their ports and harbors, but trying to sell that idea—and until the balloon goes up, no one is going to care—but that capability in the U.S. Navy has been extremely difficult, because it is real, it is not seen as a high priority item today. So I cannot say that the community is receptive to these ideas, but I will say that there are many navys and countries taking it very seriously, but I do not find it in the United States.

Senator WYDEN. Well, one last thought by way of an invitation. We got out of the Commerce Committee two significant bills in the technology area that I think will be part of the technology package that the Senate will cover in the fall. One is the cyber security, and the other is legislation that I developed to set up a way the Federal Government would look to private companies to help respond in a disaster and also give suggestions as how to prevent them.

Let me just close the hearing by saying that we would welcome your ideas and suggestions now about this technology package. We think it will go to the floor of the Senate in the fall. I want to let my colleagues wrap up if they have any additional comments.

Senator CANTWELL. I just want to say, Mr. Chairman, thank you for coming here and conducting this hearing. I know that you are having a similar hearing in Portland tomorrow. It is critically important I think that the people understand the West Coast dynamics are part industry, and that we do have competition from Vancouver, and if we do not get this figured out, we will have someone who will take advantage of that in short order.

That is critically important, and that we obviously need to get the word back from Washington, and we appreciate you again doing this, because I know this will be officially part of the record and will be information that will flow to all members that we need to expedite that process that is happening, you know, in some ways with Singapore as an individual organization, but in a much more comprehensive way with the West Coast and Asia will be a primary focus for us on the West Coast, and we appreciate you being here today in Seattle, and I know that working with my colleague, Senator Murray in the various Committees, and we are glad to have another West Coast member join us in that and appreciate what the Commerce Committee can do in bringing about a quick timeframe for dealing with this issue.

Senator WYDEN. Thank you for your expertise on all these issues, Senator.

Senator MURRAY. Mr. Chairman, just let me thank you and all of our witnesses for coming today, and I really appreciate Senator Cantwell and her commercial background, and Senator Wyden, you have been wonderful in working with us here as we work.

As Chair of the Transportation Appropriations Subcommittee, I do not have a blank checkbook with me, and we do have a lot of challenges in this year's Transportation committee. We do need to address the issue of port security and work together to be able to deal with the funding that we have available. So thank you very much.

Senator WYDEN. With that, we are adjourned.

[Whereupon at 5:30 p.m. the hearing was adjourned.]

○