S. HRG. 107–855

SECURING OUR PORTS AGAINST TERROR: TECHNOLOGY, RESOURCES, AND HOMELAND DEFENSE

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

FEBRUARY 26, 2002

Serial No. J–107–61

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

85–082 PDF WASHINGTON : 2003

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

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

EDWARD M. KENNEDY, Massachusetts	ORRIN G. HATCH, Utah
JOSEPH R. BIDEN, JR., Delaware	STROM THURMOND, South Carolina
HERBERT KOHL, Wisconsin	CHARLES E. GRASSLEY, Iowa
DIANNE FEINSTEIN, California	ARLEN SPECTER, Pennsylvania
RUSSELL D. FEINGOLD, Wisconsin	JON KYL, Arizona
CHARLES E. SCHUMER, New York	MIKE DEWINE, Ohio
RICHARD J. DURBIN, Illinois	JEFF SESSIONS, Alabama
MARIA CANTWELL, Washington	SAM BROWNBACK, Kansas
JOHN EDWARDS, North Carolina	MITCH MCCONNELL, Kentucky

BRUCE A. COHEN, *Majority Chief Counsel and Staff Director*
SHARON PROST, *Minority Chief Counsel*
MAKAN DELRAHIM, *Minority Staff Director*

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION

DIANNE FEINSTEIN, California, *Chairperson*

JOSEPH R. BIDEN, JR., Delaware	JON KYL, Arizona
HERBERT KOHL, Wisconsin	MIKE DEWINE, Ohio
MARIA CANTWELL, Washington	JEFF SESSIONS, Alabama
JOHN EDWARDS, North Carolina	MITCH MCCONNELL, Kentucky

DAVID HANTMAN, *Majority Chief Counsel*
STEPHEN HIGGINS, *Minority Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Cantwell, Hon. Maria, a U.S. Senator from the State of Washington	70
Feinstein, Hon. Dianne, a U.S. Senator from the State of California	1
Kyl, Hon. Jon, a U.S. Senator from the State of Arizona	14
Schumer, Hon. Charles E., a U.S. Senator from the State of New York	3

WITNESSES

DeBusk, F. Amanda, former Assistant Secretary for Export Enforcement, Department of Commerce, and former Commissioner, Interagency Commission on Crime and Security in U.S. Seaports, Washington, D.C.	30
Petersen, Kim E., Executive Director, Maritime Security Council, Fort Lauderdale, Florida	35
Quartel, Rob, Chairman and CEO, FreightDesk Technologies, Inc., and former Member, United States Federal Maritime Commission, McClean, Virginia	39
Schubert, William G., Maritime Administrator, Department of Transportation, Washington, D.C.	4
Steinke, Richard D., Chairman of the Board, American Association of Port Authorities, and Executive Director, Port of Long Beach, Long Beach, California	27
Tischler, Bonni, Assistant Commissioner, Office of Field Operations, United States Customs Service, Washington, D.C.	11
Upchurch, Charles W., President and CEO, SGS Global Trade Solutions, Inc., and Representative, Global Alliance for Trade Efficiency, New York, New York	57
Venuto, Kenneth T., Rear Admiral, Director of Operations Policy, United States Coast Guard, Washington, D.C.	15

SUBMISSIONS FOR THE RECORD

Advanced Research and Applications Corporation, R.A. Armistead, President and CEO, Sunnyvale, California, statement	67
International Microwave Corporation, Anthony Acri, Chief Executive Officer, East Norwalk, Connecticut, statement	71
Nacht, Michael, Dean and Professor of Public Policy, Goldman School of Public Policy, University of California, Berkeley, Berkeley, California, statement	72
Port of Oakland, Oakland, California, statement	75
Science Applications International Corporation, John H. Warner, Jr., Corporate Executive Vice President and Director, and James Winso, Corporate Vice President, General Manager Security Products, San Diego, California, statement	77

SECURING OUR PORTS AGAINST TERROR: TECHNOLOGY, RESOURCES, AND HOMELAND DEFENSE

TUESDAY, FEBRUARY 26, 2002

UNITED STATES SENATE,
SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The committee met, pursuant to notice, at 3:24 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Dianne Feinstein, chairperson of the subcommittee, presiding.

Present: Senators Feinstein, Schumer, and Kyl.

OPENING STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Chairperson FEINSTEIN. I would like to open this hearing and particularly thank our witnesses for coming. I will introduce them in a moment.

Senator Kyl, the ranking member, with whom I have the great pleasure of working, is at the White House and will be along, but will be a little late. And so in the interest of time, I thought we might begin this.

I would like to begin by just making a brief statement. A while ago, in this committee while we were considering the PATRIOT Act and the Attorney General John Ashcroft was making a presentation, he held up a copy of the Al-Qaeda terrorist handbook. And one part of that was on recruiting. Now, this is a translation, but I just want to read one paragraph.

"Recruit people carefully because such activities could lead to death or arrest. Most likely candidates are smugglers, the needy, those seeking political asylum, adventurers, workers at coffee shops, restaurants, and hotels, and workers at borders, airports, and seaports."

And it is the last word really that we are here to discuss today. Seaports are often out of the public eye, but they are a very critical and important part of economic activity. Ninety percent of cargo moves by container, and much of that is stacked stories high on huge ships.

Each year, 200 million containers move between ports, making this the most important and critical part of global trade. Our nation's seaports handle 95 percent of U.S. trade with non-contiguous

countries, meaning non-connecting countries—big words—and this trade is expected to triple in the next 15 to 20 years.

Now, a lot of this growth is going to occur in my home State, California, and we boast two of the busiest seaports in the Nation: Los Angeles/Long Beach and Oakland in the San Francisco Bay Area.

While seaports are essential hubs of commerce and transportation, they are also plagued with serious problems, and that is what we are here today to discuss and see what we might be able to do about it.

Our seaports today are extremely vulnerable to terrorism. Drug trafficking, alien smuggling, export of stolen automobiles, and international cargo theft are rampant. Yet in spite of the fact that the major problems besetting seaports all fall within the traditional jurisdiction of United States law enforcement, no Federal agency currently has comprehensive authority to regulate activity at seaports. That is point No. 1.

So, in a nutshell, I believe that many of the problems at seaports are really due to insufficient Federal oversight and the lack of personnel and technology. I know that Senators Hollings and Graham, of Florida, have introduced legislation to help solve these problems, and that legislation has passed the Senate. But there is much more that we can do to ensure the safety and integrity of our seaports and the communities that typically surround them.

Let me give you an example. Last October, Rizik Amid Farid, an Egyptian and suspected Al-Qaeda member, was found in a container aboard a vessel bound for Canada. The container also had a bed, toilet, portable heater, and water supply for the 3-week trip. Farid also had a Canadian passport, global satellite phone, cell phone, laptop computer, various cameras, identification documents, airport maps, an airline mechanic's certificate, and security passes for airports in Canada, Thailand, and Egypt.

He was found during a routine inspection by Italian authorities while the ship was at dock in southern Italy. Farid is suspected of being a senior Al-Qaeda member because the operation to smuggle him into Canada was obviously expensive and well organized.

One wonders whether other Farids have managed to come into North America through seaports. Due to short staffing and limited technology, inspectors today look at only 1 or 2 percent of containers; 98 to 99 percent are just waved through. Hence, virtually every time a ship docks, the only people who know what is on a container are the people who shipped it, maybe, and the people picking it up, maybe. And if those people are terrorists, they are free to ship munitions and weapons overseas to their compatriots or even set off a bomb, or even sleepers themselves.

So we are here today to hear from some very critical people who are very knowledgeable with respect to our seaports, and this committee is particularly looking for good ideas which can stand the test of time, are practical and doable, and so that we might put together a piece of legislation to improve the situation.

I would like now to introduce our first panel.

Captain William Schubert, United States Department of Transportation. Captain Schubert is the Department of Transportation's Maritime Administrator. He was recently confirmed last November.

He is a former maritime industry consultant and maritime industry official. He has over 27 years of professional maritime experience.

I will just mention the three of you, and then we will go right down the line, if this is all right.

Bonni Tischler is from the United States Customs Service. She is the Assistant Commissioner to the Office of Field Operations of the United States Customs Service. She is the first woman to hold that position. She is directly responsible for trade compliance, antismuggling, outbound and passenger operations, 20 Customs management centers, and 300 ports of entry. She also manages an annual operating budget of approximately $1 billion and the operations of more than 12,000 employees.

And, finally on this panel, Rear Admiral Kenneth Venuto, United States Coast Guard. Rear Admiral Kenneth Venuto is the Director of Operations Policy for the United States Coast Guard. As Director, he maintains management oversight of a wide range of programs supporting the Coast Guard's five strategic goals: maritime safety, mobility, maritime security, protection of natural resources, and, finally, national defense.

So that is our first panel, and if we may, Mr. Schubert, may we begin with you please. Welcome.

Captain SCHUBERT. Thank you, and good afternoon. Madam Chair, with your permission, I would like to submit my written comments for the record, and I have some brief comments to make.

Chairperson FEINSTEIN. May I ask you to hold up?

Captain SCHUBERT. Sure.

Chairperson FEINSTEIN. Because this might even get his vote on something, if I let him speak right now.

[Laughter.]

Senator SCHUMER. Dianne always gets my vote on whatever she wants.

Chairperson FEINSTEIN. I would like to acknowledge the senior Senator from New York, Chuck Schumer, to make a statement.

STATEMENT OF HON. CHARLES E. SCHUMER, A U.S. SENATOR FROM THE STATE OF NEW YORK

Senator SCHUMER. Well, thank you, Senator Feinstein. I very much appreciate your holding this important hearing. As the person who represents the largest ports on the West Coast and I represent the largest port on the East Coast, obviously we both have an interest in this. It is extremely timely. It is extremely important, and I want to thank the witnesses for coming. This is an issue of great concern to many, many New Yorkers and certainly to me, and your taking the leadership on this issue is wonderful.

I would ask that my entire statement be read into the record and just make a couple of brief points.

I guess what I would say is I have a fear greater than just about any other, and that is that someone will use our ports and bring a nuclear weapon through a container. The bomb in Hiroshima was a very simple device. It was two chunks of high-grade uranium, weapons grade, at opposite ends of a tube. And what the bomb did is, when it was detonated, all it did is slam those two chunks of

uranium together, creating what physicists call a critical mass of uranium, and the nuclear explosion ensued.

You don't need an airplane to deliver that kind of a bomb. You don't need a missile. You can put it in a container, send it by ship, and create huge, huge havoc—or on a truck, for that matter.

And so we have a big job ahead of us because how can we not do everything we can to stop that from happening and at the same time make sure that our ports continue to be able to flow commerce. You know, we could inspect every container hand-to-hand, and the ports would be backed up all the way from Los Angeles to Tokyo or New York to London.

So we have to do a lot. I support the Hollings bill, but I think we have to go further, and I think this hearing is so important because it highlights attention.

The bill that I am planning to introduce soon—and I hope we could debate it at some point—would first mandate that all ports in the U.S. that receive international cargo have the capability to inspect and span up to 10 percent of the containers entering the port. That means we would provide each port in the Nation with enough Customs inspectors and scanning machines to inspect up to 10 percent. Right now it is less than 3.

Second, we would create a new research and development fund to develop new technologies related to port security. We need to be able to know that every container is safe.

And, third, there are a lot of loopholes that remain in port security infrastructure. The Hollings bill closes some. Our bill closes others.

I think our first step is to support the Hollings bill and then to move forward, and, Madam Chairwoman, I look forward to working with you and salute your leadership on this issue so we can make our ports safe.

And with that I would just ask unanimous consent that my entire statement be read in the record.

Chairperson FEINSTEIN. Absolutely.

Thank you very much, Senator Schumer. I look forward to working with you, and, you know, I think we should have a hearing in this committee if your bill comes to this committee, and also we will have some of the questions hopefully that I have and you have answered today by some of the experts, and we might even be able to add to it as well. So thank you very much. I appreciate it.

And I appreciate the courtesy of you and the witnesses because of the schedule.

Chairperson FEINSTEIN. Happy to do it.

Senator SCHUMER. Thanks.

Chairperson FEINSTEIN. Captain Schubert, please.

STATEMENT OF WILLIAM G. SCHUBERT, MARITIME ADMINISTRATOR, DEPARTMENT OF TRANSPORTATION, WASHINGTON, D.C.

Captain SCHUBERT. Thank you. Madam Chair, good afternoon again, and with your permission, I would like my written statement submitted for the record.

Chairperson FEINSTEIN. So ordered.

Captain SCHUBERT. And I have some brief comments.

I am Captain William Schubert, Maritime Administrator, and I am pleased to be here today to address the important issue of port security on behalf of the Department of Transportation.

The Department of Transportation has always sought to maintain secure transportation within every mode. We continue to do so today with greater sense of urgency and direction through the newly created Transportation Security Agency, or TSA.

My own agency, the Maritime Administration, has historically played a critical role in port development and security. One of our duties has been to provide security guidance to the commercial ports in the U.S. and coordinate Government and maritime stakeholders in their security efforts. MARAD co-chaired the Presidential Commission on Crime and Security in U.S. Seaports, and as Chair of the National Port Readiness Network, MARAD plays a lead role with the military in assuring port security and protection of critical infrastructure during a mobilization.

Today, I would like to address several recent developments led by Secretary Mineta in the area of port security in which DOT has been actively involved—grants for the improvement of port infrastructure, cargo and container security, credentialing for transportation workers, and the availability of maritime insurance against terrorism-related losses. Admiral Venuto will then brief the committee on specific Coast Guard initiatives to secure our ports and protect shipping.

As you know, the Department of Defense Appropriations Act for fiscal year 2003 appropriated $93.3 million to the Transportation Security Agency to award competitive grants to critical national seaports to help finance the cost of enhancing port facility security. Such grants are to be awarded based on security assessments as determined by the Under Secretary of Transportation for Security, the Administrator of the Maritime Administration, and the Commandant of the Coast Guard.

Discussions between TSA, MARAD, and the Coast Guard resulted in an agreement that MARAD and the Coast Guard would work cooperatively on behalf of TSA to administer the emergency seaport security funding contained in the act. Secretary Mineta has just approved our implementation plan. We will soon begin to award grants based on the most urgent homeland security needs. Preference will be given to ports that have already begun demonstrated port security enhancements.

Madam Chair, if you are interested, during the question-and-answer period, I do have a brief overview of how that grant program will be administered, if you are interested.

Chairperson FEINSTEIN. I am very interested. If you want to go into it now, please feel free to.

Captain SCHUBERT. Sure. We do have handouts of this chart.

When this Department of Defense appropriation of $93.3 million came about, we at the Coast Guard and the Maritime Administration and the TSA worked diligently to put together a plan of implementation to award these grants. We recognized that the grants were done on an emergency basis or to handle on a priority basis things that would be considered urgent for port security.

So with that in mind, we have come up with this time line of which we are already past the decision memo, which has been ap-

proved by the Secretary, the selection outline, which has also been completed, and we have drafted a broad agency announcement which will be released tomorrow to the public.

After tomorrow, we will have approximately a 20-day application period. We have developed a way that applications can be filed and submitted over the Internet without any paper or time loss.

Chairperson FEINSTEIN. By port authorities?

Captain SCHUBERT. Port authorities would be eligible to submit an application in this process, yes, ma'am.

We also will furnish the committee, if you would like, a copy of the broad agency announcement once it is released tomorrow.

After a 20-day application period, all the applications are due on March 27th. The Maritime Administration regional directors and primarily the captains of the port, which will really have the final say-so, will review these applications on a regional basis and prioritize them.

Then after that happens, headquarters will review and prioritize those applications. That will take approximately 25 days. And then the recommendation will be forthcoming, and the selection board, which will be myself, the Commandant, and a representative from TSA, will review the recommendations. And if everything goes correctly by June 11th, the grants will be awarded.

I will also add that we have targeted approximately 10 percent of the $93.2 million will go towards proof-of-concept type of applications. These would be not research and development so much, but for the implementation technology that might not have been used before.

Chairperson FEINSTEIN. Thanks very much.

Captain SCHUBERT. The events of September 11th have highlighted the vulnerability of our international container shipments to acts of terrorism, with more than 12 million TEUs arriving on our shores yearly. Prior to September 11th, the Department's primary concern was the efficient movement of these containers through the transportation system. Clearly, the advent of just-in-time business processes and the use of the transportation system as a rolling inventory has tied the marine transportation system to the economic vitality of this country.

It only follows that a serious disruption of this system could have devastating effects on our economy. In recognition of this fact, the Department established an interagency Container Working Group in December to make system improvement recommendations through a well-honed security lens, balancing national security interests with economic efficiency.

Another area of concern is the issue of identifying and credentialing employees who have access to ships, ports, terminals, and cargos. This includes everyone from the point of origin to the ultimate destination. As a result, the Department established a Credentialing Direct Action Group, known as a CDAG, co-chaired by MARAD, to examine the feasibility of an identification card for all transportation workers and other persons who require access to secure areas of transportation facilities.

The primary goal of the CDAG is to fashion a nationwide security program that verifies the identity of transportation workers, validates their background information, assists transportation fa-

cilities in managing their security risk, and accounts for personal access to transportation facilities and activities of authorized personnel.

This has been a joint public-private effort. The CDAG has made a concerted effort to seek out the advice of transportation experts in devising this program. They understand that industry support is key to the success of this effort.

My last point concerns the availability of insurance for terrorism risk in the maritime industry. For ships generally, the market is providing insurance against losses from terrorist attacks. But the cost of insurance has escalated 200 to 300 percent since 9/11. For cruise ships, the cost is up 1,000 percent. Even as premiums were going up, however, the insured loss coverage was reduced by underwriters.

Turning to land-based assets, like buildings and ports, the news is very different. Reinsurance renewals fell due on January 1st, and reinsurers excluded terrorist risk. Such coverage is available from primary insurers, but coverage is very limited, and the cost is prohibitive.

The Department of Transportation does not need to be convinced that port security is a good idea. We have recognized it as a critical component of our maritime industry and our national security for many years. Nevertheless, achieving appropriate levels of security in our seaports and seeking to educate our international partners as to the need and benefits of seaport security is no small undertaking.

DOT is aggressively pursuing all aspects of transportation security in all modes, utilizing our own resources and tapping the best minds in the industry and labor. We look forward to working with you and the Members of Congress to protect our citizens and grow the economy.

I want to thank you again for inviting me here today, and now I would be happy to answer any questions you or other—well, no other committee members are here. Thank you.

[The prepared statement of Captain Schubert follows:]

STATEMENT OF WILLIAM G. SCHUBERT, MARITIME ADMINISTRATOR, UNITED STATES DEPARTMENT OF TRANSPORTATION

Good Afternoon Madam Chairman and members of the Subcommittee. I am Captain William G. Schubert, Maritime Administrator. I am pleased to be here today to address the important issue of seaport security on behalf of the Department of Transportation.

The Department of Transportation (DOT) has always sought to maintain secure transportation within every mode. We continue to do so with a greater sense of urgency and with more focus through the newly created Transportation Security Administration.

My own agency, the Maritime Administration (MARAD), has always played a critical role in port security. One of our duties is to provide port security guidance to the commercial ports in the United States and to coordinate government and commercial port stakeholders in their security efforts. MARAD Co-Chaired the Presidential Commission on Crime and Security in U.S. Seaports, and, as Chair of the National Port Readiness Network, plays a lead role with the military in assuring port security and protection of critical infrastructure during mobilization. We have developed an Inter-American Port Security Training Program in which nearly 300 port personnel have been trained in the Western Hemisphere, and the Merchant Marine Academy at Kings Point provides security training to industry. We have also been working with the port community to advance uses of technology that have posi-

tive security benefits both within the port and through its landside intermodal connections. I welcome the opportunity to continue our efforts to improve port security.

Today, I would like to address several recent developments led by Secretary Mineta in the area of port security in which DOT has been actively involved—grants for the improvement of port infrastructure, cargo and container security, credentialing for transportation workers and the availability of maritime insurance against terrorism-related losses. Admiral Venuto will then brief the Committee on specific Coast Guard initiatives to secure our ports and protect shipping.

GRANT PROGRAM FOR IMPROVEMENT OF PORT INFRASTRUCTURE

As you know, the Department of Defense Appropriations Act for FY 2002 (Act) appropriated $93.3 million to the Transportation Security Administration (TSA) to award competitive grants to critical national seaports to finance the cost of enhancing facility and operational security. Such grants are to be awarded based on the need for security assessments and enhancements as determined by the Under Secretary of Transportation for Security, the Administrator of the Maritime Administration, and the Commandant of the Coast Guard (USCG).

Discussions among TSA, MARAD, and the USCG resulted in agreement that MARAD and the USCG would work cooperatively, on behalf of TSA, to administer the emergency seaport security funding contained in the Act. MARAD and the USCG have met, and we expect final approval of our implementation plan very quickly.

MARAD and USCG will act as "agents" of TSA for the distribution of grants from the $93.3 M appropriation. The final grant approval body will be a board consisting of the Under Secretary of Transportation for Security, myself as Administrator of the Maritime Administration, and the Commandant of the Coast Guard, or our representatives. Determination of grant awards will be based on consideration of the most urgent needs from a homeland security perspective. It is anticipated that initial awards will commence in June 2002. We are moving very quickly to put this money to work.

We intend to use a small amount of this money to fund "proof of concept projects"; we will focus on critical seaports. Preference will also be given to ports that have already begun port security enhancement through some demonstrated action.

CARGO AND CONTAINER SECURITY

An analysis of our transportation system in the aftermath of the events of September 11, 2001 clearly laid bare the susceptibility of container shipments as a delivery system for an enemy's weapons, with over 12 million TEU's/year arriving at our shores. Prior to September 11th, from a DOT perspective, our primary concern was the efficient movement of these containers through the transportation system. The advent of just-in-time business processes and the use of the transportation system as a rolling inventory tied the transportation system even more integrally into the economic vitality of this country.

In order to address the security issues surrounding the movement of marine cargo containers through the international, intermodal transportation system, an interagency Container Working Group was established in December 2001. The effort is co-chaired by the Departments of Transportation and Treasury (U.S. Customs). The Container Working Group's activities are focused in four subgroups: Information Technology, Security Technologies, Business Practices, and International Affairs. Just this month, the Working Group provided recommendations to the Office of Homeland Security on Ensuring the Security of Cargo Container Transportation. Recommendations addressed improving the coordination of government and business efforts as they relate to container security; enhancing data collection; improving the physical security of containers; initiating activities on the international front; and considering all possible uses of advanced technologies to improve the profiling of containers and to increase the physical security of containers.

Even with our best efforts, our current transportation system is groaning under capacity constraints and congestion in many ports is increasing. To further complicate matters, container traffic, even with the current economic slowdown, is predicted to double in the next twenty years. Improving efficiency is one of the key ways to help solve these capacity and congestion problems. Yet efficiency improvements must now be looked at through a security lens. Our transportation system will need to operate both efficiently and securely. These twin goals of efficiency and security need to be addressed simultaneously.

We are working jointly with U.S. Customs, exporters, importers, carriers, and governments to establish business and security practices which will push the nation's virtual borders outward to the point of loading of the containers. Security must be

established before the vessel carrying the container or cargo begins its international travel. Technology and information are also essential to container security. For that reason, we strongly support the accelerated implementation of the U.S. Customs ACE and Integrated Trade Data System (ITDS) to bring it online as quickly as possible.

CREDENTIALING FOR TRANSPORTATION WORKERS

Security background checks and credentialing of all who move or have access to cargoes has never been more important. This includes everyone from facilities and conveyances to the destination warehouse. Thus, the Department established an interagency "Credentialing Direct Action Group" (CDAG), co-chaired by MARAD, to examine the feasibility and process for conducting background checks and issuing an identification card for all transportation workers and other persons who require access to secure areas of transportation facilities.

The primary goal of the CDAG is to fashion a nationwide transportation worker identity solution that verifies the identity of transportation workers, validates their background information, assists transportation facilities in managing their security risks, and accounts for personnel access to transportation facilities and activities of authorized personnel. The CDAG is primarily concerned with private-sector transportation workers, and has held numerous meetings that have included many representatives from the transportation industry and transportation labor. Such outreach efforts are necessary. They are experts in transportation, and we have found they are anxious to contribute their knowledge to solving the difficult issues surrounding personnel identification. We are building industry buy-in at the front end to ensure the success of this effort.

The most difficult issue is to define the appropriate levels of security for the broad spectrum of transportation facilities and operations and how these should be applied. There have also been some concerns regarding the anticipated background check process. Various models are being investigated by several groups to try and improve responsiveness, lower cost and improve consistency over present practices for credentialing. We also face the privacy issues presented by the collection and maintenance of databases containing personal information.

The CDAG has already developed a functional requirements document, which identifies the principal attributes that a credentialing system must have to achieve the interoperability necessary to reach across the transportation industries. This document has been shared with many of the major transportation industry associations. They have begun to provide their comments.

Under a maritime cooperative program called the Ship Operations Cooperative Program (SOCP) that is administered by the Maritime Administration, industry, in partnership with multiple government agencies, is currently working to evaluate and test a Mariner Administrative Smart Card credentialing system to reduce fraud, track mariner training, facilitate shipboard sign on/sign off and enhance shipboard security. The Smart Card Administrative Project started in October of 2000 and is a 50/50 cost sharing initiative between the 43-member SOCP and the Maritime Administration.

As a result of the September 11, 2001 events, added emphases within the project are being placed on the potential of smart card applications for addressing security concerns. Members of the cooperative including MARAD and USCG are engaged internationally with the International Maritime Organization, International Labor Organization, International Transport Workers' Federation and others to discuss security and credentialing issues. In addition, SOCP is coordinating with DOT entities that are currently working maritime security issues to ensure the project is in line with currently discussed directions. SOCP is working closely within DOT, and with other agencies including the General Services Administration, to ensure interoperability through standardization. This project has the potential for demonstrating the effectiveness of smart card technology to improve efficiency, reduce fraud and increase security in the maritime industry.

INSURANCE AGAINST TERRORISM-RELATED LOSSES

The Merchant Marine Act, 1936 (Act), authorizes the Secretary of Transportation to ensure the availability of adequate insurance for vessels engaged in the waterborne commerce of the United States. This authority, delegated to MARAD, provides coverage for vessels, their cargoes, crews, and third-party liabilities against war risks, including acts of terrorism, if commercial insurance is not available on reasonable terms and conditions. The insurance may be made available to both U.S. and foreign flag vessels.

There are two basic forms of war risk insurance. Section 1202 of the Act addresses commercial vessels in commercial trade while, Section 1205 pertains to vessels that are under charter or in the employ of the Department of Defense. Recently, President Bush authorized DOT to provide war risk insurance under Section 1202. The insurance is available for areas currently excluded in commercial war risk trading warranties: the Persian or Arabian Gulf and adjacent waters, Israel, Lebanon, Gulf of Aqaba and the Red Sea, Yemen, Pakistan, Oman, Syria, and Egypt. Authority under Section 1205 for the Middle East has remained in effect since it was authorized by Then-President Bush in August 1990. Since February 20, 2002, MARAD has written Section 1205 insurance on five vessels in the employ of the Military Sealift Command.

