S. HRG. 108–1014

THE STATE OF MARITIME SECURITY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

MARCH 24, 2004

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

U.S. GOVERNMENT PUBLISHING OFFICE

21–190 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JOHN MCCAIN, Arizona, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina, *Ranking*
CONRAD BURNS, Montana	DANIEL K. INOUYE, Hawaii
TRENT LOTT, Mississippi	JOHN D. ROCKEFELLER IV, West Virginia
KAY BAILEY HUTCHISON, Texas	JOHN F. KERRY, Massachusetts
OLYMPIA J. SNOWE, Maine	JOHN B. BREAUX, Louisiana
SAM BROWNBACK, Kansas	BYRON L. DORGAN, North Dakota
GORDON H. SMITH, Oregon	RON WYDEN, Oregon
PETER G. FITZGERALD, Illinois	BARBARA BOXER, California
JOHN ENSIGN, Nevada	BILL NELSON, Florida
GEORGE ALLEN, Virginia	MARIA CANTWELL, Washington
JOHN E. SUNUNU, New Hampshire	FRANK R. LAUTENBERG, New Jersey

JEANNE BUMPUS, *Republican Staff Director and General Counsel*
ROBERT W. CHAMBERLIN, *Republican Chief Counsel*
KEVIN D. KAYES, *Democratic Staff Director and Chief Counsel*
GREGG ELIAS, *Democratic General Counsel*

CONTENTS

WITNESSES

APPENDIX

THE STATE OF MARITIME SECURITY

WEDNESDAY, MARCH 24, 2004

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Committee met, pursuant to notice, at 9:30 a.m. in room SR–253, Russell Senate Office Building, Hon. John McCain, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOHN MCCAIN, U.S. SENATOR FROM ARIZONA

The CHAIRMAN. Good morning. The Committee meets today to consider the state of maritime security in the United States and around the world, specifically efforts related to vessel, port, and cargo security and personnel with access to vessels and cargo at maritime facilities. The Committee hopes to learn what's been done to improve maritime security over the two and a half years since the terrorist attacks on New York and Washington.

I commend Secretary Ridge and all the employees of the Department of Homeland Security who have taken on the monumental task of securing our homeland while managing the largest government reorganization in history. It's clear the Department has made significant strides and established the foundation for a layered approach to transportation security in the year and a half since the Homeland Security Act of 2002 and the Maritime Transportation Security Act were signed into law.

Yet their task is far from complete. No comprehensive maritime security plan exists. I'm concerned that a lack of resources and the demands of the reorganization have inhibited the Department's focus on its security mission.

The three witnesses from DHS here today directly oversee the agencies most involved in maritime security, the Coast Guard, Customs and Border Protection, and the Transportation Security Administration. These agencies spent millions of dollars on numerous and in some cases overlapping or duplicative pilot programs—projects, tests, initiatives, and programs aimed at improving maritime security, with questionable results.

For example, over 5,700 companies have signed up for the Customs Trade Partnership Against Terrorism, known as C–TPAT. While this would seem like a great success, many of those in the maritime industry associated with the program to increase supply chain security have started to openly question the value of this voluntary approach. Some participants continue to strongly adhere to the program's goals out of a sense of responsibility, while others,

driven by their bottom line, are moving away from the program and are only meeting those requirements in law, the regulation.

The lack of coordination and absence of established standards and goals have led to confusion for the maritime industry as to what must be done to improve security, and whom to go to with security questions. This type of confusion will lead to less cooperation from industry and ultimately to lax security.

The agencies represented here today must strive harder to improve coordination efforts. I was amazed to learn that it has only been in the last several weeks that the Coast Guard and Customs and Border Protection have reached an agreement to share manifest and vessel information reported to the two agencies by those involved in maritime transportation. I hope our government witnesses can shed some light on efforts to improve coordination and complete memorandums of agreement that define each agency's role and responsibilities.

I bring this to question the Department about this and believe that little effort has been put into completing these agreements, which not only better define agency roles, but also serve to direct and state local governments in the private sector when they try to get answers to security questions.

Further, we're going to hear from maritime industry representatives today who are concerned about future security costs. As I stated at yesterday's hearings examining the state of rail security, only modest resources have been dedicated to maritime and land security over the past two and a half years compared to the investments made to secure the airways. I believe one reason for this discrepancy is a lack of focus on maritime security on a comprehensive plan that sets standards and clearly identifies what efforts and costs are public versus private responsibilities.

If the layered approach to homeland security envisioned by DHS and its strategic plan is to work, it's imperative that all parties, both public and private, have a clear understanding of their roles and responsibilities.

I want to welcome all of our witnesses. I look forward to their statements regarding the current state of maritime security and hearing their recommendations pertaining to the needs that are still outstanding.

[The prepared statement of Senator McCain follows:]

PREPARED STATEMENT OF HON. JOHN MCCAIN, U.S. SENATOR FROM ARIZONA

The Committee meets today to consider the state of maritime security in the United States and around the world; specifically efforts related to vessel, port, and cargo security, and personnel with access to vessels and cargo .at maritime facilities. The Committee hopes to learn what has been done to improve maritime security over the two and half years since the terrorist attacks on New York and Washington.

I commend Secretary Ridge and all the employees of the Department of Homeland Security who have taken on the monumental task of securing our homeland while managing the largest government reorganization in history. It is clear the Department has made significant strides and established the foundation for a layered approach to transportation security in the year and a half since the Homeland Security Act of 2002 and the Maritime Transportation Security Act were signed into law, yet their task is far from complete.

No comprehensive maritime security plan exists, and I am concerned that a lack of resources and the demands of the reorganization have inhibited the Department's focus on its security mission. The three witnesses from DHS here today directly

oversee the agencies most involved in maritime security: the Coast Guard, Customs and Border Protection, and the Transportation Security Administration. These agencies spent millions of dollars on numerous, and in some cases overlapping or duplicative, pilot projects, tests, initiatives, and programs aimed at improving maritime security with questionable results.

For example, over 5,700 companies have signed up for the Customs Trade Partnership Against Terrorism, known as C–TPAT. While this would seem like a great success, many of those in the maritime industry associated with the program to increase supply chain security have started to openly question the value of this voluntary approach. Some participants continue to strongly adhere to the program's goals out of a sense of responsibility, while others, driven by their bottom line, are moving away from the program and are only meeting those requirements in law or regulation.

The lack of coordination and absence of established standards and goals have lead to confusion for the maritime industry as to what must be done to improve security and whom to go to with security questions. This type of confusion will lead to less cooperation from industry and ultimately to lax security. The agencies represented here today must strive harder to improve coordination efforts. I was amazed to learn that it has only been in the last several weeks that the Coast Guard and Customs and Border Protection have reached an agreement to share manifest and vessel information reported to the two agencies by those involved in maritime transportation.

I hope our government witnesses can shed some light on efforts to improve coordination and complete Memorandums of Agreement that define each agency's role and responsibilities. I have previously questioned the Department about this and believe that little effort has been put into completing these agreements which not only better define agency roles, but also serve to direct state and local governments and the private sector when they try to get answers to security questions.

Further, we are going to hear from maritime industry representatives today who are concerned about future security costs. As I stated at yesterday's hearing examining the state of rail security, only modest resources have been dedicated to maritime and land security over the past two and a half years compared to the investments made to secure the airways. I believe one reason for this discrepancy, is the lack of focus in maritime security on a comprehensive plan that sets standards, and clearly identifies what efforts and costs are public versus private responsibilities. If the layered approach to homeland security envisioned by DHS in its Strategic Plan is to work, it is imperative