Although the combined losses arising out of the attacks of September 11th are estimated in the tens of billions of dollars, we are seeing an excellent response all across the insurance industry in responding to the coverage of these losses. While the losses are of catastrophic proportions, the industry is financially sound and most property/casualty insurers are highly reinsured with major reinsurers with excellent reserves.

The insurance industry has taken a major hit as a result of September 11th events and what we are seeing is a major restructuring of terrorism risks. Many primary property/casualty insurance coverages, which would include port infrastructure, had reinsurance renewals on January 1st of this year and it appears that most reinsurers have excluded terrorism risks from their renewal coverage. A few major primary insurers are offering to write terrorism risks on fixed property, but with very limited cover (up to $50 million on some risks) at very, very high premiums. As a result of this, we have been advised by a number of insurance brokers and underwriters that upon insurance renewal many companies and properties are underinsured or uninsured for terrorism risks.

The situation is somewhat better with regard to vessel insurance, where terrorism risks are generally covered under the war risk policy. Terrorism coverage is still available for vessels and cargoes, but the cost has increased significantly. For example, war risk underwriters issued cancellation notices on war risk policies on all vessels worldwide on September 19th, (which they were permitted to do under their seven-day cancellation clauses). They reinstated these policies on September 26th with increases of annual premium of 200 to 300 percent on most fleets, except for cruise vessels, which we understand faced a 1,000 percent increase in annual premiums. In addition, war risk underwriters published new excluded zones, extending from Egypt to Pakistan, where vessels and cargoes may not enter without paying thousands or even hundreds of thousands of dollars of additional premium. Marine war risk/terrorism insurance is still available from the commercial market, although at much higher premium rates and with much more limited coverage on the liability side since September 11th. The Protection and Indemnity Clubs, a mutual arrangement of shipowners, which provide vessel liability coverage, now limit coverage for terrorism risk as of February 20th to $200 million per vessel—an amount far lower than previously. Vessels and cargoes are still moving worldwide, but the cost is higher and the terms more limited. In addition, we understand that one of the mutual clubs that provides insurance for terminals, stevedores, port authorities and transport and logistics companies for handling equipment and property was able to reinstate terrorism cover as of February 1st, but it is not clear on what terms or cost.

In summary, insurance covering risks of terrorism is still in a state of flux and we expect this to continue for some time to come.

CONCLUSION

The Department of Transportation does not need to be convinced that port security is a good idea. We have recognized it as a critical component of our maritime industry and our national security for many years. Nevertheless, achieving appropriate levels of security in our seaports and seeking to educate our international partners as to the need and benefits of seaport security is no small undertaking. DOT is aggressively pursuing all aspects of transportation security in all modes utilizing our own resources and tapping the best minds in the industry and labor.

I would be happy to answer any questions you or the other Committee members may have.

Chairperson FEINSTEIN. Thanks very much, Captain Schubert, and we will do the questions after we hear from the other two witnesses.

Next is Ms. Tischler. Welcome.

STATEMENT OF BONNI TISCHLER, ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, UNITED STATES CUSTOMS SERVICE, WASHINGTON, D.C.

Ms. TISCHLER. Madam Chairwoman, thank you for your invitation to testify before the subcommittee today. I bring you Commissioner Bonner's regards and his apologies. We have appropriations hearings tomorrow, and he is up to his eyebrows in alligators. But he does extend our invitation to you to visit with us, perhaps, at your convenience in one of the ports in California, and you can see firsthand how we target seaport cargo.

Since September 11th, Commissioner Bonner's top priority for the Customs Service has been responding to the terrorist threat at our land borders, seaports, and airports. His highest priority is doing everything we can reasonably and responsibly to keep terrorists and terrorist weapons from entering the U.S. Our Customs inspectors, canine enforcement officers, and special agents are doing just that: protecting and defending our country against the terrorist threat at all of our ports of entry.

Since September 11th, Customs has been at a Level 1 alert across the U.S. at all border entry points. Level 1 requires sustained, intensive anti-terrorist questioning and includes increased inspections of travelers and goods at every port of entry. Because there is a continued threat that international terrorists might attack again, we remain at Level 1 alert to this very day, and we will be doing a Level 1 alert for the foreseeable future.

Commissioner Bonner has implemented around-the-clock coverage by at least two armed Customs officers at every Customs location, even at low-volume crossings along our Northern border. Customs inspectors are in many places working 12 to 16 hours a day, 6 and 7 days a week.

To help ensure that Customs develops a coordinated, integrated counterterrorism strategy for border security, Commissioner Bonner established a Director of Anti-Terrorism, reporting directly to him and responsible for the coordination of Customs anti-terrorism efforts.

In an operational context and to support our Customs officers in the field, he and I have established the Office of Border Security, which reports to me. The mission of that office is to develop more sophisticated and complex anti-terrorism targeting techniques for passengers and cargo in each border environment and to provide a single point of contact for events taking place in our field.

In establishing our priority to prevent terrorists and terrorist weapons from transiting our borders, we believe that Customs must also do everything possible to push the border outwards. We must expand our perimeter of security away from our national boundaries and towards foreign points of departure.

Any effort to push the border outwards must include the direct involvement of the trade community. Commissioner Bonner established the Customs-Trade Partnership Against Terrorism, or C-TPAT, as we call it, to build on past, successful security models between Customs and the Trade that were expressly designed to prevent legitimate commercial shipments from being used to smuggle narcotics.

Another core area in these efforts is the implementation of the Container Security Initiative, or CSI. As you know, one of the stated goals of current terrorist organizations has been not only to target American lives but to target the American economy.

The vast majority of world trade, about 90 percent, moves in containers, much of it carried on oceangoing container ships. Nearly half of all incoming trade to the U.S. by value—about 46 percent—arrives by ship and most of that is in containers.

If terrorists were to succeed in concealing a weapon of mass destruction, even a crude device, among the tens of thousands of containers that enter U.S. ports every day, the devastation would be horrible and impossible to contemplate. And the impact on our global economy would be severe. As the primary agency for cargo security, I believe U.S. Customs should know everything there is to know about a container headed for this country before it leaves a foreign port, such as Rotterdam or Singapore. Customs wants that container pre-screened there, not here.

The effective use of technology depends largely on good targeting, for which we require advance information. Much has been said regarding Customs examining 2 percent of incoming cargo to the U.S. To some, the overall number of examinations may seem surprisingly low in proportion to the vast amount of trade we process. But the percentage of examination varies by associated risk, and it is important to note that the cargo Customs selects for intensive inspection is not chosen randomly. It is the result of a careful screening process, a process that uses information culled from a vast database on shipping and trading activities known as the Automated Manifest System. Using targeting mechanisms that operate within this system and information derived from our enforcement databases, we are able to sort through cargo manifests provided to Customs by shippers and carriers and choose those shipments that appear unusual, suspect, or high-risk. It is a system that has served us well, but one that definitely can be tweaked up.

Currently, the submission of advanced shipping manifests to Customs is voluntary. We cannot rest our Nation's security on the vagaries of haphazard advance information that is often incomplete and sometimes inaccurate. Timely, accurate, and complete information is vital to this Nation's security, and we should mandate that it is provided in advance.

Madam Chairwoman, I could just skip to my summation here or complete this, and may I submit this for the record?

Chairperson FEINSTEIN. Absolutely.

Ms. TISCHLER. Thank you so much.

In conclusion, the terrorists have already exploited one key component of our transportation system: commercial aviation. It is not at all unthinkable that they would seek to target others, including maritime trade. We believe our seaports and the system of global trade they support are vulnerable, and we believe that the U.S. and the Customs Service must act now to address this threat.

Thank you very much for the opportunity to testify before you today.

[The prepared statement of Ms. Tischler follows:]

STATEMENT OF BONNI G.TISCHLER, ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, UNITED STATES CUSTOMS SERVICE

Senator Feinstein thank you for your invitation to testify before this Subcommittee today. Since September 11th, Commissioner Bonner's top priority for the Customs Service has been responding to the terrorist threat at our land borders, seaports and airports. His highest priority is doing everything we reasonably and responsibly can to keep terrorists and terrorist weapons from entering the United States.

Through our Customs Inspectors and Canine Enforcement Officers, and Special Agents we are doing just that: protecting and defending our country against the terrorist threat at all our ports of entry, including our seaports.

Since September 11th, Customs has been at a Level One alert across the country—at all border entry points. Level 1 requires sustained, intensive anti-terrorist questioning, and includes increased inspections of travelers and goods at every port of entry. Because there is a continued threat that international terrorists will attack again, we remain at Level 1 alert to this day and will be at Level 1 for the foreseeable future.

As part of Commissioner Bonner's response, Customs has implemented round-the-clock coverage by at least two armed Customs officers at every Customs location, even at low volume crossings along our northern border. To this day, Customs inspectors are, in many places, working 12 to 16 hours a day, six and seven days a week.

To help ensure that Customs develops a coordinated, integrated counter-terrorism strategy for border security, Commissioner Bonner established a new Office of Anti-Terrorism.

In an operational context and to support our Customs officers in the field, we have also established the Office of Border Security. The mission of that office is to develop more sophisticated anti-terrorism targeting techniques for passengers and cargo in each border environment and provide a single point of contact for events taking place in our field.

In approaching our primary priority to prevent terrorists and terrorist weapons from transiting our borders, we believe that Customs must also do everything possible to "push the border outwards." We must expand our perimeter of security away from our national boundaries and towards foreign points of departure.

Any effort to "push the border outwards" must include the direct involvement of the trade community. The Customs-Trade Partnership Against Terrorism, or "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

Another core area in these efforts is implementation of the Container Security Initiative, or CSI. As you know, one of the stated goals of current terrorist organizations has been not only to target American lives, but to target the American economy.

The vast majority of world trade—about 90%—moves in containers, much of it carried on oceangoing container ships. Nearly half of all incoming trade to the United States by value—about 46%—arrives by ship, and most of that is in containers.

If terrorists 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 every day, the devastation would be horrible to contemplate. And the impact on our global economy would be severe. As the primary agency for cargo security, I believe U.S. Customs should know everything there is to know about a container headed for this country before it leaves a foreign port, such as Rotterdam or Singapore, for an American port. Customs wants that container pre-screened there, not here.

The effective use of technology depends largely on good targeting, for which we require advance information. Prior to September 11th, Customs examined about 2% of incoming cargo to the U.S. That percentage is significantly higher now. However, to some the overall number of examinations may still seem surprisingly low in proportion to the vast amount of trade we process. Yet it is importation to note that the cargo Customs selects for intensive inspection is not chosen randomly. It is the result of a careful screening process, a process that uses information culled from a vast database on shipping and trading activities known as the Automated Manifest System. Using targeting systems that operate within AMS, we are able to sort through the cargo manifests provided to Customs by shippers and carriers, and chose those shipments that appear unusual, suspect, or high-risk. It is a system

that has served us well, but one that can and must serve us much better in light of September 11th.

Currently the submission of advanced shipping manifests to Customs is voluntary. We cannot rest our Nation's homeland security on the vagaries of haphazard advance information that is often incomplete and sometimes inaccurate. Timely, accurate, and complete information is vital to homeland security and we should mandate it is provided in advance. Current legislation, such as S.1214 takes us a major step closer to where we ultimately need to be, particularly for the CSI—and that is to have full information on incoming cargo before it even leaves the foreign port.

As part of our immediate response to September 11th, Customs promptly sought, and the Congress promptly enacted, legislation that made the submission of data on incoming passengers to Customs' Advanced Passenger Information System mandatory for all airlines. That law was passed last November as part of the Aviation Security Bill. Initially, the Commissioner ordered all international airlines flying into the U.S. from abroad to submit advance passenger information to Customs, or face 100% inspection of people and goods departing their flights. This enabled Customs to better secure advance passenger information on all incoming international flights before the new law took effect.

Beginning with the mega-ports that export to the U.S., we should establish a new international security standard for containers in order to protect this vital system of global trade. The core elements of the CSI are the following:

- First, we must establish international security criteria for identifying high-risk cargo containers that potentially pose a risk of containing terrorists or terrorist weapons.
- Second, we must pre-screen the high-risk containers at their port of shipment—in other words before they are shipped to the U.S.
- Third, we must maximize the use of detection technology to pre-screen high-risk containers. Much of this technology already exists and is currently being used by the U.S. Customs Service.
- Fourth, we must develop and broadly deploy "smart" boxes—smart and secure containers with electronic seals and sensors that will indicate to Customs and to the private importers or carriers if particular containers have been tampered with, particularly after they have been pre-screened.

As you can glean from this list, technology and information are essential to a successful container security strategy, and to our counter-terrorist mission in general. And to put it simply, the more technology and information we have, and the earlier in the supply chain we have them, the better.

I also look forward to the completion of the Automated Commercial Environment, or ACE, which as you know is an extremely important project for the Customs Service. ACE, our new system of trade automation, offers major advances in both the collection and sorting of trade data.

We are also working with the Canadian and Mexican governments to improve information exchange and adopt benchmarked security measures that will expand our mutual borders and reduce the terrorist threat to most of the North American continent.

The terrorists have already exploited one key component of our transportation system: commercial aviation. It is not at all unthinkable that they will seek to target others, including maritime trade. We believe our seaports and the system of global trade they support are vulnerable, and we believe that the U.S. and the Customs Service must act now to address this threat. Thank you.

Chairperson FEINSTEIN. Thank you very much.

I am delighted to be joined by the ranking member, Senator Kyl of Arizona, with whom I have worked closely for a number of years now. Senator, do you wish to make a statement at this point?

STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator KYL. Madam Chairman, I would like to put my statement in the record. It says very nice things about your calling this hearing today, and I would love to repeat that to everybody. In the interest of time, I will simply say that I thank you very much for holding a hearing on this very important topic. I appreciate our witnesses' being here, and I will just put that in the record.

[The prepared statement of Senator Kyl follows:]

STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator Feinstein, thank you for calling today's hearing on protecting our nation's seaports against terrorism. Even before the tragic events of September 11, this subcommittee concerned itself with the protection of Americans from terrorist acts within our shores. I know both of us have worked to address the problem of identifying terrorists and stopping them from entering the United States. However, I do not believe that the public is aware that our seaports offer access points for terrorists and their weapons, including weapons of mass destruction, to enter our country with relative ease.

In October, Italian police discovered a suspected Al Qaeda operative hiding inside an ocean container. The container was equipped with a bed, toilet, satellite phone, computer, camera, airport maps, and airport security passes for Canadian, Thai, and Egyptian airports. All the necessary elements for another senseless act of terrorism were present. Thankfully, this terrorist was intercepted in time.

The U.S. Custom service states that only two percent of the 5.5 million cargo containers that entered our seaports in the year 2000 were ever inspected. But it is also important to recognize that, of the two percent of truck-sized containers that were inspected, many were not inspected until they reached their final destination. This means that a container may arrive in the port of Los Angeles and travel across the United States by rail or truck and not be inspected until it reaches the East Coast.

We are now aware of the economic fallout from the destruction of the World Trade Center towers by terrorists. The closing of any of the 12 major American seaports would also have severe economic effects, not only locally but throughout the nation. It is increasingly important that local, state, federal, and private entities make a coordinated effort to render our seaports safe.

I don't want to give the impression that Congress and the administration are not working on this issue. More that one-third of the 8,000 Coast Guard reservists have been called back to duty. This is a substantial call-up for an agency the size of the U.S. Coast Guard. The Coast Guard has boarded over 6,000 ships since the September 11 attacks, and 112 "security zones" have been established around port installations, commercial vessels, coastal power plants, and other infrastructure. In addition, the Senate passed the Port and Maritime Security Act of 2001. This Act is intended to examine the problem of port security, coordinate resources, authorize appropriations for equipment, and increase criminal penalties. However, we must always look to do more.

We have a very distinguished group of witnesses before us today. I am interested in examining with them how we can inspect a greater proportion of these containers without delaying the movement of goods through our ports, and what assistance Congress can provide to reach our objective of protecting our seaports, economy, and citizens.

Again, I would like to thank Senator Feinstein for holding this hearing today. We have always had an excellent working relationship and I look forward to examining this issue with her, with the skillful assistance of these witnesses.

Chairperson FEINSTEIN. Thank you.

Admiral please?

STATEMENT OF REAR ADMIRAL KENNETH T. VENUTO, DIRECTOR OF OPERATIONS POLICY, UNITED STATES COAST GUARD, WASHINGTON, D.C.

Admiral VENUTO. Madam Chairman, Senator Kyl, thank you for inviting the Coast Guard. Admiral Loy sends his regards.

I have a written statement that I would like to present for the record, and I have also a few verbal comments.

The Coast Guard is a unique organization. It is a military organization with maritime responsibilities, and it is a multi-missioned service that has got unique civil law enforcement authorities. It is the principal agency responsible for maritime homeland security and for port security of the country.

I would like to just review for a few minutes some of the things that the Coast Guard did immediately following the tragic events of 9/11 because they have a bearing on the sense of this hearing.

The Coast Guard provided a massive response right after the events of 9/11 to protect and secure the ports, waterways, and coastal areas of the United States. We still are maintaining a heightened level of security throughout our waterways.

We recalled from other missions 55 cutters, 42 aircraft, hundreds of small boats. We recalled port security units four of them that are reserve units, to provide heightened port security in New York, Boston, Seattle, and Los Angeles/Long Beach in particular.

Our Captains of the Port restricted vessel traffic and actually had some port closures during the time period. We implemented security zones around critical infrastructure on the waterside as well as high-value critical vessels.

To give you a sense, prior to 9/11, we roughly had about 12 security zones throughout the United States in one given time. Today, ma'am, we have 130 security zones going on on a daily basis, or more.

We implemented a 96-hour advance notice of arrival for ships coming from foreign ports to our country to provide a crew list as well as a sense of what their cargo was.

We provided vessel escorts to vessels which were considered to be of high interest or high value. We did joint interagency boardings on some of those vessels to make sure that everything was okay.

We implemented a prototype sea marshal program to ensure the internal security of vessels that could be used as potential weapons in our port areas in San Francisco and Los Angeles/Long Beach. We have extended the sea marshal program to roughly ten ports in the United States today, and we have done that by the call-up of reserves.

Just to give you a sense of the reserve call-up, there are 8,000 reservists in the Coast Guard Reserve. We called up 2,700 as a result of the events of 9/11. We currently still have almost 1,900 on active duty today.

Essentially, before 9/11, the Coast Guard's level of effort in our port security mission was around 2 percent. As a result of 9/11, we surged to almost 58 percent of a level of effort towards port security, which in the long run was not sustainable. Since then, as we have developed a more balanced approach, we have a level of effort, of total Coast Guard effort of about 21 percent of our mission requirements going to port security today.

We have reached out to the Navy in partnership. We have today 13 Navy coastal patrol boats helping us do port security mission areas. We have also reached out to the Office of Naval Intelligence in a joint intelligence and information operation out of Suitland in our Intelligence Coordination Center.

We have reached out to the International Maritime Organization. Last November, the Commandant personally went to the IMO and submitted a resolution for better international maritime security, and, Madam Chair, I have for your information a summary of the latest Intercessional Working Group that met in a special session.

The results of that are provided to you and the members of the committee.

The Commandant developed a ports, waterways, and coastal security strategic plan that essentially has the efforts of pushing our border outwards in kind of a layered defense, viewing our border as a continuum, basically originating from the country of origin all the way here to the United States. Our level of effort is to provide an appropriate and heightened level of security in our port areas, yet at the same time facilitating commerce.

The Commandant has set five strategic goals: to build Maritime Domain Awareness, which is basically intelligence and information sharing in an interagency effort; to control the movement of high-interest vessels that ply our coastal areas and our ports; to enhance our presence through deterrence and response capabilities by having more harbor patrols and folks at our marine safety offices being able to do more security inspections of high-value facilities; to protect our critical infrastructure and to enhance Coast Guard force protection; and to improve domestic and international partnerships.

The Commandant is in the process of developing a multi-year resource plan, and the Coast Guard appreciates the emergency response supplemental that was passed by the Congress in fiscal year 2002 to help us along in that process. And we seek your support for the President's budget because it is the first year of that 3-year plan in order to provide an appropriate level of resources to help in our port security efforts.

I could go on, ma'am, about the value of our port areas. You did it very articulately in your opening comments about the value of our ports areas to our economy. Basically, our ports contribute about $1 trillion to the gross domestic product of this country, and there are 361 ports in the country, 95,000 miles of coastline, 25,000 miles of inland waters, 3.4 million square mile exclusive economic zone, and we recognized that we have got the principal responsibility to ensure its security.

We have focused on—we can't do that alone. It requires partnerships with other Federal agencies, State and local authorities and agencies, private sector partnerships, as well as international partnerships. And we look forward to continuing in that effort.

Thank you, ma'am.

[The prepared statement of Admiral Venuto follows:]

STATEMENT OF REAR ADMIRAL KENNETH T. VENUTO, DIRECTOR OF OPERATIONS POLICY, UNITED STATES COAST GUARD

Good afternoon Madam Chairman and distinguished members of the Subcommittee. As Director of Coast Guard Operations Policy, I thank you for the opportunity to appear before you today to discuss the Coast Guard's maritime security strategy following the attacks of September 11th.

It has been said that the future has a way of arriving unannounced. The future arrived suddenly, violently and without warning on a clear day in September. In past years, our view of national security was projected mainly abroad, rather than within our own borders. Today, we suffer under the constant threat of terrorism as a means of coercion or retaliation, as much of the world already has, a reality that will no doubt continue well into the future.

Prior to September 11th, the Coast Guard's efforts were directed toward executing and enhancing maritime safety and security, environmental protection, and homeland defense in addition to our other normal peacetime missions. However, September 11th marked a change in the comfort and confidence our Americans citizens had

in their security and safety. Yet despite the obvious presence of the unseen enemy, the Coast Guard engaged in a massive response effort to protect our ports and Marine Transportation System. We also immediately escalated our force protection condition to protect our own people and facilities. The unique nature of the Coast Guard, as an agile emergency response-oriented organization within the Department of Transportation, allowed us to immediately increase our security posture, using existing active duty, reserve, civilian, and auxiliary personnel; as well as units, ships, boats and aircraft. One of the biggest lessons learned from September 11th is that the nature of the threat facing all nations has changed dramatically. What we saw on September 11th was were hijackers taking over commercial flights for the sole purpose of turning them into human guided weapons of mass destruction. We must translate that thought pattern and recognize the vulnerability of our maritime environment. We must change our assumptions underlying maritime security.

As a nation that depends so heavily on the oceans and sea lanes as avenues of prosperity, we know that whatever action we take against further acts of terrorism must protect our ports and waterways and the ships that use them. The Marine Transportation System of the United States handles more than 2 billion tons of freight, 3 billion tons of oil, transports more than 134 million passengers by ferry, and entertains more than 7 million cruise ship passengers each year. The vast majority of the cargo handled by this system is immediately loaded onto or has just been unloaded from railcars and truckbeds, making the borders of the U.S. seaport network especially vulnerable.

Preventing another attack requires an understanding of the maritime dimension of Homeland Security and constant vigilance across every mode of transportation: air, land, and sea. The agencies within the Department of Transportation, including the U.S. Coast Guard, Federal Aviation Administration, Federal Highway Administration, Federal Motor Carrier Safety Administration, Federal Railroad Administration, Federal Transit Administration, the Saint Lawrence Seaway Development Corporation, and the Maritime Administration (MARAD), touch all three modes of transportation and are cooperatively linked. This is especially true of the maritime mode. Ensuring robust port and maritime security is a national priority and an intermodal challenge, with impacts in America's heartland communities just as directly as the U.S. seaport cities where cargo and passenger vessels arrive and depart daily. The United States has more than 1,000 harbor channels, 25,000 miles of inland, intracoastal and coastal waterways, serving 361 ports containing more than 3,700 passenger and cargo terminals.

Simply stated, the Marine Transportation System is a complex transportation network, as is clearly evident in ports across the nation. These port complexes continue to grow at an amazing rate. Current growth predictions indicate that container cargo will double in the next 20 years. The biggest challenge facing our Marine Transportation System is how to ensure that legitimate cargo is not unnecessarily delayed as we and other nations introduce enhanced security measures against some very real and potent threats. The importance of the U.S. Marine Transportation System and the priority placed upon it by the Department of Transportation cannot be overstated.

I am very proud of the job our Coast Guard men and womean have been doing to deter potential future terrorist attacks in the maritime arena. Our people are working long hours, and 25 percent of our total Reserve population has been placed on active duty. In many ports, reserve members have been recalled to assist in a myriad of port security mission, such as the boarding and escorting of high interest vessels. However, this posture is not sustainable. . .nor is it an efficient or effective use of resources. Our challenge for the future is to determine what the new normalcy represents in terms of mission requirements and associated operational activity, while also ensuring that the Coast Guard is able to provide forces to meet its many responsibilities. While the most pressing security challenges have been met with existing authorities, we now must work to build a network of protections-one that transforms what has been a rapid response into a sustained effort that recognizes heightened ports, waterways and coastal security as a part of normal operations. In addition, marine security depends on the users of the maritime transportation system, including shippers and operators, and affects the trade corridors they use.

The intermodal aspect of the Marine Transportation System requires the Department of Transportation and its agencies with a stake in the system to take a coordinated approach in addressingto address the expansive security requirements. Through interagency collaboration and extensive partnering with public, private, domestic and international entities, tremendous steps have been taken to address close the strategic gaps between the current and desired level of protection for our

nation's ports and waterways. A key in this local outreach effort has been the continued engagement by the Captains of the Port with the private sector through such forums as the Port Readiness and Harbor Safety Committees. The teamwork and desire of the community to significantly enhance maritime security is exemplary. Equally important are partnering efforts with the international community. Recognizing that the maritime sector of the world's economy is the most valuable and the most vulnerable, at a recent International Maritime Organization meeting in DecemberFebruary, the Coast Guard proposed the development of concrete actions that will enhance maritime security worldwide. These proposed international recommendations are key in intercepting threats before they reach our borders, thus extending the borders of our domain awareness, an awareness that was lost leading up to the attacks of September 11th.

While effective ports, waterways and coastal security is built upon the principles of awareness, prevention, response, and consequence management, the primary objectives are awareness and prevention, since we hope to avoid any need for future consequence management. Awareness helps focus resources and provides efficiency to prevention. Prevention places a premium on awareness, detecting, identifying, and tracking threats to our ports, waterways and coastal security. However, once terrorists or the means of terrorism are on the move towards or within the United States, the nation must have the means to detect and intercept them before they reach our borders and our transportation system. While there are no guarantees, there is good reason to believe that we can improve our national ability to detect potential threats through effective use of information. Exploiting available information to separate the good from the bad, and then stop the bad, is the heart of the Coast Guard developed Maritime Domain Awareness concept and overall Ports, Waterways and Coastal Security Strategy. This strategy must facilitate legitimate maritime commerce, which is supposed to double in the next 20 years, while filtering threats by using real time intelligence.

The goals of the Coast Guard's Ports, Waterways and Coastal Security Strategy will be to:

- Build Maritime Domain Awareness.
- Control movement of High-Interest Vessels
- Enhance presence and response capabilities.
- Protect critical infrastructure and enhance USCG force protection.
- Conduct Domestic and International Outreach.

In summary, the Department of Transportation mounted a significant and rapid response to this severe and unexpected threat. Notably, maritime trade, which is critical to this country's economic strength, continues to move through ports with minimal interruption. It is no surprise that sustaining mobility will come at a higher cost to all of us. But the reality is that we live in a country that prides itself on the openness of its democracy, so we remain at risk to attacks of terrorism. It is incumbent upon our government to minimize this risk. With your support, the Coast Guard shall meet this challenge and ensure that our nation's Marine Transportation System remains the very best in the world.

Chairperson FEINSTEIN. Thank you very much, Admiral.

We will begin the questions now, and let me begin with a brief statement. I really question the effort to stretch out our ports—I have lost the right words, but to stretch out our ports so that the inspection is done at the port of origin rather than at the port of delivery. I think we open ourselves to a huge loophole if we do that. I would not bet on a port in Pakistan really not being subject to bribery, to inspect a ship rented by Osama bin Laden that might contain a nuclear device in it. No way, no how would I ever think that that could be protected against, because I don't. So I think the only protection is our own port structure.

Now, I would like to read a scenario. A suspicious ship is heading toward United States waters. It is carrying a type of cargo not found in its home port or its recent ports of call. Some of its crew are on an intelligence watch list because they are suspected of having links with radical Islamic organizations. And the ship is scheduled to arrive on the same day as a tanker carrying highly volatile fuel.

According to national security expert Stephen Flynn, despite these red flags, this highly suspicious ship could still enter U.S. waters without being stopped or examined because information about the ship is scattered in bits and pieces throughout different agencies and, thus, no one is able to see the big picture—similar, Senator to what we have talked about before.

So my question to any or all of you is: Is there a system in place to gather, compile, and analyze information from different agencies? You have mentioned the passenger manifest and crew manifest, but forget that. Is there a system in place that is interoperable to manage data, to be able to pick out a suspicious ship, and then, second, keep it from entering an American port?

Admiral VENUTO. Let me answer at least part of that question.

First of all, I think there is no current system that looks at everything right now. We don't have an integrated information system per se. We in the maritime arena are beginning to develop that. The ideal situation would be that we get all the information electronically, both on the crew, the passengers, the cargo, it was all visible, and that the various agencies who had responsibility for whatever element that is—whether it is the Coast Guard, whether it is the Customs Service, whether it is INS—could be able to get the information they need from that particular database.

Chairperson FEINSTEIN. You get intelligence data, FBI data, NSA data?

Admiral VENUTO. We get some of that, ma'am. Today we do. We require, as I said before, this 96-hour notice of arrival. What we get with that, of course, every ship is required to report their arrival 96 hours before, and they have to provide the crew list to us as well as——

Chairperson FEINSTEIN. Can you stop the ship?

Admiral VENUTO. We can prevent it from entering port if they don't get our permission, and we have, in fact, stopped vessels from coming in, told them that they had to stay out.

We had a recent case on the West Coast, out in Hawaii, where a ship wanted to come in for whatever reason, and they wanted to come in before the 96-hour notice of arrival, and we told them they could not until they provided us the crew list so we could run it through our intelligence database, which we run with the Navy, and we check on the crew to see whether they have any particular——

Chairperson FEINSTEIN. Would you get information, for example, about a ship that Osama bin Laden may have rented or in some way controlled or leased? "Leased" is the same thing as renting.

Admiral VENUTO. It depends on how much intelligence information we have on——

Chairperson FEINSTEIN. I bet the answer is no.

Admiral VENUTO. Yes, you may not. You know, one of the things, if you notice, one of the issues that we brought up at IMO was visibility of ownership on ships.

Chairperson FEINSTEIN. What is IMO?

Admiral VENUTO. It is the International Maritime Organization. It is the organization that regulates international standards of shipping throughout the world. We have used it primarily—it was primarily as a safety organization, and through U.S. efforts we

have brought up the safety standards of the international fleet throughout the world.

Chairperson FEINSTEIN. But you get no intelligence——

Admiral VENUTO. But we get no intelligence from them. The issue would be if—you may not have visibility of ownership. You may not have visibility of who, in fact, is using the ship to have their cargo come in currently. You may not have that. But Customs runs the cargo dimensions of it more. I am not as qualified to answer that particular question.

Chairperson FEINSTEIN. We have worked together on trying to make this data more interoperable between agencies, and the area that we haven't yet encountered is the seaport. And it seems to me that you ought to have intelligence data because this is the only way you are going to be able to prevent something from coming in, is some suspicion that is checked out as being, what they say, a good source so that you can take some action.

Senator Kyl, Senator Schumer pointed out his deep concern, and I know that you share it, and I share it, too, and that is that there may 1 day be a nuclear device aboard one of these ships, and we don't have the equipment to really understand that once the ship comes in. So you have got to figure once the ship comes in, it is too late. So you have got to stop the ship from coming in.

Now, how do you do that? Intelligence.

Ms. TISCHLER. Senator Feinstein, if I might?

Chairperson FEINSTEIN. Yes.

Ms. TISCHLER. I know that my colleague has something he wants to talk to you about, but I would just like to comment. So much of our sorting capability is based on advance information that we don't have because it is not enough in advance.

It is Customs' position—and Senator Hollings and Senator Kyl and you have been very helpful in trying to see that the industry got us information enough in advance to even do the targeting. It is our premise that we need the information from the trade on point of departure from wherever it is they are coming from.

Chairperson FEINSTEIN. You don't get that now?

Ms. TISCHLER. We don't get it—we get it—it is not mandatory. It is voluntary. And although we have a lot of helpers in the community and we do get quite a bit of information, the fact is that we don't get it in most cases timely enough. We don't get it complete enough. We don't get it accurately enough. We would like to lay down the data requirements from a uniformity perspective that we need every time so that the agencies can sort.

With that in mind, I know the legislation pieces that are out there. One of them—I think it is Senator Hollings' bill—addresses a 5-day lag time, which is okay if you are coming from Europe or from Asia, but if you are coming in from Venezuela or the Caribbean, they get there faster than they actually have to submit the manifest data.

And just to add on to my colleague from the Coast Guard, we do get intelligence information. We have jointly boarded ships, Customs has with the Coast Guard and the FBI based on information received from our sister agencies in the intelligence community. And the only thing that is driving us right now is that need for advance information, the intelligence from the community, and the

technology to actually sort the containers when they show up on our shores.

We do have radiation detecting capabilities, but think of this: What if—and probably it will come shielded. So it is our contention—we have radiation pagers that our inspectors have that work pretty well if there is a radiation source. If it is shielded, it is not going to pick it up. So I think we need lead detectors. And I am not trying to be facetious, but we sort of have to expand our universe in terms of the technology that is available to all the agencies that are pitted against the problem.

We have radiation portal devices that have been used on the Russian border, actually, against smuggled nuclear material in one lane of traffic. We asked if it could be stretched to a cut, like, for instance in Miami. I am a Miami girl. Government cut is where all the boats come in through when they are going to Dodge Island. It would be so much better to be able to sort a large vessel all at one time to see if there was a radiation source on the vessel before it got to the dock, if the Coast Guard missed it out at sea. And they need their own portable radiation detectors in order to really help.

But right now, some of the technology is in the works through DOE and their labs and some of it is in the works through DOD, and they are sharing with us so that we are trying to work on commercializing these pieces of equipment, which we would be glad to show you at your convenience if you come down to the port at—Los Angeles seaport or Oakland. And I think that is the answer.

So it is really a meld of the intelligence, the sharing of information, the databases themselves, the advance information. That 2 percent figure that we were talking about is based on a sorting of high-risk cargo. And at L.A. seaport, I know——

Chairperson FEINSTEIN. You know where I am going, because I have been through the border stuff now for 10 years since I have been here. Everything has been to speed trade: Let it go through, ask questions later. And we are now in an era where we can't do that.

Where I think we should go is how do we set the dynamic whereby private companies know they have to do greater diligence with respect to what goes on a ship because that ship may well be stopped and sit offshore for a month while the Coast Guard or some other agency goes through it bit by bit by bit if they don't do that due diligence.

And I agree with you on the shielding. I agree with you on the cost of the X-rays. I am very worried that—Port of Long Beach will speak for itself, but I know the inability—I talked to Customs people in Los Angeles. I know how overstressed they are and undermanned, and the load is just tremendous.

So my feeling is to create a situation whereby the companies that do the loading aren't going to take the risk of a ship getting stopped as a first step.

I want to give Senator Kyl a chance, but did you want, Captain Schubert——

Captain SCHUBERT. Yes, I would like to make a few comments.

Chairperson FEINSTEIN. And then Senator Kyl.

Captain SCHUBERT. First of all, I don't think any of the panelists have any disagreement with you whatsoever about increasing—

that we need to increase the level of security in our ports. But when it comes to cargo security, especially, and the way intermodal operations work today, all of the agencies here—the Coast Guard, Customs, the Department of Transportation, the modal administrators, all agree that when it comes to cargo coming from international ports, we must have some form of prescreening in the foreign ports.

Now, we have a Container Working Group where all three agencies have worked together on this issue, and we have identified a working plan both short term and long term to address this issue. And I am very confident that we will have a combination of technology, more inspections in foreign ports, not necessarily by U.S. Government people, but we need to be able to profile the cargo before it is loaded on the ship.

Chairperson FEINSTEIN. Who does the inspections in foreign ports? And how many foreign ports would this be?

Captain SCHUBERT. Well, there are a number of foreign ports, but there are something like 12 transshipment ports, major transshipment ports, before, you know, the cargo comes to the United States. We are talking about containers now that represent probably 80 percent of the cargo coming to the United States.

So I know it seems like a lot of ports, but we are really concerned about the ports just prior to leaving to come to the United States. Some cargo might be transshipped several times through several countries, for example. But the point is—and the best illustration that I have given many, many times since 9/11 is when we had the tragic events of 9/11, Secretary Mineta basically brought down the whole airline industry for 4 days to make sure that each plane was checked for safety and that there wasn't any more terrorists on the planes. And that took 4 days before we could get the system back up and operating again.

If we had a similar situation with a container where we had a credible threat, all we knew is that there might be ten containers coming from ten different directions with a dirty bomb or some other weapon of mass destruction in it, and we had to shut down our ports and our intermodal system to do the same thing that we did on the air side, we would have to shut our system down for 4 months. That is by some estimates, up to 4 months, just to check all the containers. If anything can bring our economy down, that can.

So we need to have a combination and several layers of security in the ports, on the ships, and also some sort of preclearance of cargo before it is actually loaded on the ship. And that is something that I think all three agencies here, plus listening to the stakeholders—the carriers, the shippers, they all agree that we need to come up with an efficient system that can do that to increase security.

Chairperson FEINSTEIN. Thanks very much.

Senator KYL. Thank you. Obviously, there is just a lot that is going to have to be done to maintain our commercial activities, but at the same time begin to deal better with terrorism than we have in the past. And obviously, too, any suggestions that you all have that we can help on I think would be very welcome.

In that regard, it is pretty clear that this is going to cost a lot of money, and particular, Commissioner Tischler, let me ask you:

What would be the effect of taking the Customs user fees away from the Customs Service in terms of your ability to perform this task?

Ms. TISCHLER. My personal opinion is it would severely hamper us. I know that there is a lot of controversy about the user fees. I know that the big user fees that go into the COBRA fund, for instance, pay for some of our people, about 1,200 of them, and pay for all of the overtime and quite a bit more. And so we are—for instance, if that one sunsets—and it is supposed to sunset September 30, 2003—we would be severely hampered in how we operated. Most of the overtime—all of the overtime that is being done by the inspectors now has really depleted the fund since 9/11. So as just a personal sentiment, because we have been struggling with the whole COBRA concept for the last 2 years as if it might sunset in 2003, it would put a big crimp in our activities.

Senator KYL. I think—correct me if I am wrong—that the biggest single—and I know there are several different funds, but the biggest is the merchandise processing fee fund.

Ms. TISCHLER. Yes, sir.

Senator KYL. And I have a figure for that of, in the year 2001, $957 million, so just under $1 billion. And I realize that this is scored against Customs. Technically it goes into the general fund, but if you were to not have the benefit of that in your appropriations, I presume it would be fairly devastating, would it not?

Ms. TISCHLER. It would absolutely be devastating. I think our total budget is closing in on $3 billion thanks to Congress and the administration. So to take that much out, if it were as the offset, would be truly devastating.

Senator KYL. Right. Now, you mentioned offset. The reason I bring this up is that at least one suggestion is that the way to pay for about $15 billion in subsidies in the energy bill from the Finance Committee is to apply these Customs user fees. And I have tried to make the point that that is not probably a good idea, and I made that point to Governor Ridge today as well. And I am sure that if that is still an idea that is out there, you will want to make sure that folks understand the implications of it were that to be done.

Ms. TISCHLER. Yes, sir. I will refer it to our Office of Finance, who I am sure will talk to OMB on the scoring issues.

Senator KYL. It is not just a matter of on the scoring issues. It is a matter of Congress deciding to take those fees and put them to another object here, in this case, the energy bill.

Ms. TISCHLER. Right, sir. I understand.

Senator KYL. Okay. Thanks.

I need to apologize to everyone. Not only was it a bad time at the beginning, but I also have a 4:15 that I did not realize earlier. And so I am not going to be able to spend as much time with all of you as I would like, but I don't want you to infer from that that I am not just as interested as Senator Feinstein is in trying to figure out ways to deal with this problem.

We have got a bill now that deals with individuals traveling to the country from abroad. In some respects, that is easier to deal with. In other respects, it is not. But we need to do the same thing here with regard to cargo. And just as we do with people, we don't

want to slow them down. We want to get as many people coming to the United States as possible. But since they are our guests, we also want to make sure that none of them are unwanted guests. And that same thing goes for any cargo, of course.

So, again, I regret that I can't stay here. I have read all of your testimony, and I regret that I won't hear the other panel. But, again, Madam Chairman, I thank you very much for your continued interest in this subject, and I look forward to working with you on ways that we can improve the ability to detect material that shouldn't be coming into the country.

Chairperson FEINSTEIN. Thank you very much. Thank you.

Before we move on to the other panel, I want to just ask, this business of having cargo checked in other ports before it comes on, and you mentioned that check would be confined to the 12 largest——

Captain SCHUBERT. No, I didn't. I didn't——

Chairperson FEINSTEIN. You said that ports that handle a large percent are really 12 of them, so I just gathered from that that you were saying——

Captain SCHUBERT. We could start with the major ports, and this is an issue that——

Chairperson FEINSTEIN. Does that include Karachi?

Ms. TISCHLER. No.

Chairperson FEINSTEIN. No? See, there——

Captain SCHUBERT. Karachi wouldn't be——

Chairperson FEINSTEIN. Pardon me?

Captain SCHUBERT. Karachi wouldn't be one of the 12 ports, no, ma'am.

Chairperson FEINSTEIN. Well, there is your weak link.

Captain SCHUBERT. Right. But what we need in the industry today—and I am speaking from my 27 years of experience in both being a ship's captain and sailing on ships, handling over $7 billion in exports for both freight forwarders and shippers. I really do understand how complex the industry is, and knowing that I can still make this next statement very confidently: The industry needs more discipline than it has had in the past. We have cases now, for example, the way the industry works today, where a container can be loaded on a ship and be halfway across the Atlantic Ocean before anybody gets any documentation on what the container is, what is in the container. That simply can't continue to be a business practice that we can accept.

What we are talking about—and I am really getting more into the Customs issue here, but it is reporting, mandatory reporting of what is said to be in the containers. And from that information and the history of the shippers that are out there, you could put together a profiling to determine what containers really need to be inspected, what containers don't have to be inspected.

This is just an important element of adding security to our maritime system. It does not in any way take away from the importance of what you said earlier about improving the security in our ports. It is just another layer that has to be thrown in there, and it is something that is absolutely necessary, in my opinion.

Chairperson FEINSTEIN. I appreciate that, and it is not up to me to argue. If the administration wants to move in this direction, that

is up to the administration, certainly. But I would like you—I have very deep concerns about it because I think it will just create a—you know, we know there are—I won't say how many, but there are a number of missing tactical nuclear weapons. We know that there is access to all of this stuff. And, you know, my goal is to keep it out of this country, and the only way I know to do it is to secure our ports to be able to keep it out. And I have always very deeply believed if it comes to commerce or if comes to protection of our people, the protection of our people comes first.

And I have got news. I don't mind having our ports shut down for 4 months if it is going to prevent a nuclear weapon from coming into this country. For me, that is a piece of cake. I mean, you do it.

When I was mayor of San Francisco, I told my airport director, who is now director of the airport in Toronto, if a bomb ever leaves here on a plane, don't show up, you don't have a job the next day. And, you know, you have got to make your people move and understand and really work, and at the time we even had bogus dogs at the airport. They weren't real dogs—I mean trained to sniff bombs. And that was San Francisco International Airport.

Now, that was a long time ago. Things have changed a lot since then. But I don't think there is anything that replaces vigilance at our ports or keeping dangerous ships out of our ports. And by dangerous ships, I mean where your intelligence alerts that there is a problem. Then you delay it and you see that there is nothing aboard that ship.

Anyway, does anyone have anything else they want to say?

Admiral VENUTO. Could I just say, Madam Chairman, just a few things?

Chairperson FEINSTEIN. Sure.

Admiral VENUTO. I think what we are trying to describe here is a risk management kind of regime where we try to establish security protocols in partnership with other agencies, with the private sector, and with international partners that are legitimate traders. And if you establish that system of protocols, that helps you then to focus the resources that we have on those suspect areas you talk about, where if we have a system of protocols with the 12 major ports that we trade with and everybody abides by the system of security protocols, then we can focus our efforts on those more suspect ships and containers and shippers that don't have the same system of protocols.

Just as our intelligence agencies—I mean, we have, we say, high-interest vessels. I can't really go into the information as to what classifies a high-interest vessel because it is classified. But we recognize that there are certain areas of the world, certain crew members, et cetera, that we need to focus on, and that helps us take our scarce resources and focus in that area.

If you look at joint inspection areas, one of the protocols that we would like to set up is to actually have inspectors in other countries, U.S. inspectors, or U.S. inspection of their security procedures—and they would do the same to us; it would have to be a partnership—in those areas. So it is a matter of profiling the right suspect vessels with our scarce resources to do that, recognizing that it is a risk management regime.

Chairperson FEINSTEIN. Thanks very much, Admiral. I appreciate it. Thank you very much for being here. We will move on to the second panel.

Thank you very much for being here. And if I may, because there are five people, perhaps I will do the introductions seriatim, one by one. Let me find my introduction list here.

The first witness is Richard Steinke from the Port of Long Beach, California. He is the executive director of the port, the busiest port in the United States and, with the Port of Los Angeles, the third largest port complex in the world. During his 5 years there, container volume passing through the port increased by 30 percent, and last year alone, nearly $200 billion in cargo passed through that port. Mr. Steinke is also the chairman of the board of the American Association of Port Authorities, an alliance of more than 150 port authorities in the United States, Canada, the Caribbean, and Latin America. Welcome, and we will be very interested in what you have to say.

STATEMENT OF RICHARD D. STEINKE, CHAIRMAN OF THE BOARD, AMERICAN ASSOCIATION OF PORT AUTHORITIES, AND EXECUTIVE DIRECTOR, PORT OF LONG BEACH, LONG BEACH, CALIFORNIA

Mr. STEINKE. Thank you, Madam Chair, and thank you for this opportunity to address you on the important matter of port security. Enhancing security is the top priority for America's ports today.

Safety and protection have been of paramount concern to the Port of Long Beach. Prior to the events of September 11th, our focus, as well as many other ports, was primarily on crime prevention, with an emphasis on cargo theft. Following the tragic terrorist attacks on the World Trade Center and the Pentagon, the focus of our efforts to protect the port and facilitate commerce and the free flow of goods has been broadened to include prevention and response to acts of terrorism.

Besides being one of the busiest ports in the world, the Port of Long Beach as well as the Ports of Oakland and San Diego in California represent part of the National Port Readiness Network. This designation by the Maritime Administration requires the port to be prepared and ready 24/7 to respond to national emergencies whether they are military or civil in nature. Our deepwater entryway is a Federal navigational channel that must remain clear and operational at all times so that ships carrying strategic cargo can enter or exit the port unimpeded.

The roadways and railways leading to these load-out centers must be adequately secured also to provide for movement of goods and people. While the Port of Long Beach's role in responding to national emergencies is a major one strategically, each and every port in the United States has the potential for playing a significant part in the security of this country by serving as a conduit for a sound national economy.

Long before the events of September 11th, the port realized a need for maintaining the highest levels of security possible. To that end, the Port of Long Beach has proactively developed a port secu-

rity plan to create and maintain a level of security that might serve as a model for the maritime industry.

Over the last decade, the Port of Long Beach has created a Port Crime and Security Committee, made up of industry stakeholders, terminal operators, Federal, State, and local law enforcement agency representatives, and terminal security officials. We meet on an ongoing basis to discuss issues related to crime, safety, and security. These meetings shape the infrastructure and open lines of communications among industry and law enforcement responsible for the safety of the people who work in the ports and the security of the cargo that move through it. Since September 11th, we have been operating at a heightened security level. We have increased the number of committees and task forces to address the expanded needs and new charge for greater protection of our port.

Greater security is not limited simply to the movement of cargo through the port. Every capital project that we undertake now has a new element built into it. Our plans for a new bridge or pier, widening of a channel, or erecting a crane all now must include considerations for security enhancements. We have recently completed a detailed security assessment of our waterfront facilities, including the Port Harbor Patrol, Long Beach Police Department, and the U.S. Coast Guard, and expect that this assessment will suggest additional improvements and upgrades. Those refinements will require funding not heretofore anticipated.

Basically, what I am saying is the new demands for security will require new sources of fundings. Funding considerations should be given to supplement the manpower needs of the participating Federal and local law enforcement agencies. We especially would like to emphasize our support for increased funding for the U.S. Coast Guard and the U.S. Customs Service. Approximately 35 percent of all waterborne cargo containers that come into the United States come through the Los Angeles/Long Beach Port Complex, so the workload of these two agencies is many times above the level expected of them in other ports throughout the country.

The Port of Long Beach believes there needs to be increased funding for U.S. ports and Federal agencies, as well as a proper balance of dollars and personnel to the ports with the greatest cargo volumes and vulnerabilities.

It is my honor to serve as chairman of the American Association of Port Authorities. AAPA strongly supports Federal programs aimed at protecting America's seaports from acts of terrorism and other Federal crimes. Following September 11th, ports took immediate action and have invested millions of dollars to heighten security at their facilities. AAPA believes increased funding is required for the Federal agencies to take the lead on maritime security such as the U.S. Coast Guard and the U.S. Customs, as I noted previously.

In addition, America's public ports need Federal financial help to implement security enhancements in a timely and effective manner. The $93.3 million provided by Congress is a good first step, but significantly more money will be needed. Because each port has unique characteristics, a one-size-fits-all approach does not work. Seaport security should be coordinated at the local level, working with the U.S. Captain of the Port to establish local security com-

mittees and develop appropriate security measures based on threat and vulnerability assessments.

There are a number of other initiatives that could be examined in a review of seaport security issues as they relate to international maritime traffic into and out of ports. Automatic Identification Systems that provide a ship's identity, position, course, and speed, seafarer identification and background check, port-of-origin container examinations, as we have talked about before, are all items that need further investigation.

I would be remiss if I did not make special note of the exemplary job done by the Coast Guard following the tragic events of September 11th. They deserve recognition for taking the lead in exerting positive control over the port at a time when confidence and assurance were needed. The Coast Guard continues to play an instrumental role in our efforts to keep our people at the Port of Long Beach and the other ports in the United States safe.

In closing, I thank you, Madam Chair, and the members of the Senate Judiciary Committee on Technology, Terrorism, and Government Information for your interest and concern in seaport security issues.

Thank you.

[The prepared statement of Mr. Steinke follows:]

STATEMENT OF RICHARD STEINKE, CHAIRMAN OF THE BOARD, AMERICAN ASSOCIATION OF PORT AUTHORITIES, AND EXECUTIVE DIRECTOR, PORT OF LONG BEACH

Madam Chair, members of the committee. Thank you for this opportunity to address you on the important matter of Port security. Enhancing security is the top priority for America's ports today.

Safety and protection have been of paramount concern to the Port of Long Beach. Prior to the events of September 11, our focus was primarily crime prevention with an emphasis on cargo theft. Following the tragic terrorist attacks on the World Trade Center and the Pentagon, the focus of our efforts to protect the Port and facilitate commerce and the free flow of goods has been broadened to include prevention and response to acts of terrorism.

Besides being one of the world's busiest seaports, the Port of Long Beach (as well as the Ports of Oakland and San Diego in California) is part of the National Port Readiness Network. This designation by the Maritime Administration requires the Port to be prepared and ready 24/7 to respond to national emergencies whether they are military or civil in nature. Our deepwater entryway is a federal navigational channel that must remain clear and operational at all times so that ships carrying strategic cargo can enter or exit the Port unimpeded.

The roadways and railways leading to these load-out centers must be adequately secured to provide for movement of goods and people. While the Port of Long Beach's role in responding to national emergencies is a major one strategically, each and every port in the United States has the potential for playing a significant part in the security of this country by serving as a conduit for a sound national economy.

Long before the events of September 11, the Port of Long Beach realized a need for maintaining the highest levels of security possible. To that end, the Port of Long Beach has proactively developed a port security plan to create and maintain a level of security that might serve as a model for the maritime industry.

Over the last decade, the Port of Long Beach created a Port Crime and Security Committee. Made up of industry stakeholders; terminal operators; federal, state, and local law enforcement agency representatives; and terminal security officials; we meet on an ongoing basis to discuss issues related to crime, safety and security. These meetings shaped the infrastructure and opened lines of communications among industry and law enforcement responsible for the safety of the people who work in the ports and the security of the cargo that move through it. Since September 11, we have been operating at a heightened security level. We have increased the number of committees and task forces to address the expanded needs and new charge for greater protection of our port.

Greater security is not limited simply to the movement of cargo through the Port. Every capital project that we undertake now has a new element built into it. Our

plans for a new bridge or pier, widening of a channel, or erecting a crane all now must include considerations for security enhancements. We have recently completed a detailed security assessment of our waterfront facilities, including Port Harbor Patrol, Long Beach Police Department, and the U.S. Coast Guard, and expect that this assessment will suggest improvements or upgrades. Those refinements will require funding not heretofore anticipated.

Basically, what I am saying is that the new demands for security will require new sources of funds. Funding considerations should be given to supplement the manpower needs of the participating federal and local law enforcement agencies. We especially would like to emphasize our support for increased funding for the U.S. Coast Guard and the U.S. Customs Service. Approximately 35% of all waterborne cargo that comes into the United States comes through the Los Angeles/Long Beach Port Complex, so the workload of these two agencies is many times above the level expected of them in other ports throughout the country.

The Port of Long Beach believes there needs to be increased funding for the U.S. ports and federal agencies, as well as a proper balance of dollars and personnel to the ports with the greatest cargo volumes and vulnerabilities.

It is my honor to serve as Chairman of the American Association of Port Authorities. AAPA strongly supports federal programs aimed at protecting America's seaports from acts of terrorism and other federal crimes. Following September 11, ports took immediate action and have invested millions of dollars to heighten security at their facilities. AAPA believes increased funding is required for the federal agencies that take the lead on maritime security, such as the U.S. Coast Guard and U.S. Customs as I noted previously.

In addition, America's public ports need federal financial help to implement security enhancements in a timely and effective manner. The $93.3 million provided by Congress is a good first step, but significantly more money is needed. Because each port has unique characteristics, a one-size-fits-all approach does not work. Seaport security should be coordinated at the local level, working with the U.S. Coast Guard Captain of the Port to establish local security committees and develop appropriate security measures based on threat and vulnerability assessments.

There are a number of other initiatives that could be examined in a review of seaport security issues as they relate to international maritime traffic into and out of the ports. Automatic Identification Systems (AIS) that provide a ship's identity, position, course and speed, seafarer identification and background check, port of origin container examinations, are all items that need further investigation.

I would be remiss if I did not make special note of the exemplary job done by the Coast Guard following the tragic events of September 11. They deserve recognition for taking the lead in exerting positive control over the Port at a time when confidence and assurance were needed. The Coast Guard continues to play an instrumental role in our efforts to keep our people and the Port of Long Beach safe.

In closing, I thank you Madam Chair and all the members of The Senate Judiciary Subcommittee on Technology, Terrorism and Government Information for your interest and concern in seaport security issues.

Chairperson FEINSTEIN. Thank you very much, Mr. Steinke.

Amanda DeBusk, welcome. Amanda DeBusk is the former Commerce Department Assistant Secretary for Export Enforcement. She was head of a 165-person organization in charge of enforcing U.S. export controls and international trade negotiations and initiatives. She is a former Commissioner on the Interagency Commission on Crime and Security in U.S. Seaports.

Welcome.

STATEMENT OF F. AMANDA DEBUSK, FORMER ASSISTANT SECRETARY FOR EXPORT ENFORCEMENT, DEPARTMENT OF COMMERCE, AND FORMER COMMISSIONER, INTERAGENCY COMMISSION ON CRIME AND SECURITY IN U.S. SEAPORTS, WASHINGTON, D.C.

Ms. DEBUSK. Thank you very much.

Today, I would like to highlight some of the recommendations of the Seaports Commission and, in particular, to talk about some of those recommendations that were not completely addressed in the

Port and Maritime Security Act that passed the Senate this past December.

Let me begin by providing some context for the Commission's study. The Seaports Commission was looking at terrorist threats in connection with the new millennium. We were concerned about how wide open our seaports are compared to our airports. In most cases, there is easy access to the seaports.

Criminal activity at the seaports is a big problem. The Commission found significant criminal activity was taking place at most of the 12 seaports surveyed. One of the cases my former office investigated involved a riot control vehicle that was exported to China as a fire truck. The vehicle was huge. It resembled a tank, and it had a turret on the top for spraying pepper gas. It was exported in a container, and at the time no one knew what was inside that container. So if someone can smuggle a tank through a seaport, it does not make us feel secure about catching chemical weapons or a nuclear bomb.

Chairperson FEINSTEIN. Did it come from a California port?

Ms. DEBUSK. Yes, it did.

Chairperson FEINSTEIN. I won't ask—or shall I ask which one?

Ms. DEBUSK. Los Angeles.

Chairperson FEINSTEIN. Thank you.

Ms. DEBUSK. The Commission found that the state of security at seaports generally ranged from poor to fair, with a few exceptions where the security was good. The Commission made recommendations that, if implemented, would go a long way in combating terrorism at our seaports. I will discuss recommendations on physical security, cargo security, and data needs, something that you had touched upon.

First, concerning physical security, the Commission provided recommendations on minimum physical security standards covering fences, lights, gates, restrictions on vehicle access, restrictions on carrying firearms, the establishment of a credentialing process, considering criminal background checks for those with access to sensitive areas of the port, and development of a private security officer certification program.

The Port and Maritime Security Act provides for the development of Maritime Facility Security Plans that would address these needs. However, to develop and implement these plans, which are very complex, would take a long time. While there is authority for interim measures, there is no standard for these interim measures. An alternative might be to immediately put in place standards identified by the Commission and permit waivers if a seaport had a good reason not to implement a particular requirement. That would move us along more quickly.

For example, we could put in place a restriction on carrying guns at seaports. It makes no sense to prohibit nail clippers at airports but allow guns at seaports. Of the 12 seaports surveyed by the Commission, not a single one restricted firearms. And to my knowledge, this situation has not changed.

Chairperson FEINSTEIN. Could you explain that? When you say firearms, your officers would carry firearms.

Ms. DEBUSK. That is exactly right.

Chairperson FEINSTEIN. But what do you mean by restricting firearms?

Ms. DEBUSK. Suppose that I, private citizen, Amanda DeBusk, decided to stroll down to the port, I could have my gun with me.

Chairperson FEINSTEIN. Interesting.

Ms. DEBUSK. Exactly right. This would seem something that is so basic that it is—it was pretty amazing to us that not a single seaport had that restriction.

Chairperson FEINSTEIN. None of the major seaports had any restriction on anybody walking in with a gun?

Ms. DEBUSK. That is correct. You are correct.

Chairperson FEINSTEIN. Thank you.

Ms. DEBUSK. So certainly the Seaport Commission, which was composed of officials from law enforcement agencies, recommended that arms at the seaport be restricted to law enforcement personnel.

Another example of a basic security requirement that could immediately be implemented is a restriction on private vehicle access to the ports. At many ports, access is uncontrolled. At one of the ports I visited, we saw a line of vehicles parked right beside the vessel. We were told that these were the dock workers' vehicles parked there for convenience. At the time, we were concerned that the vehicles could be hiding places for smuggled drugs. Today we must consider the possibility that a car bomb or a dirty nuclear weapon could be hidden in those vehicles. So, once again, that is something that could be implemented immediately.

Now I would like to turn to recommendations concerning cargo security. We need better information about cargo transiting the ports. On the import side, the information is often vague, and import entries may be filed 5 days after arrival. On the export side, information is likewise often vague and is required 10 days after export. As the Seaports Commission noted, consolidated shipments often contain no information on what is included in a container, listing the cargo as "various" or "assorted merchandise."

The Port and Maritime Security Act would tighten up on the timeliness by requiring information on imports to be provided prior to importation and information on exports to be provided within 24 hours of when cargo is delivered to the marine terminal operator. However, the legislation does not address the specificity of the information, which goes to comments from the earlier panel about targeting. A concern with providing more detailed information is that it would allow high-value cargo to be targeted for theft by those with access to the information.

One solution might be to tighten up on existing requirements. The Seaports Commission studied compliance. In a 1999 study, Customs found a 53 percent discrepancy rate for ship manifests in terms of the number of containers on board. Over half of the vessels had either more or fewer containers on board than were reported.

There are also numerous instances of people being smuggled in containers. You told us about the Al-Qaeda operative, Farid. Unfortunately, it is a common occurrence for illegal aliens to be smuggled into the United States in containers. The Seaports Commission catalogued literally hundreds of these situations. It used to be

that these individuals were smuggled relatively short distances, but now they are coming long distances. In Los Angeles, Immigration arrested 30 illegal aliens in containers that had come all the way from China.

Clearly, we do not have a handle on how many containers are transiting our seaports or on what is in those containers. The Seaports Commission found that lax compliance and non-compliance may be related to penalties. The maximum penalty for incorrect information is $1,000. The Seaports Commission noted that carriers appear to treat the penalties as a cost of doing business. If the Congress legislated higher penalties, compliance probably would improve.

Last, I would like to mention data issues, starting with the basics. In analyzing crime at the seaports, the Seaports Commission encountered a lack of data. The Commission recommended that databases be modified to ensure the collection and retrievability of data relating to crime at the seaports. The Port and Maritime Security Act does not address this issue. The Congress could task an agency with responsibility for data gathering and provide the resources. With better data, law enforcement agencies could identify patterns and weaknesses at particular ports.

I would like to close with a statement in the Commission's report: "A terrorist act involving chemical, biological, radiological, or nuclear weapons at one of these seaports could result in extensive loss of lives, property, and business, affect the operations of harbors and the transportation infrastructure, including bridges, railroads, and highways, and cause extensive environmental damage."

We need to take action now to reduce the risk of future catastrophes. Thank you for inviting me to testify.

[The prepared statement of Ms. DeBusk follows:]

STATEMENT OF F. AMANDA DEBUSK, FORMER ASSISTANT SECRETARY FOR EXPORT ENFORCEMENT, UNITED STATES COMMERCE DEPARTMENT

Chairman Feinstein, Senator Kyl, members of the Committee, I am honored to be here today. I am speaking to you as a former Commissioner on the Interagency Commission on Crime and Security in U.S. Seaports. President Clinton established the Commission by Executive Memorandum on April 27, 1999. I served on the Commission as the Commerce Department representative in my capacity as Assistant Secretary for Export Enforcement.

Senator Bob Graham was instrumental in the creation of the Commission. Chairman Feinstein testified before the Commission on February 16, 2000 at a hearing in San Francisco. Senators Hollings and Graham introduced legislation implementing many of the Commission's recommendations. That legislation passed the Senate on December 20 as the Port and Maritime Security Act of 2001.

Today I would like to highlight the Commission's recommendations that are most important for this Committee and that are not completely addressed in the Port and Maritime Security Act. Let me begin by providing some context for the Commission's study. The Seaports Commission was looking at terrorist threats in connection with the events celebrating the New Millennium. We were concerned about how wide open our seaports are compared to our airports. In most cases, there is easy access to the seaports.

Criminal activity at the seaports is a big problem. The Commission found that significant criminal activity was taking place at most of the 12 seaports surveyed. One of the cases my former office investigated involved a riot control vehicle that was exported to China as a fire truck. The vehicle resembled a tank and had a turret for spraying pepper gas. It was exported in a container, and no one knew at the time of export what was inside. If someone can smuggle a tank through a seaport, it does not make us feel secure about catching chemical weapons or a nuclear bomb.

The Commission found that the state of security at seaports generally ranged from poor to fair, with a few exceptions where the security was good. The Commis-

sion made recommendations that, if implemented, would go a long way in combating terrorism at our seaports. I will discuss some recommendations on physical security, cargo security and data needs.

First, concerning physical security, the Commission provided recommendations on minimum physical security standards covering fences, lights, gates, restrictions on vehicle access, restrictions on carrying firearms, the establishment of a credentialing process, considering criminal background checks for those with access to sensitive areas of the port, and development of a private security officer certification program. The Port and Maritime Security Act provides for the development of Maritime Facility Security Plans that would address these physical security issues. To develop and implement these complex plans is likely to take a long time. While there is authority for interim security measures, there are no standards for these measures. An alternative might be to immediately put in place minimum standards identified by the Commission and permit waivers if a seaport had a good reason not to implement a particular requirement.

For example, we could immediately put in place a restriction on carrying guns at seaports. It makes no sense to prohibit nail clippers at airports, but allow guns at seaports. Of the 12 seaports surveyed by the Commission, not a single one restricted firearms. To my knowledge, this situation has not changed. The Seaports Commission, composed of officials from federal agencies involved in law enforcement at the seaports, recommended restrictions on firearms except for law enforcement personnel.

Another example of a basic physical security requirement that could be immediately implemented is the restriction on private vehicle access to the ports. At many ports, access is virtually uncontrolled. At one of the ports I visited, we saw a line of vehicles parked right beside the vessel. We were told that these were the dockworkers' vehicles parked there for convenience. At the time, we were concerned that the vehicles could be hiding places for smuggled drugs. Today we must consider the possibility that a car bomb or a "dirty nuclear weapon" could be hidden in those vehicles.

Now I would like to turn to recommendations concerning cargo security. We need better information about cargo transiting the ports. On the import side, information is often vague and import entries may be filed 5 days after arrival. On the export side, information is likewise often vague and is required 10 days after export. As the Seaports Commission noted, consolidated shipments often contain no information on what is included in a container, listing the cargo as "various" or "assorted merchandise."

The Port and Maritime Security Act would tighten up on timeliness by requiring that information on imports must be provided prior to importation and information on exports must be provided within 24 hours of when cargo is delivered to the marine terminal operator. However, the legislation does not address the specificity of information. A concern with providing more detailed information is that it would allow high value cargo to be targeted for theft by those with access to the information.

One solution might be to tighten up on existing requirements. The Seaports Commission studied compliance issues. In a 1999 study, Customs found a 53% discrepancy rate for ship manifests in terms of the number of containers on board. Over half of the vessels had either more or fewer containers on board than were reported.

There are numerous instances of people being smuggled in containers. Customs Commissioner Bonner reported in a recent speech that Italian authorities found a suspected Al Qaeda operative locked in a shipping container bound for Canada. Inside the container, the suspect had a bed, a bathroom, airport maps, security passes and an airport mechanic's certificate.

Unfortunately, it is a common occurrence for illegal aliens to be smuggled into the United States in containers. The Seaports Commission catalogued literally hundreds of these situations. It used to be that these individuals were smuggled relatively short distances, mainly into the Port of Miami, but this is not the case any more. In Los Angeles, Immigration arrested 30 illegal aliens in containers that had come all the way from China.

Clearly, we do not have a handle on how many containers are transiting our seaports or on what is in those containers. The Seaports Commission found that lax compliance and non-compliance may be related to penalties. The maximum penalty for incorrect information is $1000. The Seaports Commission noted that carriers appear to treat the penalties as a cost of doing business. If the Congress legislated higher penalties, compliance probably would improve.

Last, I would like to mention data issues. In analyzing crime at the seaports, the Seaports Commission encountered a lack of data. The Seaports Commission recommended that databases be modified to ensure the collection and retrievability of

data relating to crime at the seaports. The Port and Maritime Security Act does not address this issue. The Congress could task an agency with responsibility for data gathering and provide the necessary resources. With better data, law enforcement agencies could identify patterns and weaknesses at particular ports.

I would like to close with a statement in the Commission's report: "A terrorist act involving chemical, biological, radiological, or nuclear weapons at one of these seaports could result in extensive loss of lives, property and business, affect the operations of harbors and the transportation infrastructure, including bridges, railroads and highways, and cause extensive environmental damage." We need to take action now to reduce the risk of future catastrophes. Thank you for inviting me to testify on this important subject.

Chairperson FEINSTEIN. Thank you. Excellent testimony, and we will talk to you more in our Q&A period.

Let me just go on and introduce now Mr. Kim Petersen of the Maritime Security Council. He serves as the executive director of the Security Council. He has over 22 years of experience in domestic and international security and anti-terrorism activities. He has directed operations for former U.S. Secretaries of State Henry Kissinger and Alexander Haig and served as the senior staff member in both the United States Senate and the Defense Department.

Welcome, Mr. Petersen.

STATEMENT OF KIM E. PETERSEN, EXECUTIVE DIRECTOR, MARITIME SECURITY COUNCIL, FORT LAUDERDALE, FLORIDA

Mr. PETERSEN. Thank you, Madam Chair. As the executive——

Chairperson FEINSTEIN. And before you start, what we are really interested in—and maybe this might—are suggestions. You know, Ms. DeBusk did it, things we might do legislatively to tighten up our system. So if you have——

Mr. PETERSEN. I have lots of them.

Chairperson FEINSTEIN. Good.

Mr. PETERSEN. As the executive director of the Maritime Security Council, I am pleased to have the opportunity to address the committee today and relate the views and concerns of our membership. I also ask that my written testimony be entered into the record, and I will provide a few brief remarks.

Chairperson FEINSTEIN. It will. Thank you.

Mr. PETERSEN. As background, the Maritime Security Council was created in 1988 to address the many security concerns of the U.S. and international maritime community. We are a member-driven organization representing 65 percent of the world's shipping that works closely with United States Government agencies concerned with maritime security and counterterrorism. Our mission is to advance the security interests of the international maritime community against terrorists and other transnational criminal threats.

In addition to being the principal clearinghouse for the exchange of information between its carrier members, the MSC also acts as a liaison with regulators and governments offering vital intelligence on crimes at sea and information on security conditions in foreign ports. The Maritime Security Council has been designated as a maritime security advisor to both the U.S. State Department and Interpol, the international police organization.

It is important to acknowledge that the maritime industry, both the sea carriers and the ports, have been working for years to address the issue of crime and security in the maritime environment.

The passenger cruise industry unilaterally developed and implemented security control and accountability measures designed to mitigate or deter criminal activity through the identification and exclusion of unauthorized personnel. Some States, most notably Florida, had begun extensive port security programs that have become models for the rest of the Nation.

However, subsequent to the terrorist attacks of September 11, the maritime industry's focus changed from mitigation of criminal activities to the prevention of terrorism. This has had the effect of directing resources at a new and more complex threat while at the same time providing viable safeguards against criminal concerns, such as container theft, drug smuggling, and conspiracies to bring in illegal aliens.

While it is readily accepted that our seaports are a critical component of the U.S. national infrastructure, a clear understanding of how these engines of commerce are protected is not so readily appreciated. What is of surprise to many is that it is not the Federal Government that is providing security for the Nation's seaports but, rather, it is local governments and port authorities coupled with local law enforcement and private security companies. Were it not for local governments protecting the seaports themselves, Federal agencies such as INS, Customs, and the Coast Guard would not be able to perform their mission. Therefore, it is of significant concern to the Maritime Security Council that the extraordinary needs of port authorities and local governments for funding to perform fundamental security operations not be overlooked when monies for security enhancements and recurring operational costs are being allocated. Absent State-directed funding and Federal reimbursements for completed security capital improvements, we can expect that many ports will simply be unable to meet the many ongoing challenges created as a consequence of the horrible events of September 11.

As I testified before the U.S. Senate's Commerce Committee in October, it would be a catastrophic mistake for us to consider U.S. borders and coastlines as our first line of defense against foreign-based foes. In addition to enhancing domestic seaport security measures, the Maritime Security Council believes it is critical to push back the boundary of homeland security to foreign ports of origin. Particularly in an age of increasingly available weapons of mass destruction, it must be seen as a dangerous policy to await the arrival of suspicious cargo into an American seaport before it is subjected to a first round of scrutiny.

I understand your concerns, Madam Chair, about the potential of container inspections being subverted in ports such as Karachi. It is, therefore, our recommendation that a program analogous to the Federal Aviation Administration's Foreign Airport Security Assessment Program be developed and funded. A Foreign Seaport Assessment Program in tandem with a prescreening program, as recommended by U.S. Customs and the Maritime Administration, would need to identify those ports that fail to meet minimum security standards with such standards being agreed to through the UN's International Maritime Organization. The next critical element would be for the U.S. to spearhead a program that would provide technical assistance and, where necessary, financial help to

those ports that serve as potential points of origin for those bent on harming American interests.

The Maritime Security Council recommends to this committee that every port of origin with ships bound for a U.S. destination should be audited at least once every 3 years, with non-compliant ports being audited annually until they reach compliance. Implementation of this program, and the sanctions that would become a part of it, will create a self-sustaining financial incentive for compliance with these new international port security standards.

In conclusion, the Maritime Security Council thanks you, Madam Chairwoman, and the other members of the subcommittee for the opportunity to provide this testimony. We stand prepared, as we always have, to assist the committee and its staff in these important efforts, and we will be dedicating a significant portion of the International Maritime Security Conference, which we are holding in Fort Lauderdale on March 6th through 8th, to discuss the issues raised in this hearing.

Thank you.

[The prepared statement of Mr. Petersen follows:]

STATEMENT OF KIM E. PETERSEN, EXECUTIVE DIRECTOR, MARITIME SECURITY COUNCIL, FORT LAUDERDALE, FLORIDA

Thank you Chairman Feinstein and members of the Committee. As the Executive Director of the Maritime Security Council, I am pleased to have this opportunity to address the committee today to relate the views and concerns of our membership.

BACKGROUND

The Maritime Security Council was created in 1988 to address the many security concerns of the US and international maritime community. We are a member-driven organization that works closely with United States government agencies concerned with maritime security and counterterrorism. Our mission is to advance the security interests of the international maritime community against terrorist and other transnational criminal threats. The MSC represents maritime interests before government bodies; works in partnership with industry and government; disseminates timely information to its members; encourages the development of industry-specific, task-appropriate security technologies; and, convenes conferences and meetings for the membership.

The MSC has established partnerships with a number of these agencies to prevent or respond to a wide range of transnational criminal activities, including terrorism, illegal drug trafficking, piracy, theft, and trafficking in human cargo.

In addition to being the principle clearinghouse for the exchange of information between its carrier members, the MSC also acts as a liaison with regulators and governments offering vital intelligence on crimes at sea, and information on security conditions in foreign ports. The Maritime Security Council has been designated as a maritime security advisor to both the US State Department, through its Overseas Security Advisory Council, and Interpol, the international police agency. As a consequence of these roles, the MSC was called on to assist in the development of US Sea Carrier Initiative and Super Carrier Programs and was instrumental in helping develop sections of the Port, Maritime, and Rail Security Act of 2001.

MARITIME INDUSTRY ACTIONS

It is important to acknowledge that the maritime industry, both the sea carriers and the ports, have been working for years to address the issue of crime and security in the maritime environment. The passenger cruise industry unilaterally developed and implemented access control and accountability measures designed to mitigate or deter criminal activity through the identification and exclusion of unauthorized personnel. Some states, most notably Florida, had begun extensive port security programs that have become models for the rest of the nation.

However, subsequent to the terrorist attacks of September 11, the maritime industry's focus changed from mitigation of criminal activities to the prevention of terrorism. This has had the effect of directing resources at a new and more complex

threat, while at the same time providing viable safeguards against criminal concerns, such as container theft, drug smuggling, and conspiracies to bring in illegal aliens.

THREATS AND CHALLENGES TO MARITIME HOMELAND SECURITY

While it is readily accepted that our seaports are a critical component of the US national infrastructure, a clear understanding of how these engines of commerce are protected is not so readily appreciated. What is of surprise to many is that it is not the federal government that is providing security for our nations seaports, but rather it is local governments and port authorities coupled with local law enforcement and private security companies. Were it not for local governments protecting the seaports themselves, federal agencies such as INS, Customs, and the Coast Guard would not be able to perform their mission. Therefore, it is of significant concern to the Maritime Security Council that the extraordinary needs of port authorities and local governments for funding to perform fundamental security operations necessary not be overlooked when monies for infrastructure security enhancements and recurring operational costs are being allocated. Absent state-directed funding and federal reimbursements for completed security capital improvements, we can expect that many ports will simply be unable to meet the many challenges created as a consequence of the horrible events of September 11.

MARITIME HOMELAND SECURITY: WHERE DOES IT BEGIN?

As I testified before the US Senate's Commerce Committee in October, it would be a catastrophic mistake for us to consider US borders and coastlines as our first line of defense against foreign-based foes. In addition to enhancing domestic seaport security measures, the Maritime Security Council believes it is critical to push back the boundary of homeland security to foreign ports of origin. Particularly in an age of increasingly available Weapons of Mass Destruction, it must be seen as a dangerous policy to await the arrival of a suspicious cargo into an American seaport before it is subjected to scrutiny.

A program analogous to the Federal Aviation Administration's foreign airport security assessment program needs to be developed and funded. A foreign seaport assessment program would need to identify those ports that fail to meet minimum security standards with such standards being agreed to through the UN's International Maritime Organization. There is presently movement in that direction by the US Coast Guard, the Department of Transportation, and organizations such as the Maritime Security Council in meetings with the IMO in London. The next critical element would be for the US to spearhead a program that would provide technical assistance and, where necessary, financial help to those ports that serve as potential points of origin for those bent on harming American interests.

The Maritime Security Council recommends to this Committee that every port of origin with ships bound for a US destination should be audited at least once every three years, with non-compliant ports being audited annually until they achieve compliance. Implementation of this program, and the sanctions that would become a part of it, will create self-sustaining financial incentives for compliance with these new international port security standards.

TRAINING AND CERTIFICATION OF MARITIME SECURITY PROFESSIONALS

The Maritime, Port and Rail Security Act of 2001 creates a mechanism for establishing training and certification standards for maritime security professionals. It creates the Maritime Security Institute, under the direction of the Federal Law Enforcement Training Center, as an international center for training and certification. This program would also be open to foreign personnel responsible for managing port or vessel security operations. The Maritime Security Council is proud to have been instrumental in this component of the Act and we believe it will prove to be one of the significant legacies of this legislation.

CONCLUSION

The Maritime Security Council thanks you, Madam Chairwomen and the other members of the Committee for the opportunity to provide this testimony. We at the MSC stand prepared, as we always have, to assist the Committee and its staff on its important efforts, and we will be dedicating a significant portion of our International Maritime Security Conference, being held in Ft. Lauderdale, March 6–8, 2002, to discuss the issues raised in this hearing.

Thank you.

Chairperson FEINSTEIN. Thank you very much. I have got a burgeoning question, but I will wait.

It is a pleasure for me to welcome Mr. Rob Quartel of FreightDesk Technologies. He is the chairman and CEO of this company. The company is a leading provider of Internet-based cargo applications for international cargo management. He is also a former member of the United States Federal Maritime Commission and is recognized as an expert in international maritime and U.S. national transportation policy.

Mr. Quartel, if you would do the same thing, if you could enter your statement in the record and just kind of talk on where you see the picture and what you think could be done to be helpful.

STATEMENT OF ROB QUARTEL, CHAIRMAN AND CEO, FREIGHTDESK TECHNOLOGIES, INC., AND FORMER MEMBER, UNITED STATES FEDERAL MARITIME COMMISSION, MCLEAN, VIRGINIA

Mr. QUARTEL. That would be great. Do you have a copy of the slides, Senator?

Chairperson FEINSTEIN. I do not.

Mr. QUARTEL. I wonder if there is a way we can get this so you can see it. But I would like to enter the statement into the record.

Let me begin by saying I endorse almost all of the actions that people on this panel and the earlier panel have talked to about what you do about a port, and I think we all have seen each other in different contexts.

When I walked in here, I said to Deputy Commissioner Tischler, who I had not met—and I was glad to meet her—that I was the author of the concept, or at least the first person——

Chairperson FEINSTEIN. Oh, you are the author of pushing the borders——

Mr. QUARTEL. Pushing the border back.

Chairperson FEINSTEIN. Oh, you have a doubting Tomasina here.

Mr. QUARTEL. Well, she said she was the author. She said she had thought of it first, and after that, I think I will let her be the author.

Chairperson FEINSTEIN. Oh.

Mr. QUARTEL. But, in point of fact, it is something that woke me up in the middle of the night, not long after September 11th, thinking about the volume of trade, how it actually operates, and really that is kind of what I would like to talk about today.

I am going to skip through a couple slides because I think it goes to this. Everything that people have talked to in terms of technology—seals, all of that kind of stuff—I endorse. But let me just say that you can seal containers, you can inspect the ports, you can put more guards, you can get rid of guns, you can do all of the physical things to a port; but none of that would stop a weapon of mass destruction from going under the Golden Gate Bridge and blowing up. It is a little bit like a ball player with a mitt and another guy with a hand grenade. The port is the guy with the mitt. Do you want to be the guy with the mitt? Is that going to stop the hand grenade?

The game here, the technology, is to stop the hand grenade before it ever gets lobbed at the port, and I think that is why it is

a combination of technologies. It is a net to capture if it gets to the port, it is the technology to stop it——

Chairperson FEINSTEIN. Let me stop you, because this thing seems so flawed to me because you can't—if you do, let's say, 12 ports, the big ports——

Mr. QUARTEL. That is not enough.

Chairperson FEINSTEIN. It is a signal to everybody. You don't ship a tactical nuclear weapon through a big port. You go to a small port. So, I mean, how does this solve anything by pushing the borders back?

Mr. QUARTEL. Well, you are exactly right, but I think we need to define what we mean. We don't mean physically pushing the border back, and I don't think most people mean actually inspecting a container.

If you take a quick look at this first slide, this is what international trade looks like. Typical international trade has in it 20 to 30 parties, 30 to 40 documents. It spews data, a couple hundred data elements all across the process. And I think if you want to deal with a container coming in with a bomb, you have to think about it as a piece of the process.

The Coast Guard has defined what they call maritime domain awareness, which is being aware of the domain around the port, all critical, all important. When I think about international trade, there are really five domains. There is the beginning of the cargo, when you have got manufacturers and other people who are putting it in the container and moving it to a port of lading overseas. You have got that port, which has security issues. You have it in motion, over the ocean or in the air, or anything else. You have the port of discharge in Los Angeles, for example. And then you have an inland movement, and really what we are talking about here is a piece of the onion. You know, this is a process like an onion. There is one thing you do, then another thing you do, then another thing you do, layer on layer on layer.

The quickest, frankly easiest thing you can do is to start to capture information, not just data but information on a cargo. And you can do that from the minute someone orders it. Every purchase overseas generates a purchase order from someone in the United States. And, Senator, this is the kind of stuff that is not now done.

If you want to export something to Osama bin Laden, there is a denied party list that says you can't do it——

Chairperson FEINSTEIN. He is not going to buy a tactical nuclear weapon at Wal-Mart.

Mr. QUARTEL. Right.

Chairperson FEINSTEIN. You know, he is going to buy it from some Russian black marketeer.

Mr. QUARTEL. Absolutely. But if I wanted to export something to him from the United States, he is on a denied list. And I am simplifying it. But there is no comparable list that says he couldn't send it to us. So that is kind of a first level of data check and kind of the data concept. This is not just stopping it at the port. The data concept is to start gathering commercial intelligence which can tell you about the container, the shipments in it, the people who touched it, who paid for it, where it went, where it is going. For example, the kind of stuff I would want to know before it ever

got to the United States is not whether necessarily it originated in Karachi, but did it originate in Malaysia via Indonesia where you have Muslim dissidents, slipped into the mainstream of one of these 12 ports, by the way, you know, one of the biggest ports shipping to California, and it is somehow going to get on a train, once it gets through the port, and go all the way to New York and go by Yankee Stadium when the President of the United States is throwing out the ball.

So it is not just the what of it that you want to capture in data, and the contents. It is also the situation. And the only way you can do that is by capturing a set of commercial information and a set of law enforcement and national security information.

And you asked the question, correctly, do we have a single place in the United States Government that captures and processes this data, and the answer is no. You know, you have got Customs. You have got DOT. You have got Coast Guard. You have got Office of Naval Intelligence. You have got DOD. You have got all of these guys taking a little piece of the problem——

Chairperson FEINSTEIN. They are all afraid to say it isn't adequate now.

Mr. QUARTEL. Right, absolutely. So when I look at it, you create a commercial database which plugs into the commercial system. Remember, it is spewing data; every piece of data you would ever need is available somewhere before it ever hits the first ship.

You want to put together law enforcement and national security data——

Chairperson FEINSTEIN. You are talking about contraband data now?

Mr. QUARTEL. No. This is data on the situation. For example, Customs captures the manifest, the ship manifest. Half of what is on a ship is called FAK, "freight all kinds," which means that it was placed there, it doesn't say what is in the container. And in the other half of the data, it is wrong half the time. Okay? So to collect the ship manifest, I would have before this hearing said it is great, it at least tells you what is supposed to be on the ship. Well, 53 percent of that doesn't—you know, is wrong, too.

On the other hand, if you capture a purchase order, it tells you who bought it and who paid for it and what it is they wanted to get and when they wanted it shipped and who they were going to have it moved by. If you capture the transportation data, you can find the truck that was hired out of Malaysia to move it to the rail, the rail that was hired to move it to the ship, the ship—okay, you have got the ship, Customs and Coast Guard, Coast Guard has data on who owns the ship and who all these guys are. It is not in one place, but that is the process.

Chairperson FEINSTEIN. But there is no purchase order on this stuff we are talking about.

Mr. QUARTEL. Everything, everything in international trade, originates with a purchase order. The issue is that the purpose order, yes, is falsified. So what you have to do—and this, you know—I collect data. I am not the guy who would run the algorithm. But what we know is that if you—here, I will give you another quick chart here, and I will shut up so you can get to the other people here. But you may have a cargo listed as steel rebar

out of Poland. Other data will tell you that steel rebar is not made in Poland. That is a very simple check. So you know that that is a falsified purchase order or falsified manifest or bill of lading.

Chairperson FEINSTEIN. Now, who knows that? Who is getting that data? The port?

Mr. QUARTEL. Customs could know—well, no one gets all this data right now, except the shipper. Kind of one of the messages I would like to get to you and the Congress is that shippers and buyers and sellers in international trade—and this is how I make my living, and other companies like us. They want visibility. They want to know that they are going to get what they ordered, that it is going to get there when they want it. They want to know that it is using the transportation they have selected. They may have negotiated a contract. Eighty percent of what goes on there is actually subcontracted out to freight forwarders and third-party logistics providers. They want the same information.

So people are gradually wanting all the information in the commercial sector that I believe the Government would need to be able to profile a cargo.

So if I have one message, it is that all the data is there to be able to make decisions. It is not all caught in one place, but it is being generated by the commercial process, and the Government can get engaged in it. So when we talk about profiling, profiling just helps you select which ones you want to inspect in Rotterdam and whether you have a Customs guy doing it or whether you have the Dutch doing it or somebody else. It gets you to a point of intercept, okay? And that is really where you want to stop it. That is the way you are going to protect the U.S. port.

I would be happy to talk to all of this in all detail. I have, you know, charts on when the data comes in and everything else. But a notion of profiling is not that that is the end. That is really the beginning. It is trying to stop the guy from throwing it.

Chairperson FEINSTEIN. So you are saying that nothing gets on a ship without a purchase order, and if it is an illicit—if it is contraband of any kind, the purchase order is forged, and that the key is to get at the forgery.

Mr. QUARTEL. Right. That is correct. You want to get at——

Chairperson FEINSTEIN. I want to ask—but we have a vote, and I have about 10 minutes to get to the vote. What I would like to do, if we could, is hear from Mr. Upchurch, and then take a brief recess, and then come back, because it is just us, and have an opportunity to discuss this. And I would like your reaction to that purchase order issue, Mr. Steinke, if we could. So let's just move on to Mr. Upchurch.

[The prepared statement of Mr. Quartel follows:]

STATEMENT OF ROB QUARTEL, CHAIRMAN AND CEO, FREIGHTDESK TECHNOLOGIES AND FORMER MEMBER, U.S. FEDERAL MARITIME COMMISSION

I would like to thank the members of this Committee for their invitation today. I'll begin with an assertion that I think should be made policy:

- Every container destined to enter or pass through the United States should be treated as a potential weapon of mass destruction; every ship that carries it as a delivery device; and every port and point inland as a potential target.

While the discussion here today focuses on protecting the port—natural given the legislation before the committee—the port, frankly, is the least of the problem.

Yes, it's important to protect the security of the physical infrastructure, yes we have to worry about the safety of specialized vessels and guard against attacks like those which took place on the USS Cole, yes, the technology for sealing and tracking containers is important. But in terms of the system of intermodal international trade—shipping, moving goods around the world in international trade—the port of entry is just one—not even the most important—piece of the puzzle.

If you think about trade as a process of integrated pieces, then the port should be considered the point of last—not first—resort in our war on trade terrorism.

To be blunt about it, nothing we have heard discussed today—whether it's electronic seals or port inspections or beefed up patrols or biometric-aided identification cards or GPS or other physical tracking devices on containers or earlier reporting of a ship manifest or neutron scanning 2 percent or 20 percent of all containers going to the United States—whatever—has more than a small probability of stopping a determined terrorist from slipping a lethal shipment into the mainstream of international commerce and driving it under the Golden Gate Bridge to an end that none of us would like to see.

That's because the action starts well before the port.

So, focusing on stopping a weaponized cargo at the US port is too little, too late: The port is a potential target, not just a gateway. Ports have little interaction with cargoes other than to lift them off or on the ship, to store them, or to serve as a border funnel for customs activities. Their job is in some respects no different than that of a rail yard or similar intermodal exchange node. They are either efficient pass-throughs, propelling cargoes on their way to their final destination—or, they may become bottlenecks, driving some 20 percent of the national economy into the ground.

If we can't allow a weaponized container in a port, neither can we allow it on the ship, the principal means of delivering goods in intercontinental trade to the United States. Ships suspected to carry these weapons—some ships of which today carry the equivalent of 6500 or more containers—can only be turned back to the point of embarkation—not stopped, searched, and accessed for removal of an 8x8x48 foot 20-ton container while on the high seas

- Interdiction of terrorist activities really needs to begin at the beginning—with the shipper and his customer, at both the physical and transactional start of an order.

While I fully support the measures designed to protect our seaports contained in this legislation, I suggest to this committee that the first line of defense in the future isn't the traditional physical border the port represents, but a new technology border—a virtual, electronic border—that we need to push back overseas.

So, when we talk about technology in this hearing, I think we have to talk about information technology, first—because THAT is the first line of defense for our ports.

The fact of the matter is that we can't inspect every one of the 17,000 containers that end up in the United States on any given day, either here or in the overseas ports in which they originate, without destroying the fabric of our economy. But we CAN create a hierarchical approach combining physical inspection, human trust procedures and a new process of early electronic inspection employing the latest in information technologies.

Why is this electronic border a necessary approach? If I can, let me turn your attention to a couple of slides.

This first slide illustrates a key point: International trade is a tremendously complex business. A typical trade will have as many as 20–25 involved parties—buyers, sellers, inland transporters on both sides of the ocean, ocean and other water carriers, middlemen, financiers, governments and others—and will generate 30–40 documents. Some 6 million containers, many carrying cargoes for multiple owners and valued on average at $60,000 each, entered the US in the year 2000, on ships carrying from 3–6000 containers each. If we were to add a physical inspection to one of the very large ships carrying these cargoes to the US through the world's hub ports—the Regina Maersk, for example—a single hour's delay per 20-foot container would add from 150–250 man-days (roughly 1½ to 3 man-years of work shifts) to the time it took to offload the 6000 containers riding that one ship.

Literally millions of people and hundreds of thousands of companies worldwide are engaged in the business of moving cargoes internationally. In the US alone, there are an estimated 400,000 importing and exporting companies, 5,000 licensed forwarders and customs brokers, perhaps as many as 40,000 consolidators large and small, and millions engaged in the transportation industry. Worldwide, there are at

least in theory some 500 ocean carriers—although probably 10–15 carry 90 percent of cargoes shipped between continents—an estimated 50–70,000 forwarders and tens of thousands more intermediaries, not to mention several million companies moving goods.

This is a process that literally spews data—data on the contents, on who touched the cargo, who paid for it, where it's been, where it's going.

And it's a process into which commercial shippers—the people who own, buy, or sell a cargo—tap into daily, in one form or another, to collaborate on transportation and financial transactions, to exchange documents, to meet regulatory requirements of the various jurisdictions in which they operate, in addition, of course, to documenting the basic buy-sell transaction that begins the shipment.

So, when I look at what technology you need to protect a US port, I look back to the beginning of the process, before the port, before the ship, before the port of embarkation, before even sealing the container. I look to the buy-sell transaction and the purchase order that is generated from it. Then I look to the manufacturer or supplier overseas, his manufacturing and supplier processes, how and where he or a consolidator somewhere loads the container, when and how it was sealed, how it was moved, who touched it, who paid for it—and even where it might be going once the cargo reaches the United States. For the most part, every bit of that data is available—somewhere and in some form, but not necessarily captured in one place by the private sector, and certainly not by the US government—but there nonetheless, before the cargo ever gets loaded onto a ship bound for a US port.

Throughout this process, the shippers of the goods are for the most part physically out of control of the trade. They've hired freight forwarders or consolidators or third party logistics companies to handle the business because their expertise is in the manufacturing, marketing, and sale of the product. All they really care about at the gross level is that they get exactly what they ordered—no more and no less—and that it gets there at the time and price promised. Some have created intelligent order systems, spent millions of dollars on enterprise resource planning and automated customer service systems, and others have acquired or constructed internally services like those offered by my own company which allow them to track, measure, and steer the progress of their goods through the transportation chain, either physically or in terms of process and paperwork, the latter actually being more important in the manufacturing process than where something actually is. As long as they know it's on course, are apprised of delays, have the ability to re-plan a move or a manufacturing process in the event of a supply chain problem—than they are satisfied. That's really all they need.

The focus of logisticians and companies—particularly American companies—over the last several decades has been on making that flow faster, cheaper, more transparent, and faster yet. Our success at that provides an enormous competitive advantage to many of our companies and makes a huge contribution to the reduction in the cost of numerous articles and products crucial to everyday life in the United States.

Some in the government have suggested that, as in aviation, security rather than speed might provide the competitive edge for ports in the US in the future.

With all due respect, speed and cost were the two most important criteria for the selection of ports and transportation before September 11—and they will, for all but a handful of shippers—continue to be the most important criteria in the future.

There is a reason for that: Speed equals money.

Because the manufacturing system knows that, logistics costs have steadily declined from 25 percent to lower than 15 percent of GDP over the last 20 years. Carrying costs associated just with inventory at rest—goods in storage, the response of a manufacturer to uncertainties in the supply chain—in 2000 amounted to nearly $400 billion. A number of experts have estimated that just a five percent addition to the logistics process—thus causing an increase in inventories, the response industry will have to take in order to make up for slow processing times—would cost the economy an additional $75 billion annually. That's the equivalent, by the way, of some 75,000 jobs lost, not counting the multiplier effect of these wholly non-productive costs

Introducing uncertainty, slowing down cargoes through physical inspection of every container and every box inside it, otherwise derailing the transportation system, is exactly the opposite of what we should do if our goal is to maintain a healthy American economy.

So, the most critical piece of the technology solution to guarding our ports, in my mind, is this: Profile cargoes, just as we profile people in the passenger airline industry, before they ever get on the ship—or plane, truck, or train—bound for the United States and its ports.

The data that the private sector uses to make its processes more efficient is the same data that the United States government needs to understand the commercial processes underlying a cargo profiling process.

My second slide talks to that process, but in short form, it's pretty straightforward.

In the profiling scheme that I have suggested, commercial data would: (1) Be captured prior to loading of a container on a ship, train, plane, or truck in international commerce, from the shipper, consignee, intermediary, banks, and all others that had an interest in or touched or processed the shipment; (2) Combined with certain relevant law enforcement and national security information; and, (3) Be processed through a form of artificial intelligence (including evolutionary computing) to provide a "profile" for every container and shipment within it. The profiling process would generate a "go-no go" decision driving further actions—loading on a carrier, physical inspection, further profiling, etc.

The profile would be based not only on what the cargo was said to be, but where it came from, its likelihood of being what it is stated to be, who handled it from packing through transport to a port, who would be handling it afterwards, where it had been and where it was going, who had a financial interest in it, etc. The algorithm would need to consider not only fact-based data (eg, what the product was and who touched it), but situational data—eg, a container originating in an unstable country and passing by Yankee Stadium on the day and hour the President was scheduled to throw out the first ball.

Based on some probability calculus, the air, ocean, train, or truck carrier could be told that the government either felt the cargo was safe to carry—or—that further investigation, including perhaps a physical inspection, was necessary. If a carrier then loaded the cargo deemed safe and was later told enroute that the cargo might require further investigation, then the carrier—having cooperated with the USG on the pre-release process—should be held harmless from further government sanctions, although it might well have to divert the vessel prior to or on arrival in a US port. (Indemnification here is a form of positive coercion that avoids the extraterritoriality issue.)

If a carrier received notification that a shipment was suspect prior to loading, it should then be required to arrange to have the cargo physically screened, or disclose why not. Screening could be carried out by U.S. Customs officials stationed in overseas points, foreign officials subject to bilaterals and some level of performance auditing, or by the companies themselves, again subject to performance auditing and rigorous procedural standards. The actual inspection could take several forms, ranging from passively examining the container (neutron scanning, motion detection, etc), to employing radiological and chemical "sniffers," to breaking the seal and opening it up.

Each of these methods has costs, risks, and probabilities associated with it and would be employed differentially against the perceived calculated risk. Screening might, in many cases, consist merely of re-checking documentation for inconsistencies and communicating with those who provided the documents to clarify the issue. Breaking a seal would, however, require some form of indemnifying the carrier, including possibly an entry order to do so from US Customs. None of these actions, however, have to involve a foreign government. The United States has the authority to deny entry of vessels that it deems of risk to itself, and to deny entry of goods deemed illegal. Providing process incentives to carry out the inspection prior to leading the port or embarkation is a legitimate, effective form of positive coercion. In the end, however, there is no doubt that the support of foreign trading partners and international organizations should be solicited, if only because our leading trading partners are themselves potential targets and will no doubt feel the need for reciprocal protections.

This raises other issues, of course, one being the question of whether or not we would need to place US Customs inspectors inside foreign ports of embarkation. My answer is: Maybe yes, maybe no. US government agencies frequently place inspectors, expeditors, and agents inside the premises of companies in the continental United States, sometimes with and sometimes without the invitation of the private companies involved. Companies often place employees whose job it is to ascertain quality, manage logistics, and to perform other expediting services in the home facilities of suppliers or customers, again at the invitation of the parties. US Customs inspectors could certainly be stationed inside the facilities of major carriers and manufacturers overseas, at their invitation, without generating an official response from a foreign government, in order to provide processing capabilities. Carriers and manufacturers that did this—whether by invitation or by USG mandate—could legitimately be considered "trusted parties" and receive "fast lane" treatment on arriv-

al in Customs in the United States, assuming that proper cargo security procedures were employed across the length of the supply chain.

The bottom line, however, is that this is NOT about inspecting the majority of containers or shipments. The goal, in fact, is to use information technology to substantially reduce the need to physically inspect containers, and to do so at a point in the logistics process that is the least damaging to it economically, and at which diversion of a contaminated cargo can be safely accomplished without delaying other cargoes.

Nor, by the way, is this about enforcing US customs compliance rules overseas—something that frequently seems to be mistaken for the prevention of terrorism in many of the proposals placed on the table. This is about determining which cargoes might be a threat to the United States and its citizens, not about whether or not US tariff rules are complied with. The latter has only a little to do with helping to ascertain the former, which is largely a function designed for revenue capture. Not only are these not the same things, but, treating this process as a means of enforcing customs rules could actually undermine the anti-terrorism effort. A legal cargo can become a lethal cargo under the proper circumstances. Thus, treating this as a customs compliance problem not only doesn't solve the problem, it actually lulls the public and the USG into a dangerously false sense of security.

There are three important attributes to this solution and the approach I suggest. First and foremost, it taps into the existing commercial trade management process and leverages existing relationships into a new holistic structure. Second, it is potentially fully independent of the need for international cooperation, as it requires only the compliance of the US-side of the equation, particularly if process compliance was specifically designated to be the responsibility of the buyer, a suggestion I have made elsewhere. And, finally, it is an approach that makes the greatest use of the technologies being developed by the private sector for use by commercial customers in a normal but obviously complex operating environment.

All of this is easy to suggest, of course, and somewhat more difficult to implement.

But, to give you an idea of where we actually stand, four existing commercial documents already reported in one form or another to Customs and the Coast Guard can provide much—but not all—of the data that would allow us to profile a cargo based on contents, involved parties, and transport mode and path prior to its ever getting on a ship: (1) The Shippers Letter of Instruction; (2) Commercial Invoice; (3) Certificate of Origin; and (4) The carrier's Bill of Lading. To that I would add (5) financial data, perhaps captured through Letters of Credit or bank reporting; (6) Inland transportation leg information not now captured by ocean carriers or the government, on both sides of the supply chain; and perhaps additional information.

On the commercial side, database structures already exist that are designed to integrate data from disparate sources (for example, EDI transmissions, faxes, the web, and email) and that, in computer parlance, allow you to instantiate a fully attributed shipment. Why a shipment? Because trade moves in shipments, first, and only then in containers. From the standpoint of profiling, shipment records need to be fully attributed—meaning that they need to contain detailed information about the shipment including all of the parties that are involved in the transaction, the route/itinerary of the shipment, the items that are contained in the shipment, the events/status of the shipment and its financial terms and any other information that was thought necessary. And, the system needs to be able to collect, process and integrate this data and to provide the required normalized data elements to support container and risk profiling in support of Homeland Security.

Collecting and managing the commercial data isn't rocket science, although not a lot of us do it. But it is what the private sector is beginning to look for today.

Analyzing the data IS rocket science, however. But, again, the required processes are already in use inside the government and the commercial sectors alike—in everything from looking for illicit drug traffic to screening genetic samples for new drugs for medical purposes.

Without going into a lot of detail, the analytical process should be designed at the simplest level to check against lists—Denied Party Screening, for example; and at the most complex level to think, to learn, and to detect deviations from what we know in our own experience is normal in the operations of international transportation and manufacturing—anomalies captured in rules and facts which may pertain to both specific and general information, relationships between data, expectations and other expertise. Items that violate expectations or otherwise contradict human expertise are considered to be more suspicious.

But, of course, cargo profiling is only part of the solution. As should be evident from the above description, this is an onion, with numerous layers. At varying stages across the process we have to layer on passive and physical inspection, physical protection of the ports, protection of the cargo integrity from the basic risks of

international transport—spoilage, tampering, theft—the ability to interdict specific cargoes, tracking and visibility solutions, many of which we have heard about today—that allow us to maintain not only the integrity of the cargo but of the transport system itself once a cargo is in motion.

Cargo profiling is an approach and a system that I believe that the Transportation Security Administration at the US Department of Transportation already has the authority to implement—a question separate from whether or not they have the dollars to do so. (I would note that profiling would certainly cost far less and take less time to implement than a full system of inspections, electronic seals, etc.) TSA needs the support, almost in a sub-contracting role, of the US Customs Service, the US Coast Guard, the various modal agencies, and, perhaps the US Department of Commerce alike. The data base process could perhaps ultimately be embedded into and as an extension of the Automated Customs Enforcement (ACE) system that Customs is currently building—but which is scheduled to take another five years to deliver. The US Coast Guard and other national security and defense agencies also have extensive law enforcement and national security data base efforts going on, and numerous government data bases could be tapped through the new process for relevant data without violating the need to maintain the competitive position of individual companies and due process for the parties involved.

I don't believe, however, that we should or need to wait that long to implement a robust, commercially relevant, profiling solution. We should be looking—today—at other USG data bases, including the so-called ITDS system being developed several years ago at Treasury, outside of Customs, as a possible stopgap; and, we should be looking to the private sector as well for information technology accelerators. Several groups of commercial and governmental players have suggested demonstration projects that would cover ports and inland movements on both sides of the traffic on both the East and West Coasts, using commercially available information technologies and real-world data and cargo movements.

As a general comment here, I believe strongly that a critical issue here will be to obtain voluntary—not just mandatory—commercial compliance with all of the parties in the commercial transaction. Many of the processes covered here are outside the domain of US law enforcement. We can't today make foreign suppliers abide by all of these rules, but we can certainly tell their US customers—today—that they may face delays unless they know their sources and can validate cargo and process integrity. We can't today tell a foreign port that it has to purchase millions of dollars worth of screening devices for the cargoes destined for the US which our screening picks out as suspect, but we can—today—certainly negotiate procedural agreements through the IMO and individual American ports and distribution arms can provide speed incentives for those that work with us. The ocean carriers barely make 1–2 percent ROI, so they will only be driven into bankruptcy if we require that they purchase screening machines and add hundreds of new security personnel, but we may be able to help them through the imposition of a user charge on all cargoes going through US ports, a portion of which is used to offset their additional costs. We can't today mandate that the carriers for which the US is only one of several stops profile all of their cargoes before sailing; but we can no doubt—today—find a way to say that if we determine that a cargo is found to be suspect the entire ship will be turned back because we won't risk the US port.

In closing, I'd like to reiterate the point with which I began: US ports aren't the first line of defense but almost the last.

This Committee and this government have a real obligation to see that no weaponized container ever makes it to the port, period. They have an obligation to protect the integrity of cargoes once entered, and they have an obligation to their customers—the failure of which to provide will destroy their commercial viability and that of the general economy—to provide a speedy, low-cost transportation move. I believe we have the technical means to tap into the commercial process, to profile shipments and containers, and thus, in concert with other actions, to see that no container intended to be used as a terrorist device ever gets on a ship, a plane, a truck or a train bound for the United States. We have the technology to do it, but the process starts well before a container ever reaches a port.

Members of this Committee: When the aviation system went down on September 11, we already had a security system, as imperfect as it was, in place, which could be re-booted three days later at a higher state of readiness.

However—If a container blew at a port or somewhere else in the international transportation chain ending in the United States, this nation and its leaders would have no choice but to shut down the entire system of trade with our country. We have no security system in place in our international trade system comparable to that which pre-existed in passenger airline travel that we can re-boot. We have nothing at all in place to properly secure over $2 trillion in trade and the millions

of American jobs associated with it. Electronic seals, tracking, additional port security—none of that will solve that problem adequately. We DO have the technology available to begin to profile shipments aimed at the United States, today. It's not the complete solution, but it's an appropriate start.

Again, I appreciate the Committee's time, and would be glad to discuss it further.

SEVEN THINGS WE COULD BE DOING NOW TO PROTECT OUR PORTS:

1. *We should begin the process of moving to pre-movement data filing on the entire shipment process, including not only customs compliance filings, but transportation and financial data*. And, we should begin immediately to tighten the document process. Mandating reporting of a manifest four days out is only marginally useful. Better would be to mandate filing of all ship manifests for vessels with cargoes bound for the US at least 24 hours prior to embarkation from a foreign port, even if only in incomplete form, with confirmation at final departure. The reality of the ship manifest is that it is useful only to document what is believed was loaded on a ship or plane, as a chain of custody certification. Over half of what moves on ships moves "FAK" (Freight All Kinds), meaning that the carrier has no idea what is in the containers it carries. Of the remaining manifest data, at least half is likely to contain inaccuracies. Nevertheless, requiring pre-departure filing of a ship manifest will have a certain "Hawthorne Effect" on the process, meaning that paying more attention to it would induce behavioral changes in the process—ranging from fostering mistakes by individuals attempting to circumvent the process, to exposing inconsistencies in data filings, to reducing errors among those attempting to comply legally because of the presumed additional scrutiny by government officials.

2. *Shippers or consignees or their agents should be made legally responsible for complying with all data mandates on a timely basis.* We should consider the immediate implementation of a purchase-order entry system, in which individuals purchasing goods from overseas should file a notification of the purchase and expected entry date and related parties early in the process; and they should perhaps in return be given an import number against which all subsequent data and documentation is filed. This is not a suggestion for an Import License, which would require a new bureaucracy, but simply the assignment of a number for later data and cargo tracking.

3. *We should make better use of intermediaries in the international trade process*. Over 80 percent of all cargoes in international trade are outsourced in whole or in part to freight forwarders, customs brokers, NVO's, consolidators, 3PL's and other who are expert in the process. Most of these parties are already licensed by the US Federal Maritime Commisson; and their numbers are small (4000 forwarders, for example), so their activities could be monitored. Licensing procedures should be intensified, perhaps including the addition of background checks; and the licensing and oversight of these regulated entities moved to the US Customs Service where there are more and better resources for this activity. Forwarders and other licensed entities should be enlisted today, and issued a set of procedural scrutinizes NOW that would allow them to become part of the "watch" process.

4. *The US should consider adopting and mandating the use of the International Bill of Lading* owned by the International Freight Forwarders Association (FIATA) as a means of introducing consistency into cargo documentation.

5. *We should mandate conversion to electronic data transmission (whether by EDI, web, etc) from all modes and players in the transportation and trade process by a date certain.*

6. *The Transportation Security Administration in DOT should formally, publicly be placed in charge of the profiling and international trade process*. Transportation is the one constant in an international movement. The USCG, Customs, and the Office of Naval Intelligence should be enlisted as "sub-contractors" for various parts of the program. The US Department of Commerce should be considered as the point at which the PO Entry System is filed, and the place from which a "go-no go" decision is conveyed from the USG to a commercial carrier.

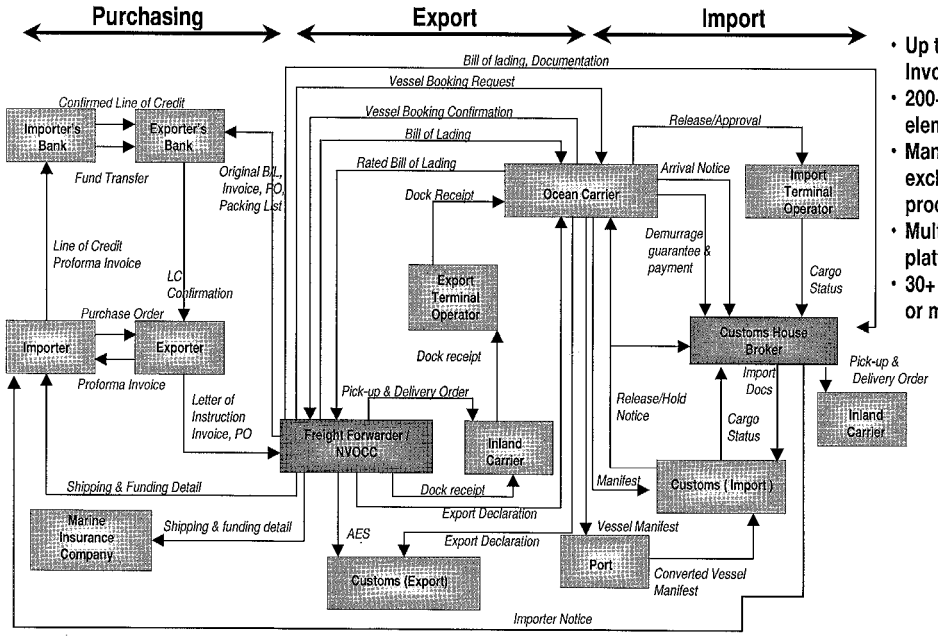
7. *We should begin immediately to test implementation of a container profiling process that originates overseas, using commercially available data base structures, algorithms, and knowledge*. The data issues contained in aggregating information on a cargo, its movements, the players that touch it, across multiple modes and legs, and transmitted by the variety of electronic and non-electronic means, have already been solved in large part by the private sector seeking to obtain transportation and supply chain visibility and control.

Pushing the Border Back

Using Commercial Data To Analyze Potential Terror Threats Posed by Inbound Container Traffic

FreightDesk
TECHNOLOGIES

Complex Data Flow for International Shipments

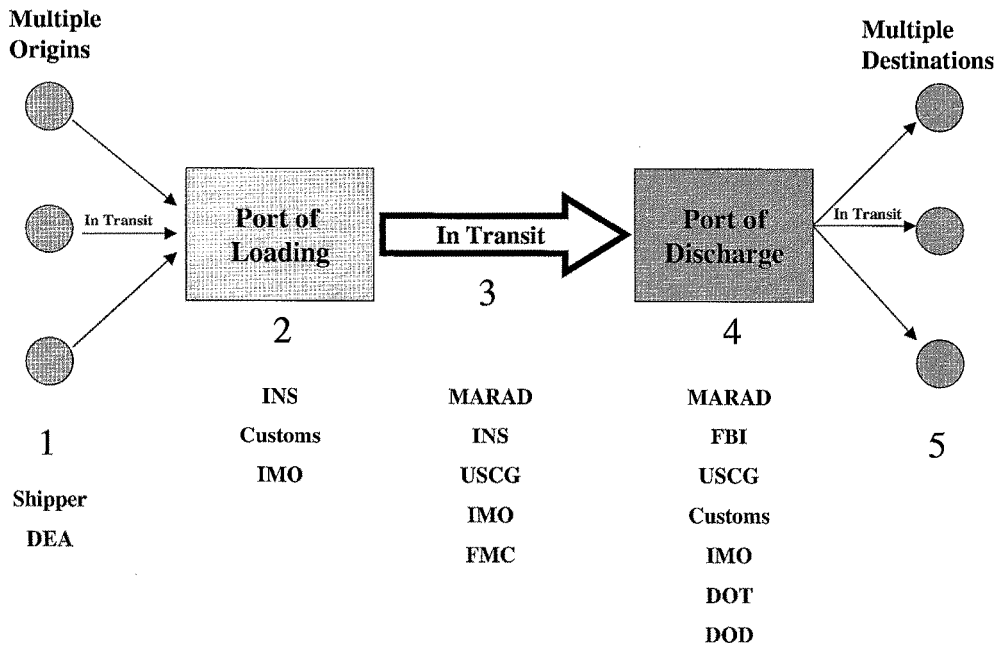


- Up to 20 Involved Parties
- 200+ data elements
- Manual data exchange processes
- Multiple data platforms
- 30+ documents or messages

FreightDesk TECHNOLOGIES

International Freight Movement: Five Domains

Domain Analysis can Suggest a Hierarchy of Responses and Responsibility

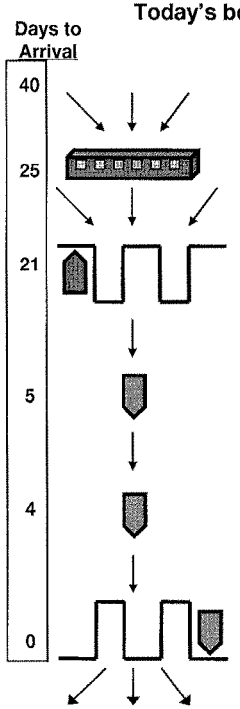


FreightDesk TECHNOLOGIES

Information Sources and Timing

Proprietary

Today's border is "fuzzy": data is reported at fluid times and not analyzed for threat

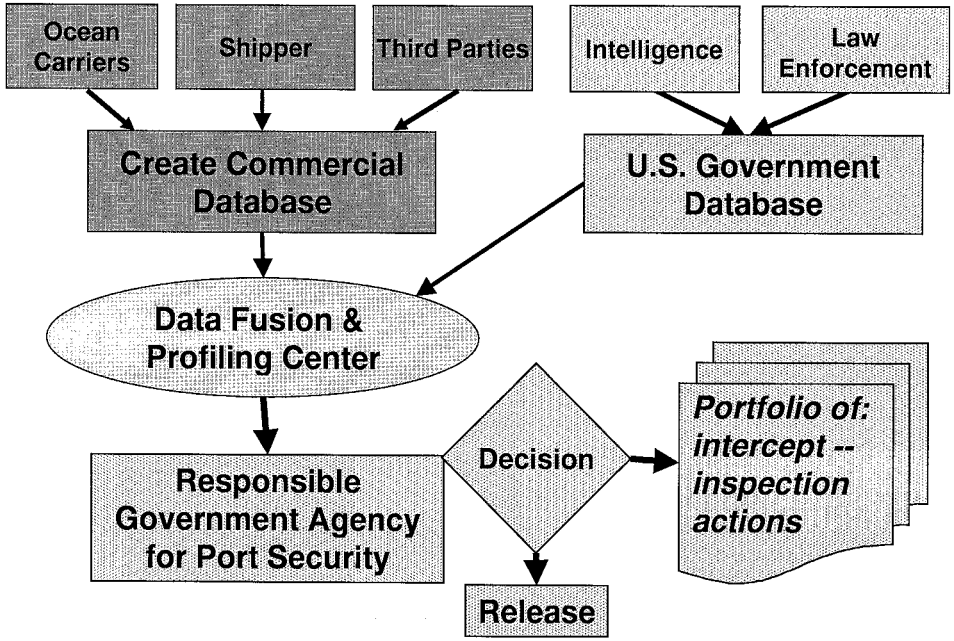


	Process Step	Source of Data
Seller	• Seller and Buyer agree	• Seller generates documents •*Shippers Letter of Instruction* • *Commercial Invoice*
Overseas Inland Consolidation Warehouse	• One or more consolidation layers mask goods' origins and involved parties (40%)	• Forwarder/consolidator generates documents •*House Bill of Lading*
	Virtual Border	
Foreign Port of Voyage Origin	• Carriers accept containers from multiple sources, with only partial data on contents and origins	• Carrier generates documents •*Master Bill of Lading*
Voyage Underway	• Earliest possible filing of U.S. Customs entry information (ABI)	• Customs broker and/or shipper reporting •*Customs form 7501 and 3461*
Carrier Reporting	• Ship manifest information must be filed by 4 days prior to arrival (AMS)	• Additional carrier reporting •*Shipment Status* •*Vessel Manifest*
First U.S. Destination Port	• U.S. Customs applies physical and commercial border in port zones	• Additional documents may finally be received here •*Surface Bill of Lading*
Buyer	**Border Today** Red documents reported to Customs	• Buyer generates Purchase •*Purchase Order*

Fluid Time Frame

Proprietary

Profiling System



Customs Information Contains Many Valuable Data Elements. Successful Profiling Requires More Data, Earlier

Manifest information

- Bill of Lading Number
- Shipper, Consignee, Notify Parties
- Container Numbers, Weights and Dimensions
- Cargo Description and Harmonized Nomenclature
- Hazardous Material Information
- Port of Origin, Unloading, Final Destination
- Vessel and Voyage Information

Full Data Element Capture

- Routing and carriers prior to delivery to import carrier
- Full Involved Party Listing; Forwarders and Manufacturers
- Letter of Credit Information; Bank names and information
- Consolidation Information
- U.S. Inland Delivery Routing
- Unit Cost of Items

FreightDesk
TECHNOLOGIES

Examples of Anomalies that can be checked using data currently available

Anomaly	Commercial Document	Data element for Anomaly
Cargo Incongruent with Origin	Commercial Invoice, Master Bill of Lading	Routing, Item listing
High value cargo and slow mode	Commercial Invoice, Master Bill of Lading	Item values, routing information
Document discrepancy	Any	Documents do not conform to each other
New Shipper or Consignee	Commercial Invoice, Bill of Lading, Certificate of Origin	Shipper or Consignee Sections
Violation of established shipping or commercial patterns by parties	Any	Any – more in timing/receipt of documents (ex. Once-a-week shipper ships twice in one week)
Suspect source area and transship to small ship	Shippers Letter of Instruction, Bill of Lading	Origin of cargo, route
Point of origin	Shippers Letter of Instruction	Pickup location
Illogical commercial transactions	Commercial Invoice	Comparison of Consignee and Cargo (ex. Furniture company receiving garments)

FreightDesk
TECHNOLOGIES

Sample U.S. Import Documents with Major Data Elements

		Used Before Shipment							Used During Shipment							
	Data Elements	Pro-Forma Invoice	Packing List	Certificate of Origin	Shipper's Letter of Instruction	Insurance Certificate	Inspection Certificate	Letter of Credit	Commercial Invoice	Transmittal Letter	Customs Form 7501	Bill of Lading	Inland Bill of Lading	Vessel Manifest	Delivery Instruction	Customs Form 3461
1	Invoice Number	x							x							
2	Date of Issuance	x							x							
3	Shipper's/Exporters name & address	x	x	x	x	x	x	x	x	x		x	x	x	x	
4	Exporter Identification Number (EIN)				x	x	x	x				x	x	x	x	
5	Agent of Exporter				x	x	x	x				x	x	x	x	
6	Intermediate Consignee's name & addres	x	x		x	x	x	x	x	x		x	x	x	x	
7	Ultimate Consignee's name & address	x	x	x	x	x	x	x	x		x	x	x	x	x	x
8	Quantity	x	x	x	x	x		x	x	x	x		x	x	x	x
9	Unit Price	x	x		x	x		x	x		x		x	x	x	
10	Total Price	x	x		x	x		x	x	x	x		x	x	x	x
11	Net Weight	x	x	x	x	x	x	x	x				x	x	x	
12	Gross Weight	x	x	x	x	x	x	x	x		x		x	x	x	
13	Descrition of Merchandise	x	x	x	x				x		x					x
14	Terms of Payment	x							x	x						
15	Incoterms	x			x				x	x						
16	Estimated Shipment Date	x														
17	Currency of Payment	x						x	x	x	x					
18	Time Limit	x						x	x							
19	Miscellanious Charges (FCA, CIF)	x						x	x							
20	Letter of Credit Number							x	x	x						
21	Letter of Credit Date							x	x	x						
22	Import License number								x							
23	Harmonized Commodity number				x				x							x
24	Ocean Carrier Name			x					x		x	x		x		x
25	Ocean Carrier Route								x			x		x		
26	Voyage Number										x	x		x		x
27	Vessel Flag													x		
28	Foreign Port of Export										x			x		x
29	Loading Pier													x		
30	Port of Unloading										x			x		x
31	Method of Transportation															
32	Country of Ultimate Destination				x						x	x				x
33	Bill of Lading Number							x	x							
34	Marks, Nos. & Kinds of Packages		x	x	x											

Chairperson FEINSTEIN. Mr. Upchurch is the president and CEO of SGS Global Trade Solutions. They operate in 140 different countries. SGS inspects a significant amount of containerized cargo bound for the United States and other countries around the world, and he is testifying today as Chair of the Safe Trade Committee of the Global Alliance for Trade Efficiency.

Thank you very much and welcome.

STATEMENT OF CHARLES W. UPCHURCH, PRESIDENT AND CEO, SGS GLOBAL TRADE SOLUTIONS, INC., AND REPRESENTATIVE, GLOBAL ALLIANCE FOR TRADE EFFICIENCY, NEW YORK, NEW YORK

Mr. UPCHURCH. Thank you, Madam Chair.

Madam Chair, in the interest of time and also in the interest of your own personal request to cut to the chase and propose some solutions, I will disregard much of my prepared oral testimony and address some of your specific concerns.

Chairperson FEINSTEIN. Good.

Mr. UPCHURCH. Many of the witnesses here today have talked about the need for layers in security, and I believe that there is a consensus that that is required. I believe we all agree that our ports need to be strengthened, and we need to follow through on your own recommendations to be able to detect contraband or weapons of mass destruction as they come into the port. But the need to push back the border, the need to add additional layers as supplementary pieces is also very important.

I think it is very important, the proposal of Commissioner Bonner, to go to the ten largest megaports with the latest technology in container scanners and also with the latest risk-profiling techniques and to check containers on a risk management basis. This is very important. It is also very important in the private sector, particularly with the shippers, but also with the manufacturers, the carriers, et cetera, to introduce supply chain security standards and to implement those vigorously and to audit those so that another layer of security can be added.

The point and the recommendation that I wanted to give you today is that there is another layer that can be added. It is possible to inspect every container in Karachi or in Kuala Lumpur or in Yemen and to verify the integrity of the container, to——

Chairperson FEINSTEIN. By a person that you are 100 percent sure has not been bribed?

Mr. UPCHURCH. Yes, that is possible to put that level of check in. That is what companies like my own do. We do operate global mandates for governments. I have managed these programs for the last 16 years. They do include container security. We do go to inordinate lengths to audit our personnel, to do background, to carry out security, to frequently intervene at every instance. And then that is not enough. We also have to check the container again after it has been inspected to see if there are signs of tampering.

Is it possible to be 100 percent sure? Probably not. But is it possible to be fairly sure? Is it possible to take great measures and to add another layer of security? Yes, it is.

Unfortunately—please go ahead.

Chairperson FEINSTEIN. See, I am still deeply troubled that we are going to spend all this money to get this "push the border back" whereby it is going to touch maybe 80 percent of the cargo coming through 12 ports, but that is going to leave all these other ports all over the world essentially untended, which is exactly where this is going to go, I mean where a device is going to go.

Mr. UPCHURCH. Which is why I am proposing today that you do add this other layer in, that you are able to extend the U.S. Government through a global network into these other small ports by accrediting the private sector to work with the Government to act on their behalf. This can be done through accreditation programs. Accreditation programs even generate royalties that help fund the very stringent control that the U.S. Government would have to place on the private sector as they carry this out.

The private sector works through existing legal entities in every country, and they are able to carry out this work without the need for any bilateral agreement, so it can be implemented very quickly.

The private sector can invoice the foreign exporter, meaning there is no cost to the U.S. Government to implement a program like this. Technology is required because once—and having managed many of these programs and I have seen many things, particularly in Southeast Asia where container fraud is raised to an art form, technology is required. it is important once the integrity of the container is checked, the goods are verified that there are no prohibited goods being loaded into the container, it is sealed. But it is important to have technology in that container in the form of a transponder with sensors that will detect entry, unauthorized entry into the container, such as changes to light and air pressure. Because once an inspector leaves in the port of Karachi or wherever, then it is possible to enter that container again without breaking the seal, and it is very difficult to detect. And that is where the technology would help greatly. With GPS it can be tracked consistently throughout the voyage, from the time the inspector leaves until it arrives in the U.S. port. And these sensors are very reliable, and they will detect if anyone has entered that container, whether they have manipulated the door or they have chosen to just simply cut out a panel and re-weld it and repaint the container.

Chairperson FEINSTEIN. Is it possible to make one of those sensors a radiologic sensor?

Mr. UPCHURCH. Yes, of course it is. Once you have a transponder unit, you can put any type of sensor on it that you want. I have mentioned two, which are changes to light and air pressure, because those are the easiest to detect entry into a container. But you could have other sensors on the transponder, including a radiological sensor.

Chairperson FEINSTEIN. Is the transponder inherent in the structure of the container? I once went to Evergreen in Taiwan where I saw them produce a container 24 hours a day, you know, every minute a new container came off the line. Are these built in or are they added?

Mr. UPCHURCH. They have to be added. In order to carry out——

Chairperson FEINSTEIN. Doesn't that make them vulnerable, then?

Mr. UPCHURCH. Well, they have to be—they may be added at the time that the inspector comes. He may add them himself. It may be that the Government and the private sector and the shipping companies work together to ensure that containers that have these transponder units that are verified at the time of inspection are available.

In order to implement a program like this, legislation is required that mandates that containers coming to the United States are inspected at the time of loading. This is a critical aspect, because we promote trade-efficient, cost-effective, and quickly implemented programs. Once a container is looked at during the normal flow of trade, which is when the shipper is actually moving the goods into the container, then there is a very trade-efficient process. The Government would have to implement a regulation, legislation, requiring that the containers are inspected at the time of loading in the country of origin. They would likely want to exempt low-risk countries so that you are only targeting high-risk countries as one layer in this multi-layer onion that my friend Rob has described. This is just one layer, but it is a very important layer. It is the most secure foundation layer that you can place, and that is to look at every single container coming from high-risk countries and then to track those containers to make sure that they are not entered into again. And if you put up a piece like that with the other layers, which are the supply chain security standard that normal trade would need to implement and that needs to be audited, with the verification in the major transshipment ports that is based on risk management, and with the strengthening of the U.S. ports that you are advocating, then you begin to have a very good border security strategy.

Chairperson FEINSTEIN. And this would be financed essentially through fees paid by the countries to have their ports certified?

Mr. UPCHURCH. By trade.

Chairperson FEINSTEIN. By countries or companies?

Mr. UPCHURCH. Companies. Trade, private trade, private sector would pay for this. These types of programs exist today. There is a WTO agreement that governs these types of programs that ensure the right of every country in the world to implement these types of trade programs that require inspection prior to shipment. Today alone there are several hundred shipments from the United States that are being inspected by the private sector on behalf of foreign governments to meet their particular needs. Those are often involved in Customs compliance programs. This is a security compliance program, but it is the same thing in terms of the WTO agreement that governs this. So it is possible for——

Chairperson FEINSTEIN. Let me ask you, how many companies are there in the world in these ports that you would have to secure their cooperation and participation?

Mr. UPCHURCH. What do you mean by how many——

Chairperson FEINSTEIN. Well, you said the companies essentially would do this.

Mr. UPCHURCH. Well, there are within GATE, which is the Global Alliance for Trade Efficiency, some of our members are service providers, and there are inspection companies and technology providers that have global networks. There are not many of them, but

there are enough of them that would allow the U.S. Government to set up an accreditation program and to control those that they accredited to carry it out. They have offices in every single country in the world and every port in the world.

Chairperson FEINSTEIN. You see, the thing that worries me about all of this, it is sort of like when I went to the border between San Diego and Mexico and watched the thousands of trucks pound through, and there are people, and yet all it takes is for one agent to get bribed by a drug cartel to turn his head and wave a truck through. Bottom line, your technology—and I appreciate that, but the bottom line, it comes down to the human. And I am his appointing authority. I am going to pick up the phone and said, Richard, you let a bomb come into the Port of Long Beach, you know, don't show up the next day, you don't have a job. Or what are you going to do to assure me that a bomb isn't going to come into Long Beach? How can he ensure with that kind of system? He can't.

Mr. UPCHURCH. It is difficult, but the private sector does have a risk to manage itself. Typically, for every five inspectors there is an auditor, and there is an enormous amount of—there is an internal security department that not only does internal investigation but does external investigation. Private sector security inspection companies have to carry out investigations of companies. They have to put together risk management databases of all of the noncompliant companies that they come across. And that is the type of information that can be shared with the U.S. Government. These companies can be the eyes and ears of the U.S. Government on the docks of Karachi, which is something that is very difficult to do today.

[The prepared statement of Mr. Upchurch follows:]

STATEMENT OF CHARLES W. UPCHURCH, PRESIDENT & CEO, SGS GLOBAL TRADE SOLUTIONS, INC., WASHINGTON, D.C.

Madame Chair and distinguished members of the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information.

My name is Charles Upchurch and I am President and CEO of SGS Global Trade Solutions, Inc., headquartered in New York. I am also a member of the Global Alliance for Trade Efficiency, known as GATE. GATE is a multi-national not-for-profit organization focused on improving the efficiency and security of trade. GATE represents technology solution providers, inspection and certification companies, shippers, financial institutions, Fortune 500 companies, manufacturers, importers and exporters.

GATE maintains close and cooperative relationships on customs and trade-related issues with the World Customs Organization, the World Bank, the European Union, and the Office of the US Trade Representative.

I have been asked today to offer you trade efficient recommendations and solutions for the protection of US ports including the necessary existing technology.

In protecting US ports, technology plays an important role in what we believe is at least a three step process. The first step is to carry out a security inspection of the container at the time of loading; the second is to seal the container; and the third, or final step being the use of global tracking technology to monitor the cargo while in transit.As the Subcommittee is aware, the shipment of goods in containers represents a significant security risk as they can hide weapons of mass destruction from easy detection. Inspecting containers upon arrival is already too late in the supply chain for this particular risk. US Customs Commissioner Robert Bonner has recently outlined a four step plan to minimize this risk: establishing international criteria for containers, pre-screening high risk containers, maximizing the use of detection technology, and the development of "smart boxes" with electronic seals and sensors.

We support these recommendations which include figuratively extending America's borders to allow for the security inspection of cargo prior to shipment. However,

the potential exists that these efforts to improve container security would incur a very high cost to the government, would take a significant amount of time to implement due to the negotiation of bilateral agreements and would likely hinder trade efficiency by requiring changes to current trade patterns and processes. We would like to propose ideas that will strengthen these recommendations to improve container security while avoiding the potential problems.

It is our recommendation that the Subcommittee consider establishing a solid foundation for container security by requiring in high risk countries compulsory security inspection at the time of loading goods into the container. This is not only the most secure method of pre-screening high risk containers but it is also the least disruptive to trade as it occurs within the normal logistics process. If a container has not been inspected at loading, pre-screening would require either scanning or unloading the container in a port area. Scanning containers is a useful complementary tool but has limitations in its effectiveness as a sole solution and unloading/reloading containers is very expensive.

Once a container has been inspected and sealed at the time of goods loading there is still the risk that weapons of mass destruction can be introduced into the container. There are many ways to enter a container without breaking the seal while evading detection. It is therefore critical to monitor containers after inspection and sealing to detect any unauthorized entry prior to arrival in the USA.

Cost effective technology exists to track individual container shipments and is already in use to track vehicles today. Small inexpensive GPS transponder units can be installed inside containers with sensors to detect any changes, such as to light and air pressure, that would indicate entry. The transponders would be continually monitored by information technology and an alert will only be generated for intervention when a sensor indicates container integrity has been compromised prior to arrival in a US port.

The most cost effective and the quickest way for the US Government to create a program of compulsory inspections in high risk countries is to accredit private sector security inspection companies and technology solution providers. Private sector security inspection companies operate through existing legal entities in all countries and can inspect cargo at the time of container loading within the normal pattern of trade. They can also invoice the foreign exporter for the cost of the container security inspection and monitoring. The US Government can establish sufficient criteria to accredit appropriate service providers. Accreditation usually generates a royalty payment which could fund the strong control to be exercised by the US Government over the service providers.

The program I have outlined can only be implemented by introducing legislation that requires compulsory security inspection in the country of exportation of all containers destined for the USA. Under this program, the government would likely elect to exempt countries that are considered low risk threats. This would provide flexibility in the program and focus the compulsory inspections only on high-risk countries.

The Subcommittee may be aware that entrusting security inspections to the private sector has already been recommended by a working group composed of representatives of the Department of Transportation and the US Customs Service in a report to Secretary Mineta, Secretary O'Neill, and Governor Ridge.

We applaud the Subcommittee on its efforts to introduce technology into container and port security. On behalf of GATE we request that the Subcommittee consider the concept of compulsory container security inspection and the use of accredited private sector service providers in protecting US ports.

Thank you for your time and I will be pleased to answer any questions you may have.

Chairperson FEINSTEIN. I am going to take a brief recess. If you don't mind staying a little bit, I will just be 5 minutes, and I am going to ask Ms. DeBusk to say whether she thinks that is workable when I come back.

Ms. DEBUSK. Sure, I will be glad to.

Chairperson FEINSTEIN. Thank you very much.

[Recess 5:15 to 5:35 p.m.]

Chairperson FEINSTEIN. Now, because we are small and intimate, we can perhaps just talk for a few minutes. I saw the gentleman that had to leave, and I am glad he has offered to provide help, and

I wanted to ask all of you to provide help to Senator Kyl's staff and my staff and see if we can't put something together.

Ms. DeBusk, let me ask you this question: There is no government that I know of that has tried more to prevent the shipping of illegal immigrants in containers than the Chinese Government, and yet they have failed to do so. As late as 3 weeks ago, a container, I gather, came into Los Angeles with illegal immigrants aboard.

If the Chinese Government, with all of their resources, can't stop this illegal traffic, what would lead you to believe that we can create a system that would stop somebody from putting a bomb on one of these containers? And so maybe you could respond. Maybe you could respond to this issue with that in mind.

Ms. DEBUSK. Sure, I would like to do that, and thank you for the question.

First of all, I think you hit the nail on the head when you were suggesting that a solution had to be comprehensive, not just 12 ports. And let me just give you a real-life example of a situation here in the United States.

The Port of Miami had a major problem with stolen autos.

Chairperson FEINSTEIN. Stolen?

Ms. DEBUSK. Autos, and they were being exported from the Port of Miami down into the Caribbean. And there were all sorts of stolen autos that were being put in these containers and exported. So they got one of these fancy X-ray machines, these VAC machines, and they started X-raying those containers. All of a sudden they had no more stolen autos, but guess what? Port Everglades, which did not have one of these fancy X-ray machines, all of a sudden had a major problem with stolen autos.

So if you want to have a solution that is based on technology or inspections or anything along these lines, it has to be comprehensive because, otherwise, the bad guys will just go to the weak link in the chain there.

The second thing that I wanted to comment on is that ensuring the integrity of inspectors is a really difficult, difficult thing to do if you are thinking about people in foreign countries who are inspecting things at foreign ports.

This issue came up when I was in Government at the Commerce Department. The question was whether we should let private inspectors check on how U.S. technology was being used in foreign countries. And our decision was negative. We said, no, the only inspection that is going to count for us is an inspection by a U.S. agent. And that is not because we didn't want to rely on information from our foreign counterparts, but just based on experience there are just lots of things that can go wrong in foreign countries.

The other issue that would have to be looked at very closely is who is the client and who is paying the bill, because, once again, if there is an inspection agency who is being paid by the shipper and they discover at tremendous problem—there is, in fact, a nuclear bomb in that container on that vessel—it is unlikely they are going to want to go to the U.S. Government with that information because, otherwise, their client is going to be left with an oceanliner that nobody is going to use. Who wants to be using an oceanliner where you can put nuclear bombs on it?

So there is also an inherent conflict of interest that would have to be addressed there in terms of who is paying the bill for these inspections.

Chairperson FEINSTEIN. Gentlemen, any comments?

Mr. QUARTEL. Can I comment on anything?

Chairperson FEINSTEIN. Sure. Why not?

Mr. QUARTEL. If I can go back to some of what was said, too, I also agree with Amanda on this, but what I also would not endorse is the notion that you do 12 ports or 10 ports. I think the reality is that we get cargos in 300-some ports in the United States, and it is sent from several thousand points of origin globally. And the beauty of data and commercial systems and trade is that it doesn't have to be port or anything else specific. If something is coming to the United States, you can know who ordered it and paid for it. You can know where it was manufactured, and in Asia——

Chairperson FEINSTEIN. Take the containers with people in them.

Mr. QUARTEL. You can know that that container originated——

Chairperson FEINSTEIN. How? How? Coming from China, how do you know?

Mr. QUARTEL. Well, you know, these are—I don't have every answer, but I know that a container from China with people in it, you can know it is coming out of Tianjin where these people may have originated 90 percent of the cases. So that says you want to inspect containers coming out of Tianjin. Or——

Chairperson FEINSTEIN. Don't you think the Chinese are doing that?

Mr. QUARTEL. Who knows what the Chinese are doing? And I don't mean to be flip, but I really honestly, Senator—you know, they are very technologically backwards. They substitute labor for technology probably too often. They are notoriously corrupt in all of these things. So I don't think you or any of us can assume that they are doing all the things that we would do as a government to stop it.

But, for example, you would know who the freight forwarder was or the consolidator who packed the container before it was sealed. That is all information that is contained in a transaction, and it can be reported somewhere. And really all we are suggesting in our notion of data collection is that you have data on every transaction, every place it has been, everybody who touched it.

Chairperson FEINSTEIN. Well, let me interrupt you, just in the interest—you are then suggesting a kind of international agreement with participating nations or participating ports, however you want to do it, but it would be some kind of agreement that everybody would enter into?

Mr. QUARTEL. I think you could do it much more simply than that. I don't think it matters what any other international government thinks. The reality is that if you told the American shipper who ordered the cargo to be sent to the United States—and every cargo coming here is bought by an American somewhere—that it is his responsibility to see that that cargo is secured and that he is responsible for seeing these 19 different data elements, including all the transportation, all the handling, all the finances, all the so-and-so, and report it to some authority in the United States Gov-

ernment before it ever gets on a ship or a train or a plane, or whatever——

Chairperson FEINSTEIN. Supposing it is half a container sent to Joe Dokes, Joe Dokes is just an individual——

Mr. QUARTEL. It is not actually the container. The reality is you want to go as far down as a shipment. A single container could contain 20 different shipments from 20 different owners.

Chairperson FEINSTEIN. Okay. So these owners are just private individuals.

Mr. QUARTEL. Absolutely. And, you know, one of the things I would suggest, if you want legislative suggestions, I think one of the things you could think about—we already have an export license requirement. You could well have a requirement for some form of import identification based on a purchase order. As soon as you ordered something from overseas, you filed a purchase order. Now, I am not saying you create a license requirement with a lot of bureaucrats. But even that, giving someone an identifier for every transaction coming into the United States from the very day it was ordered will make the process more simple and have more discipline.

Chairperson FEINSTEIN. That is not a bad idea, actually.

Mr. QUARTEL. There are a number of things you can do like that. But, you know, in the end it comes on to the U.S. importer. Eighty percent of all transactions in trade are outsourced to freight forwarders, Customs brokers, and third-party logistics providers. But in the United States they are all licensed. So there are 4,000 or 5,000 of those licensed by the FMC, Federal Maritime Commission, where I used to sit. I would move the licensing requirement and I would move them to Customs. I would tighten up the licensing requirements. I would probably do background checks on freight forwarders and say, If you are moving the cargos, you need to know who you are dealing with on the other side.

So, again, it is layers and layers, but there are some very specific things you can do. A freight forwarder today will typically know who he is dealing with overseas, and if he doesn't, then he sort of watches the transaction and he himself will probably check the container or ask one of his Customs agents——

Chairperson FEINSTEIN. Is there any shipment that comes in without a freight forwarder?

Mr. QUARTEL. Yes, probably 20-some percent have—20, 25 percent have internal company freight forwarders and things like that. But you could mandate that a licensed party be involved with it.

Chairperson FEINSTEIN. In other words, that no——

Mr. QUARTEL. And Amanda, I know, has some thoughts on it.

Chairperson FEINSTEIN [continuing]. Shipment comes into the United States that doesn't have a freight forwarder?

Mr. QUARTEL. Or other licensed agent of the Government involved in the process.

Ms. DEBUSK. One of the other things to think about is if you want to start doing things abroad, looking at those containers abroad or checking to see if Chinese individuals are in those containers, spot checks are a wonderful thing. Given limited resources, it is, you know, impossible for the United States Government to all of a sudden hire enough agents to go abroad to every single port.

But spot checks are beautiful things, and it definitely increases compliance immensely because when you know that there is, you know, a one in 10 chance or a one in 50 chance, or whatever it is, that you may be caught, it certainly provides strong deterrence. So a combination of cooperation with foreign officials, with private sector inspections, backed up by spot checks by U.S. Government officials would certainly, you know, move the ball forward in terms of our security.

Mr. QUARTEL. I wonder if I could make one other quick addition to all of that, too, which is, I think the other concept that is really important to bear in mind is that a legal cargo that comes to the United States legally can become a lethal cargo in the right circumstances.

Chairperson FEINSTEIN. Say that again? A legal cargo can become an illegal cargo?

Mr. QUARTEL. Can become a lethal cargo.

Chairperson FEINSTEIN. Lethal. Thank you.

Mr. QUARTEL. And by that—for example, we have talked an awful lot about radiation, but, for example, fertilizer or fertilizer-type chemicals are legal. I don't know all the terms and conditions, and there are conditions that would bind it. But it is legal to bring those kinds of things into the U.S. Now, it would be documented. Customs would say it is fine. Frankly, you could probably inspect it, and nothing is in it. But let's say a sailor on a ship on the water puts a blasting cap and a GPS on it, and all of a sudden it still legal, but it is lethal.

Now, a container can hold 12 to 13 times as much fertilizer as Timothy McVeigh's bomb in Oklahoma City. So think about the damage one container of a legal cargo could do.

Now, the beauty and power of information is——

Chairperson FEINSTEIN. Right under a critical bridge coming into a harbor or whatever.

Mr. QUARTEL. Yes, ma'am.

Chairperson FEINSTEIN. Right.

Mr. QUARTEL. But the beauty and power of information is that you not only want to know what it is, but you can also think through the situation in which the shipment or cargo is placed. Is it placed in a dangerous situation? Is it coming out of someplace where, even though it looks good, you might want to worry about terrorists or people in subterfuge and subversion there?

So, you know, this is not a simple problem of analyzing it, but I think the message on this is that the data to do it on the commercial side is there. It is more than what Customs and the U.S. Government gets today. And I think the law enforcement data is beginning to be there and the national security data, and I have been involved in talking with some of these agencies, and they do have issues about how they talk to each other. But it can be done.

Chairperson FEINSTEIN. Do you have any comments, Mr. Steinke?

Mr. STEINKE. Madam Chair, I would make a comment in agreement with——

Chairperson FEINSTEIN. Could you move the mike down a little bit? Thanks.

Mr. STEINKE. With Rob, that there seems to be a disconnect or a lack of integration about information in general, whether it be on the Federal side with the myriad of agencies, be it Customs, Coast Guard, FBI, INS, who have certain jurisdictions within the ports or in the commercial environment with freight forwarders, Customs brokers, shipping lines, shippers, et cetera. Though I think the industry has tried, I don't see that there has been that connection and integration of information, and I think that is something——

Chairperson FEINSTEIN. Do you get any information as the chief executive of a huge port, do you get any kind of——

Mr. STEINKE. Traditionally——

Chairperson FEINSTEIN [continuing]. That something may be awry on a ship?

Mr. STEINKE. Senator, we do not get any information other than what we may get through our fire department as far as checking on hazardous cargo. Traditionally, the FBI or Customs or the Coast Guard will not interact with the port because it is not within our jurisdiction to know. And many times they will specifically not want me as the CEO of that port to know what the situation is. They may advise us that they may be inspecting, you know, certain terminals on an ongoing basis based on certain types of cargo profiles that they have identified. But we are not intimately integrated with lots of the functions that take place.

Chairperson FEINSTEIN. Do you think that is a mistake?

Mr. STEINKE. I think we need to have more information from a port standpoint than we do now.

Chairperson FEINSTEIN. I do, too. I mean, you ought to have some kind of security clearance to be able to—you have no security clearance?

Mr. STEINKE. No, we don't. And, again, we have traditionally seen ourselves historically as a transfer point and part of this logistics chain. Local port authorities have not set policy. We have been charged with the responsibility of developing facilities so that terminal operating companies and shipping lines can move cargo without delay from one point of transfer to another, and that is the roles that we have seen ourselves as U.S. ports in for, you know, the last several years.

Chairperson FEINSTEIN. See, I think that role is changing because you have really become a guardian, too, and airports have—the role has changed. They are not just passive entities anymore in all of this. I think that is a real problem. Go ahead.

Mr. QUARTEL. Well, and to that, I think—and Richard can correct me, but the reality is that ports come in all sizes and all forms of Government entities. Some ports are largely private. Public ports within them, as you well know, have private entities at various docks. Some ports are merged with airports in terms of governmental authorities.

Chairperson FEINSTEIN. But he runs the whole shebang.

Mr. QUARTEL. In LA/Long Beach.

Chairperson FEINSTEIN. In LA/Long Beach. That is a huge port.

Mr. QUARTEL. Right. So, yes, to that point in terms of getting the information.

Chairperson FEINSTEIN. Right. And I realize there are little places, but big stuff——

Mr. QUARTEL. Well, but I think you made the point——

Chairperson FEINSTEIN [continuing]. Is going to come in there.

Mr. QUARTEL. Yes, ma'am. I think you were making the point also about the security piece of that. We have a port in Richmond, Virginia, up the James River. I don't know whether it is public or private. I have a summer house on an island in the Chesapeake, and there are 25 docks that a ship could come in with a container, a small ship, mind you, but they could bring a container in. Now, there is a Coast Guard station around the other end of the island, but they are not necessarily going to see it.

So, you know, there are all sorts of ways to subvert the system.

Chairperson FEINSTEIN. That is why you have to keep them from coming in loaded with something.

Mr. QUARTEL. Yes.

Chairperson FEINSTEIN. Well, it is a very interesting problem, but really challenging. I would really like to find a way to use technology, but also to use human beings to really create a kind of network that is global that can protect our citizens.

Mr. QUARTEL. That is right.

Chairperson FEINSTEIN. And I wonder, would you all be willing to work with our staffs, Senator Kyl's staff and my staff, and see if we can't come together and be helpful in this?

Mr. QUARTEL. Yes, I would be glad to do that.

Ms. DEBUSK. Sure.

Chairperson FEINSTEIN. I would really appreciate it.

Mr. STEINKE. My pleasure.

Chairperson FEINSTEIN. Is there anything else any of you would like to say? No. Then thank you very, very much, and this hearing is adjourned.

[Whereupon, at 5:51 p.m., the subcommittee was adjourned.]

[Submissions for the record follow.]

SUBMISSIONS FOR THE RECORD

Statement of R. A. Armistead, President and CEO, ARACOR

I am responding to your request for my thoughts regarding seaport security issues and technology that is available to help mitigate the threats at our nation's seaports.

OVERVIEW

- Over 90% of United States international trade comes through our nation's seaports.
- Over 70% is shipped in sea cargo containers.
- 25 U.S. seaports account for 98% of all container shipments.
- The top 50 seaports in the United States account for approximately 90% of all the cargo.

California ports rank high in terms of cargo handled. The ports of Long Beach, Los Angeles and Oakland are among the top five ports in the U.S. in terms of container throughput; Long Beach and Los Angeles regularly rank in the top 10 in the world.

Seaports are generally uncontrolled facilities, where people can freely enter and leave. For the most part, cargo passes through our ports without being inspected. Reportedly, only 2% of incoming cargo containers are inspected. Thus, duty avoiders, smugglers and terrorists have a very high probability of shipping contraband into the U.S. without detection. Once outside the seaport, a cargo container can end up anywhere in the country without having been inspected or opened. Therefore, the seaport is the most effective location for stopping incoming contraband.

Virtually all cargo inspections are performed by customs inspectors. They use dogs, drills and, in some cases, physical searches involving unloading the cargo and

subjecting individual items to examination. However, dogs cannot smell "duty fraud" and are not trained to detect weapons of terrorism. Drill samples provide a random check and physical searches of large containers, which require two-to-three person-days, are rarely done. Thus, even for the 2% of the containers that are selected for inspection, there is some chance that contraband will escape detection.

NEW TECHNOLOGY

There are reasons to believe that new technology that has recently come on the market can help to mitigate the security threat represented by cargo entering our nation's seaports. In particular, x-ray inspection systems designed for use at seaports can:

- See through the cargo and detect contraband even if concealed behind false walls or in hollow structures.
- Inspect a 20-foot container in less than 30 seconds.
- Continuously inspect a line of containers and trucks.
- Be augmented to automatically detect nuclear weapons or special nuclear materials, even if shielded.

Thus, with the proper logistics, a high percentage of the cargo could be inspected to protect against terrorism without severely impacting the flow of commerce. It is highly unlikely that resources will ever be sufficient for inspecting all of the entering containers. Thus, inspection technology at our seaports should be considered as one element in a layered defense. Other elements could include inspections at the point of shipment, high-integrity seals, the profiling of cargoes like done for airport passengers, etc.

The material that follows takes a closer look at seaport security issues; reviews new technology that can assist in addressing the threats; and looks at "barriers" that impede the introduction of this technology.

SEAPORT VULNERABILITY

What does a terrorist look for in selecting a target? Probably, such things as accessibility, the likelihood of success and the amount or "visibility" of the loss the U.S. would suffer from a successful attack.

California alone has three of the largest ports in the nation, annually handling over 10 million containers carrying tens of billions of dollars worth of goods. A terrorist attack that shuts down any of these ports for even a few weeks would have enormous consequences to California and the nation. Such events could include the sinking of a ship in a shipping channel, the explosion of a small nuclear weapon or dirty bomb at the port, or the release of a chemical or biological contaminant. Both the Los Angeles and the Oakland-San Francisco areas contain cities of high worldwide visibility with dense populations and high-technology manufacturing centers. An attack on one of these cities caused by weapons arriving by cargo container would also have devastating consequences.

The events of September 11 awakened the nation to the fact that we are under attack and our nation, which prides itself on the free flow of people, goods and ideas, has many areas of vulnerability. At the same time that our nation is attempting to address areas of vulnerability, terrorist organizations are undoubtedly focusing on detecting other areas that have not yet been addressed. The nation's leaders have determined that spending tens of billions of dollars on airport security is worthwhile, in spite of the economic impact. The same resolve needs to be shown toward spending on security at seaports, where the risk of catastrophe from imported terror could be even greater than at airports.

If U.S. ports were secure, the nation would benefit in the following ways:

- Weapons of terrorism, such as explosives, special nuclear materials and nuclear weapons would be prevented from entering the country.
- Billions of dollars worth of stolen cars, electronics, computers, and other valuable goods would be intercepted before they could be shipped out of the country.
- Billions of dollars of additional duties and taxes would be collected by detecting fraudulent manifests on imported goods.
- Counterfeit goods would be prevented from entering the country.
- Illegal drugs, believed to be entering the U.S. by seain increasing amounts, would be kept off our streets.

NEW TECHNOLOGY AND BARRIERS TO USE

New Technology: Over the last five years, several types of new nonintrusive inspection systems have come on the market. These systems employ x rays, gamma rays or neutrons to screen the cargo for contraband. For the most part, the earliest

use of such technology was along the border with Mexico. At the time of implementation, only low-energy x-ray inspection systems were available. Though only capable of inspecting empty or lightly-loaded trucks, they were considered appropriate at the time because of a flow of nominally empty trucks coming from the border. However, these low-energy systems have little or no application to seaports due to their limited cargo penetration. In fact, existing low-energy inspection systems at the Mexican border will have to be supplemented to improve security, if the open border provisions of NAFTA go into effect.

At this time, Customs has several systems to choose from that offer different combinations of price and performance. Our company (ARACOR) manufactures the Eagle® inspection system which combines mobility, relocatability and the highest imaging performance of all the systems. It provides cargo penetration that is almost a factor of two times greater than its nearest competition and more than three times that of the low-energy systems at the Mexican border.

U.S. Customs Service has made detailed measurements of the performance of all of the available cargo inspection systems and graded them into four "performance levels." ARACOR's Eagle is the only system that has been placed into level four, the highest performance category. ARACOR is also working with the DoE National Nuclear Security Administration and the DoD Defense Threat Reduction Agency to implement combined x-ray and neutron technology for the specific detection of drugs, explosives, special nuclear materials and nuclear weapons.

Barriers to Use: Are these new technologies being quickly introduced into use at the nation's seaports? The answer is clearly no! There are a number of reasons for the slow adoption rate

• Resistance to New Technology: Since the beginning, Customs inspectors have depended on their hands, experience, instincts and dogs. To introduce new technology, such as x-ray inspection systems, requires that the inspectors be convinced that the technology represents an improvement. Some inspectors at ports may resist new technology, which requires changes to established procedures and may reduce their overtime pay. Moreover, they have to be trained how to operate and maintain the systems and analyze the images.

Budgets: Although they provide a much greater inspection efficiency and throughput, the new systems are relatively expensive. Customs has not been given a budget that is adequate for adding the required number of inspection systems to our seaports. Even if systems were only to be placed at the 20 largest US ports, a considerable number of systems would be required for inspecting a high percentage of the cargo. The Port of Oakland has 11 separate terminals and Los Angeles has 28 or more. Until recently, most of the available equipment budget has been devoted to the southwest border. Even now, more attention seems to be focused on the Canadian border than on the nation's seaports. It almost appears that there will have to be an attack at a seaport before much attention (and budget) is focused in that direction.

Mixed Jurisdictions: A number of separate "groups" must agree (or be forced to agree) before the security threat at U.S. seaports can be addressed.

1. The Administration and Congress: Airport security is our nation's current focus. The seaport security issue cannot truly be addressed until the national "spotlight" is focused on it and an appropriate budget is allocated. Legislated milestones for implementing seaport security improvements, such as those in the airport security legislation, will ensure that the necessary measures will be accomplished in a timely manner.
2. U.S. Customs: Customs will likely have primary responsibility for implementing the "will of Congress" as it pertains to seaport security. However, even after Congress provides the budgetary authority, individuals at Customs must take appropriate action. Experience to-date indicates a reluctance to make decisions and take actions that may be questioned. This overly cautious past performance suggests that the move to introduce new technology will likely be made very slowly. Once enabling legislation and budgets are in place, empowered US Customs officials must take the necessary steps to achieve the established objectives and meet the required milestones.
3. New Organizations and Missions: The events of September 11 resulted in the establishment of new organizations, such as the National Transportation Administration and the Office of Homeland Security, and the revision of missions for other organizations. For example, the US Customs Service has changed its focus from interdicting drugs to protecting against terrorism. The organizations affected by these changes are still trying to determine how best to fulfill their missions and combine their talents to work together in a coordinated effort. Hopefully, the uncertainties inherent dur-

ing this transition period will not hinder effective decision-making and implementation of new initiatives, such as seaport security.

4. Port Authorities: The primary goal of the Port Authorities is to make money by attracting commerce. They fear that a slow down in the handling of cargo due to inspection would result in the loss of business. At the Mexican border, the US government owns the property that is used for conducting inspections. However, at seaports, Customs is only a tenant. Customs officials have told me that they could not purchase Eagles because Port Authorities would not agree to provide them space for operation! In some cases, land at a port has been set aside for Customs inspections but the location is so remote that the efficiency and cost of inspections are severely impacted. Legislation and/or persuasion are needed to enable Customs to operate cargo inspection equipment at ports in a manner that meets the national security requirements with minimal impact on the flow of goods through the port.

5. Longshoremen's Union: The Longshoremen who work at the ports must also "buy into" new operations, including cargo inspection, which some may not welcome. In the past, they have resisted the introduction of improved inspection technology and allegedly perpetrated acts of equipment vandalism. A Longshoremen's Union strike at one or more seaports could also have a significant economic impact. Therefore, the Longshoremen, have a major influence on port operations and security and must be persuaded to join the nation's fight against terrorism.

Can these barriers to use be overcome? The answer is definitely yes! However, action must start at the top levels of government and will definitely require a larger budget for equipment and inspectors.

I have tried to concisely put forth my views on several topics related to seaport security. I hope this material will be of some use to the Committee. However, there are additional details that could be provided on each topic so, if more is desired, please do not hesitate to contact me.

Statement of Hon. Maria Cantwell, a U.S. Senator from the State of Washington

I want to thank Senator Feinstein for chairing this hearing and providing this opportunity to discuss the vital issue of seaport security.

Our nation's seaports lie at the heart of our economy and transportation system. Yet, they also represent a significant point of vulnerability in our national security. Of the over six million shipping containers that enter the United States annually, only a mere two percent are inspected. While inspecting every container entering our ports would unquestionably bring our economy to a grinding halt, the impact of a terrorist attack in our ports would be devastating.

This dilemma illustrates the need to discuss security alternatives which integrate new ways of thinking and new technologies. To this end, I look forward to hearing testimony from representatives of the Department of Transportation, US Customs Service, and US Coast Guard today. I also look forward to this Committee and the full Congress considering several legislative proposals to strengthen seaport security in the near future.

I was pleased by the Senate's passage of S. 1214, the Port and Maritime Security Act of 2001, and I urge the House to consider this important piece of legislation on the floor. This bill addresses the need for increased security measures for shipping containers at the point-of-origin. Focusing on point-of-departure and mandating advance shipping manifests represent security measures that are proactive rather than reactionary.

My home state of Washington boasts the largest locally controlled port system in the world with over 70 ports ranging dramatically in size, infrastructure, and purpose. In Washington, ports play an integral role in our state's economy as the nexus for international trade and a leading provider of high-quality jobs for our residents. In fact, one out of every four jobs in Washington state is dependent upon trade facilitated by seaports.

Securing these seaports and our ports nationwide is essential to a functioning economy and public safety. It is an issue most deserving of our attention, and I would like to thank Senator Feinstein again for bringing it to the forefront today.

Statement of Anthony Acri, CEO, International Microwave Corporation

International Microwave Corporation (IMC) submits the following testimony in response to the February 26, 2002, Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information, hearing on "Securing Our Ports Against Terror: Technology, Resources and Homeland Defenses."

I want to thank Senator Feinstein for holding this hearing and bringing national attention to this important issue. Our nation's seaports have insufficient security and may be vulnerable to terrorist attack. The tragic and unanticipated events of September 11 have brought matters of national security into sharp focus. But the Senator identified this problem two years ago when she said "many of the problems at seaports are due to insufficient federal oversight and lack of personnel and technology. We should do more to combat crime and fraud at seaports and reduce their susceptibility to terrorist attack."

Senator, you are right. Ports lack sufficient security, and technology is the solution. This week's testimony made clear that the primary area of port security concern is cargo and container inspection. But, none of the witnesses focused on two emerging threats that will be exacerbated by increasing inspection of arriving cargo: (1) physical security at port facilities; and (2) the shortage of security personnel. Increased inspection of shipping containers means fewer personnel overseeing the physical security of port facilities. Given these manpower limitations, the answer lies in the use of technology.

Amanda DeBusk testified that a study by the Interagency Commission on Crime and Security at U.S. Seaports (the "Commission") found that significant criminal activity was taking place at most of the twelve seaports surveyed. The Commission also found that the state of security at seaports ranged from fair to poor. Over 12 million containers arrive at U.S. seaports each year, and only one to two percent of all cargo is inspected. In that small portion of inspected containers, law enforcement officials have found secreted huge caches of illegal drugs, contraband weapons, and illegal aliens.

To address this problem, regulators have been focusing on increasing the inspection of containers and pre-screening cargo in foreign ports of shipment. But Congress must consider what the witnesses left unaddressed: increased oversight of containers may decrease physical security of ports by drawing personnel away from surveillance and security patrol of port grounds. Increased inspection and oversight of containers may provoke a rise in theft at port facilities, as lawbreakers seek to steal or retrieve smuggled contraband. If facility integrity measures are not in place, there will be nothing to deter such an increase in criminal activity.

In our opinion, effectively increasing port security will not work unless improved security measures are deployed across all aspects of port operation - cargo inspections accompanied by employee credentialing, and increased physical integrity of port facilities.

As the Senator pointed out, most seaports lack basic security technology, such as video surveillance, and do not even conduct internal or perimeter vehicle patrols. At the Port of Oakland, one of the nation's busiest ports, only one or two piers have 24-hour closed circuit TV security, and most of the port remains unguarded at night except for occasional visits by a lone Oakland policeman. The Commission study recommended that seaports be governed by certain minimum physical security standards covering fences, lights and gates. As Rear Admiral Kenneth Venuto, U.S. Coast Guard Director of Operations Policy stated in his testimony, effective port security "is built on principles of awareness. . . . Awareness helps focus resources and provides efficiency to prevention."

There is no better way to increase awareness and security than adopting a comprehensive video surveillance program. Video surveillance technology maximizes sight in a time of decreased personnel. America's seaports need to install video technology currently used along our borders that acts as a 'force multiplier," allowing one person's eyes to do the work of many.

For example, IMC's enhanced surveillance system is fast becoming the most popular and widely accepted video monitoring system used by government and private industry. IMC's system combines single or dual long range day cameras and thermal imaging night cameras on customized poles that can scan a twelve square mile area, 360 degrees, 24 hours a day, in any kind of weather. Video signals are transmitted to a central surveillance facility via microwave or fiberoptic cable, where security personnel can manipulate remote cameras, monitor highresolution screens for suspicious activity, and direct mobile forces. As an affixed or portable system, IMC WatchTowers can be used in numerous capacities, including protecting ports, bases,

embassies, nuclear facilities, airports, or borders. IMC's WatchTower system has become known as "the force multiplier" because it enables security forces to use fewer people to watch more territory and better supervise field response teams.

In the fall of 2000, the Immigration and Naturalization Service (INS) and the U.S. Border Patrol awarded IMC a $200 Million, four-year turnkey contract to design, manufacture, install and maintain the WatchTower system along U.S. borders. IMC's WatchTowers are securing our borders from illegal aliens and drug trafficking while protecting the safety of our federal agents and Americans living along the border. A Texas Border Patrol Agent-in-Charge called IMC's WatchTower "the best technology I've ever seen in my entire career." Use of this proven effective technology can easily be expanded from its current employment by the U.S. Border Patrol to address the problem of securing U.S. seaport facilities.

The U.S. Department of Transportation (DOT) will shortly begin accepting applications from ports for grants to enhance seaport security under the new Port Security Grants program administered by the Maritime Association (MARAD) and the U.S. Coast Guard, on behalf of the Transportation Security Administration (TSA). The grant category for enhanced facility and operational security at ports, including physical security, should not be minimized.

It is essential that America's ports are the safest, most secure port facilities in the world. The "emerging threat" against the United States has, in fact, emerged. In our opinion, the next emerging threat to our nation will be the shortage of qualified law enforcement personnel and the well-document lapses of civilian security employees. Initiatives such as the Port Security Grants program should prioritize the use of technologies that maximize the individual capabilities, such as "the force multiplier" of the WatchTower system, where one person can be the eyes of ten.

We thank the Committee for this opportunity to testify and are able to meet with you to further discuss the national security and information landscape, and how IMC has contributed to real security solutions.

Statement of Michael Nacht,[1] Professor, University of California, Berkeley

Madame Chairperson, it is a privilege to submit this testimony for inclusion in the Congressional Record.

The events of September 11 and subsequent acts of bio-terrorism are a startling wake-up call for the need to enhance the protection not only of the American people, but of our vital industrial assets. Protection of critical infrastructure has now been established as a top priority of the Office of Homeland Security. A key element of this infrastructure is our network of major port facilities. The ports that ring the East, West and Gulf Coasts are vital economic engines whose safe and smart operations are essential for American participation in the global economy.

Still, more than five months after the terrorist attack, a great deal needs to be done immediately if we are to safeguard these facilities from terrorism and crime. It is essential to realize that increasing the efficient operation of the ports will produce enhanced security.

Failure to protect these facilities could have catastrophic effects. For example, a chemical high explosive coated with radioactive material that was detonated in a major port during peak work hours would likely produce prompt fatalities far in excess of those at the World Trade Center on September 11. And the psychological effects of the attack-skyrocketing uncertainty worldwide about the safety of US ports—would have a profoundly deleterious impact on US maritime trade and therefore on the health of the entire national economy.

Consider the situation on the West Coast. The ports at Los Angeles and Long Beach, Oakland, Seattle, Tacoma and Portland handle containerized cargo that support nearly four million workers throughout the United States. In 2000 almost $260 billion of containerized exports and imports transited through these ports, creating total business revenue of $723 billion, equivalent to 7% of the nation's gross domestic product. Credible estimates suggest that international trade between the United States and Asia will double in the next decade, producing dramatic increases in these measures of economic activity, assuming maritime trade remains unimpeded.

---

[1] Michael Nacht is Dean and Professor of Public Policy in the Goldman School of Public Policy at the University of California, Berkeley. He is a member of the Threat Reduction Advisory Committee to the Office of the Secretary of Defense where he chairs a panel on Combating Terrorism Using Weapons of Mass Destruction.

The ports face formidable challenges, however. These include inadequate protection against terrorist attack and criminal activity; a shortage of available land for expansion; large numbers of trucks entering the ports that add significantly to road congestion and air pollution and whose queues increase port vulnerability to terrorism and crime; and inefficient use of available technologies and work practices that reduce productivity in the container yards and cost the maritime industry as much as $1 billion annually. But a number of feasible modifications could be implemented drawing on existing operations at ports in Singapore, Hong Kong, the Netherlands, the United Kingdom and elsewhere.

The key point is that the utilization of existing simple and basic technologies can facilitate the seamless flow of information, eliminating errors and delays currently introduced by human intervention. Both the security and the productivity of the ports would be enhanced significantly if these technologies were applied and existing work practices were modified.

Indeed much of what should be done at the West Coast ports is already standard practice at some East Coast and Gulf Coast ports as well as at many facilities abroad. What is needed, therefore, are not radically new technologies or procedures.

If we fail to put into practice these easy-to-understand and easy-to-implement technologies, we do so at our own peril.

A Snapshot of Current West Coast Port Operations [2]

There is no technological "silver bullet" that will magically revolutionize port operations. But there are a number of applications of existing technology that would collectively and over time have a dramatic impact on the security and productivity of the ports.

Consider the basic elements of current West Coast port operations. Each port has a number of terminals that are utilized by one or more global carriers. About 20 operators have 50-80% of global capacity and an even higher percentage of traps-Pacific capacity.[3] Trucks, mostly operated by independent trucking companies, arrive at the ports in large numbers early on weekday mornings. Most carry container loads to be placed on ships for export. They also pick up containers that have arrived as imports. Some trucks arrive empty (called "bobtails") to pick up containers.

At the gate to the terminal, the trucker provides information to a clerk identifying himself, his load, and the load he plans to pick up. If everything is in order, the clerk instructs the trucker where to drop his container and where to pick up his new load.

Clerks have information stored in computers about the location of containers in the yard that have been off-loaded from ships. If everything is not in order, the trucker pulls off to the side to a "trouble area" where he works out with another clerk the issues that have precluded him from entering the yard.

The amount of time the trucker has to wait to enter the yard is the "queuing time." The amount of time the trucker spends in the yard before leaving is the "trucker dwell time." Productivity of the terminal is directly related to the number of containers, or TEUs, handled per area per unit of time, the minimization of queuing time, and the minimization of trucker dwell time, among other measures.

In the meantime, the containers on ships are off-loaded by stevedores who operate large, ship-to-shore gantry cranes. Some containers are placed on wheeled chassis and are parked in the yard by longshore tractor operators. Other containers are taken to specified locations in the yard and stacked on the ground, usually three-to-four high. Some of the containers are eventually removed from the yard by trucks, usually for delivery to destinations not far from the port. Others are placed on railroad cars for intermodal transportation to destinations distant from the port.[4]

It is not unusual for containers to be misplaced. Containers in this category are labeled "unable to locate" or UTL. In some West Coast terminals it is estimated that 610% of the containers in the yard are UTL.

---

[2] For a more detailed account of port operations and needed adjustments see Michael Nacht, "Working Smarter, Faster, Safer: Technological Innovations and Adjusted Work Practices for Enhanced Security and Productivity at West Coast Ports," October 26, 2001.

[3] The largest is Maersk-Sealand, a Danish firm that, at the beginning of 2000, had 236 ships and carried more than 565,000 TEUs, about 8% of the world fleet. Many of the carriers are privately owned, some are government-backed, and still others are a combination. There are numerous forms of cooperation among the carriers. Particularly notable are "alliances" among carriers that foster customer focus, produce cost advantages, and encourage sharing of facilities and equipment. See Container Shipping Industry: Moving the Box-Shifting the Paradigm, October 2000, Ing Barings Asian Regional Research. pp. 6–7.

[4] Note that sometimes trucks take containers from the terminal to locations for consolidation with other containers rather than for delivery. Then these containers are loaded on to trains for transit elsewhere. This process is known as "transloading."

Efficient movement of the containers in the yard and high-accuracy knowledge of the location of each container obviously affects the dwell time of truckers. If containers are left at the yard in excess of an agreed period of time, the trucker is charged a fee (a "demurrage" or late charge) that is either paid by the trucker or his employer.

What then is to be done? Here are six recommendations.

1. *Trucker Identification and Registration System*

Today, truck driver identification is determined by the clerk at the gate, and is subject to the imperfections of human inspections. it is the norm that only when the truck driver reaches the gate is his identity made known. Driver identification is determined by the clerk at the gate, and is subject to the idiosyncrasies of individual human inspections. Instead, each driver should be issued a port-specific picture identification card with driver license number, vehicle registration, work permit, safety record, and insurance information.[5] A registry should be established that holds this information for all truckers permitted to enter the facilities of a given port.

2. *Port Personnel Smart Card Authentication System*

A smart card system using "biometrics" can perform identification and authentication almost instantaneously using electronic fingerprint identification, facial geometry, signature recognition and voice recognition. Every port employee and trucker authorized to enter the port area should be issued a smart card [a plastic card the size of a credit card with a power computer chip embedded within it containing relevant information (e.g., driver license number) and unique biometric information (e.g., fingerprint)]. The chip would be programmed to permit each individual access only to pre-authorized sector of the port.

The system would have to be implemented in such a fashion as to minimize interference with the rapid movement of the containers through the yard, which is essential for high terminal productivity.[6]

3. *Trucker Appointment System*

A number of ports worldwide, including some on the East Coast, have introduced systems in which each container pick-up from or delivery to the terminal is conducted on an appointment basis. An electronic record of a planned pick-up or delivery would be provided to the gate control personnel before the truck arrived at the terminal ("pre-filing of information"). This record would include driver identification and insurance information; pickup and delivery authorization; trucking company identification; booking data; container identification; special handling (for example, hazardous material identification or refrigerated container setting) information; and seal numbers (all containers currently are closed with traditional security seals that can only be cut with extremely heavy bolt cutters to minimize tampering). The record could be tied to a universal transaction number that would be used to track container movement from origin to destination.[7]

Some trucks could be pre-authorized to proceed through the gate without stopping. There are terminals in Los Angeles/Long Beach that already use an elementary version of this system for "bobtails" (trucks with chassis but no containers). With this method bobtail arrival is scheduled in advance by fax. When the bobtail approaches the terminal it does not wait in the standard gate queue but travels along a passing lane and enters the yard after the normal identification security check without otherwise stopping, thus reducing appreciably the overall queuing time for the terminal.

The appointment system should also be linked to an "appointment window." Drivers would have a specific 30-minute time, for example, in which to enter the terminal. These appointment windows would be established through internet communication in which truckers could determine both the status of the container to be picked up and the availability of an appointment at the marine terminal. If they were running early or late, the driver would communicate with terminal personnel by cell phone to determine if they could adjust their arrival time. By staggering the arrival of trucks using a computer-generated algorithm, there would be substantial reductions in road congestion outside the terminal, queuing time, and dwell time.

Again, it is important to stress that reduction of road congestion outside the terminal, queuing time, and dwell time all contribute to increased security as well as enhanced productivity.

---

[5] See Thomas Ward, "Improving Container Transport Security," September 2001.

[6] In general, implementation of systems to enhance security will increase operating costs and could introduce new strains on deliveries. See Claudia Deutsch, "Agents of Recovery Under Stress," The New York Times, October 9, 2001, pp. C1, C14.

[7] This system is not novel. It is already widely used by warehouse personnel of major retail corporations in the United States who handle large amounts of freight by truck each day.

4. *Electronically Read Tamper Evident Seals*

Special security seals, termed "electronically read tamper evident seals," should be required for installation on all containers. Coupled with a global positioning system connection, they could provide real-time evidence of seal tampering to a container monitor at the terminal.[8]

5. *Container Intelligence*

Currently, painted markings are the only external form of container identification. At most terminals, closed circuit television monitors are used by gate clerks to read license plates and container numbers. Still the waiting time at the gate can be appreciable.[9] One improvement would be to install optical character recognition (OCR) readers at the terminal gates that would record the container number and add it to the terminal's database. Alternatively, all containers could carry electronic tags that emit signals received by antenna at the gate and record the appropriate information. If the electronic tag were connected to a differential global positioning system, the location of the container once in the yard would be known with almost perfect accuracy. Implementation of either approach would reduce waiting time at the gate appreciably and lower the risk of mistakes associated with a casual labor force (see 6. below).

At present the assignment of yard equipment at most terminals is based on the experience and intuition of the longshoremen. With precise knowledge of container location and the implementation of an appointment system, the assignment of yard equipment could be optimized with a straightforward, computer-generated algorithm.

To enhance container intelligence these measures must be coupled with the screening of containers closer to the point of origin (not in US ports). Measures to strengthen cooperation with ports worldwide have merit and should be seriously considered.

6. *Automated Dispatch Hall and Dedicated Work Force*

For many years until today, the procedure for longshoremen work assignments has been predicated on gathering workers each morning at a central location within the harbor area, providing assignments to each individual, and then scattering the workers throughout the port to their particular workstations. This approach has three major disadvantages: it is very time consuming, it leads to continuously changing work assignments (a "casual work force"), and it reduces security since the current system makes it easier for non-authorized personnel to enter the yard. Instead, an automated dispatch hall should be established in which all workers are issued valid identification cards and every effort is made in advance to match worker skills with positions that need to be filled. Where at all possible, continuity would be emphasized so that a dedicated, steady work force would be deployed throughout the port area. Workers would know in advance where they are to work, thereby eliminating the waiting time each morning from arrival at the dispatch hall to arrival at the workstation. And they would build up a pattern of consistency in their assignments that would enhance their skills and provide more efficiency, predictability, and productivity in container yard operations.

The Congress needs to exercise its vital watchdog role to ensure that these recommendations are implemented as rapidly as possible. It is not melodramatic to conclude that we procrastinate at our peril.

Statement of Port of Oakland

The Port of Oakland welcomes the opportunity to provide this written testimony before the Senate Judiciary Committee's Subcommittee on Technology, Terrorism and Government Information. We applaud the Subcommittee for holding this important hearing. We at the Port of Oakland are working diligently to improve security at our maritime facilities in the wake of the terrorist attacks of September 11, 2001. In conjunction with the U.S. Coast Guard and our maritime tenants we have al-

[8] Container security is a major problem in itself, related closely to the security of ships as they enter port. This involves U.S. Coast Guard operations and other issues that are not addressed in this testimony.

[9] In many instances, current work practices at the gate involve unnecessary human involvement that is inefficient and time-consuming. The system employed in many terminals is analogous to a bank customer obtaining funds at an automatic teller machine, acquiring a receipt for his transaction, but then having to go into the bank to have the teller validate that the receipt is genuine.

ready instituted a number of new interim security procedures and protocols, as well as begun planning for more permanent measures.

Since September 11t", the U.S. Coast Guard has instituted a wide range of security measures on all ships entering U. S. ports. In the San Francisco Bay, these measures include the establishment a security zone from the San Francisco Bay entrance seaward to 12 nautical miles. Vessels are screened and profiled according to risk, with high-risk vessels being boarded and escorted. Some vessels are also boarded and escorted at random.

In addition, 1/2 mile security zones have been established in areas of San Francisco Bay adjacent to San Francisco International Airport and Oakland International Airport. Persons and vessels are prohibited from entering these zones without permission from the local Captain of the Port. The Bay Area Coast Guard Office was the first Coast Guard Division to institute this new Sea Marshal program. It continues to implement the program throughout the San Francisco Bay Area.

The Port of Oakland's terminal operators in the wake of the September 11th attacks immediately implemented a wide variety of terminal security and protective measures. These include:

1. Limiting access to facilities by visitors to vessels, tours, port contractors
2. Scheduling appointments by vendors, contractors, suppliers for needed vessel or terminal services.
3. Installing new security warning signs at gates and entrances.
4. Enhancing gate security procedures to stop all private vehicles, checking ID's
5. Preventing passengers in delivery trucks from entering the facility.
6. Checking and verifying documentation of all hazardous cargo before allowing entrance to facilities.
7. Increasing the number of roving security guards to check all fenced perimeters as well as the waterside of the terminal.

Working with other ports on the West Coast, the Port of Oakland has been working closely with the U.S. Coast Guard and its terminal operators in further developing interim security guidelines that would set minimum standards for all Port facilities in the U.S. Coast Guard's Pacific Area [California, Oregon, Washington, Alaska, Hawaii and Guam]. The Port established a local Seaport Security Committee, inviting terminal operators and shipping line representatives, the local Captain of the Port, Port Pilots, local police, as well as representatives from the U. S. Customs Service and the Immigration and Naturalization Service (INS) to review and provide input as the guidelines were developed. These interim guidelines were authorized on January 28, 2002 and will take effect over the next several months. It is anticipated that these guidelines will remain in effect until permanent regulations are published, we hope, in the next year.

The Seaport Committee is also exploring the feasibility of a new identification system required for all port workers within Oakland and San Francisco Bay, as well as working with the Oakland Police Department to determine appropriate levels of increased patrol and law enforcement presence within the Port area. The Port has also volunteered to participate in a Maritime Administration-sponsored smart-card identification system prototype evaluation.

Port staff and terminal management staff are updating facility security plans and developing a listing of facility security improvements that will be required to come into compliance with federal regulations when fully implemented. The Port's operations staff in cooperation with the Port's terminal operator tenants have completed a physical survey of all marine terminal facilities and initiated service requests to repair or upgrade fences and other physical security measures as appropriate. The Port has also identified more major security infrastructure projects that will be needed to enhance Port security. These include:

Item	Description	Estimated cost million
1.	Emergency communication system for U.S.C.G./Oakland Police/U.S. Customs/ Terminal Operators/Port and Terminal-to Terminal telephone/radio alert system..	.30
2.	Armored gates/spikes to prevent egress.	2.50
3.	Radiation readers at exit gates.	.70
4.	Surveillance cameras and improved terminal security lighting, port-wide; video surveillance of key entrance corridors to Port area..	12.30
5.	Improving/replacing terminal fencing with k-rail/cables, fiber-optic alert systems	13.60
6.	Hardening/under grounding key high-voltage utility lines/port area sub-stations.	11.80
7.	Smart Card Access Control system and installation.	4.50

Item	Description	Estimated cost million
8.	Augmenting Oakland Police emergency Response capability and installation of Police substation in Port area..	2.80
9.	Crash barriers/armored gates to prevent Access [high security requirement]	9.30
10.	Miscellaneous security enhancements Port-wide and construction contingencies.	10.20
	TOTAL ESTIMATED COST	$68.00

Other California Ports costs have cited similar costs related to additional security measures ranging from $25 million to more than $100 million depending on the size and activity of the Port.

Prior to September 11th the Port's security resources were primarily invested in preventing crime and cargo theft. Since September 11th, our focus has changed to incorporate the potential threat of terrorism. Perhaps the biggest challenge facing our industry in addressing this security issue is the fact that there has not been a clearly defined threat to the nations' seaports. Given the increasing volumes of people and goods moving through our seaports, the U. S. government and the international community has no credible way to reliably detect and intercept illegal and dangerous people and goods that move through our maritime and surface transport networks.

Seaports cannot be separated from the international transportation system to which they belong. Ports are, in essence, nodes in a network where cargo is loaded on or unloaded from one mode—a ship—to or from other modes—trucks, trains, and on occasion, planes. Efforts to improve security within the port, therefore, require that parallel security efforts be undertaken in the rest of the transportation and logistics network. Port security initiatives must be harmonized within a regional and international context. Unilateral efforts to improve security in California ports, for example, without similar efforts to improve security in the ports of our neighbors will lead shipping companies and importers to "port-shop"; i.e., to move their business to other market-entry points where their goods are cleared more quickly. Finally, Ports should not be viewed as a primary line of defense in an effort to protect the U.S. homeland. A credible security system should identify and take the steps to preserve the flow of trade and travel that allows California and the U.S. to remain open and competitive in today's global market.

Regarding on-going drug interdiction efforts that Senator Feinstein and the Subcommittee are examining, we can tell you that the number of drug and weapon seizures at Bay Area seaports has not drastically changed in the past year.

The U.S. Coast Guard and the U.S. Customs Service are the federal agencies primarily responsible for drug interdiction. The Coast Guard conducts inspections at sea, whereas the U.S. Customs Service actively searches for drugs in containers that reach U.S. ports. Since September 11th, there have only been a few incidents of drug smuggling at the Bay Area ports—two occurred in San Francisco. None have occurred in Oakland.

It is our understanding that although there has been a decrease in manpower devoted to drug interdiction at the U.S. Customs Service, due to a new focus on security issues, the reduction has not taken away from the U.S. Customs Service's commitment to intercepting illegal drug shipments into the United States.

The California National Guard has recently been brought into this effort. The Guard will be loaning a mobile container inspection machine that searches for drugs and weapons (vehicle and cargo inspection systems). We expect to have the use of this machine and six National Guard personnel for the month of March.

The Port of Oakland thanks the Subcommittee and Senator Feinstein for the opportunity to submit this testimony. We look forward to working with you as we work to insure that our nation's ports as safe as possible for the benefit of all the American people.

Statement of John H. Warner, Jr., PhD, Corporate Executive Vice President and Director, Science Applications International Corporation (SAIC), and James Winso, Corporate Vice President, General Manager Security Products, Science Applications International Corporation (SAIC)

After the September 11, 2001 terrorist attacks, SAIC completed an internally-funded, fast-paced study to determine ways to improve our country's port security and to deal with the millions of containers entering our country each year. A team

of experienced counter-terrorism experts with domain expertise in weapons of mass destruction (WMD) and maritime trade was convened for this study. This statement provides a brief summary of the results of this study.

About 20 million containers enter the U.S. each year through our port and border crossings. Approximately 40% of the containers entering U.S. portsenter through the major California ports. Our study focused on the WMD threats with emphasis on nuclear weapons, but with some consideration of biological weapons also. We examined several threat scenarios, global transportation, various security related technologies, as well as institutional involvement and barriers for improving port security. An overall system architecture for improved port security was developed. Significant results are summarized below:

1. The problem is complex and an overall systems level approach is needed with both short term and long term objectives.

2. There is a strong difference between the nuclear threat with intended detonation in a harbor versus the nuclear threat for intended movement of the weapon to another part of the country. Obviously, the weapon intended for detonation in a harbor needs to be identified and neutralized well prior to harbor entry and ship unloading.

3. Long term, and for threats for targets interior to the U.S., while non-intrusive inspection or intrusive inspection can take place entirely in the U.S., some degree of cooperation of countries exporting to the U.S. is important for vetting containers based on their history and the identity of the people, organizations and countries involved in transporting them to the U.S. Inspection, tagging, sealing and tracking technologies are useful in such a process. A process could be established to vet containers depending on the conditions of origin and transport. The vetting process would determine which containers needed the more disruptive, intrusive inspection at the U.S. port. Processes to minimize disruption of trade for this concept were developed.

4. Long term, and for threats where the U.S. port is the target, the above concept fails because high confidence is needed in understanding which containers might be threats prior to entry into U.S. waters. Inspection must occur either at the point of origination or offshore from the U.S. Containers could be inspected by a certified inspection agency at loading and then sealed externally or internally or both. Non-certified containers would need 100% non-intrusive inspection prior to entry into U.S. waters. This could be far more disruptive to trade. By a suitable combination of rule making and carrier operated inspection processes, economic incentives in the form of ease of entry into U.S. ports, reduced trade violations and enhanced revenue collection, such a concept could be made attractive and could actually facilitate legal commerce. However, the ability to gain the cooperation of trading partners for such inspections may 'require the U.S. to reciprocate by inspecting all containers leaving the U.S. and bound for agreement countries.

The above concepts need to be studied in far more detail and any implementation would take time, as well as the cooperation of trading partners. Obviously, some partners would be more cooperative than others. However, recently the world went through the Y2K problem and cooperation was achieved to insure that ships entering U.S. ports were Y2K compliant prior to entry. Although a smaller problem, the incentives were established to encourage safe operation and navigation of ships in U.S. ports. The U.S. Coast Guard working with international maritime organizations played a strong role in achieving this cooperation.

The U.S. cannot afford to wait for a "silver-bullet" comprehensive solution to our port security problems before we act. Short term, more non-intrusive inspection is important for containers arriving in the U.S and this should be done as soon as possible. At present, only a very small percentage of containers are inspected at the U.S. entry ports due to the high manpower requirements for physically unloading and reloading containers. Technologies and products are available today, which, if properly used, could make substantial improvements to U.S. port security without such high manpower requirements.

As one example, SAIC produces the VACIS (Vehicle and Cargo Inspection System) in our San Diego facilities. The U.S. Customs Services has purchased over 80 VACIS units and has been implementing them at an accelerated rate for the past three years. These non-intrusive inspection systems have been deployed by U.S. Customs along the land borders with Mexico and Canada and are also being deployed in U.S. seaports. They have proven their effectiveness over the last several years by enabling significant seizures of contraband entering the U.S. The mobile VACIS version appears to be particularly well suited to be used at U.S. ports, since the unit can be easily moved to the ships being unloaded and the inspection time

is minimum. Thus, containers can be inspected without impacting the flow of commerce in the ports.

Pioneered by the U.S. Customs Service in 1994, the SAIC VACIS system has become the world's most advanced gamma-ray inspection system for cargo containers (e.g., trucks, railroad cars, shipping containers, etc.). VACIS uses naturally occurring gamma rays to inspect an entire container in a matter of seconds even while the container vehicle is in motion. The system emits a narrow, low intensity gamma beam that is directed at a highly sensitive detector array. As this beam penetrates a moving or stationary object, a computer generates a high-resolution image of the container under inspection. SAIC's patented technique allows reconstruction of this Radiographic Image of the contents of the container with an extremely small amount of Ionizing Radiation (a dosage equivalent to that received in one minute of aircraft flight). This image is generated by custom software that was developed by SAIC's image processing scientists and engineers specifically for this application.

Designed for simplicity of operation and maintenance, all of SAIC's modular gamma ray systems have a minimum of moving parts, easily replaceable components and easy-to-use software. Each individual component has been proven in countless commercial applications and, in fact, the availability rate of the over 50 VACIS units deployed by U.S. Customs has been demonstrated at over 95% over the last four years. VACIS' simple yet effective design and proven operational success means VACIS offers easy installation, reduced training time, with minimal maintenance and repair. All of these features have supported U.S. Customs ambitious program for implementing an effective cargo-screening program.

Other technologies and products are available for sensing different emissions or other characteristics associated with various threats. For example, one version of VACIS will allow imaging while simultaneously detecting radiation emitted from the container. Other sensors, with various degrees of effectiveness, exist for chemical detection.

In summary, an overall systems level approach to the problem of increasing our port security is important to achieve the proper degree of security without causing strong barriers to commerce. Achieving long term objectives will take time and effort. However, technologies are available today to achieve major improvements in port security and meet shorter-term objectives with only minor impact on the flow of commerce.

○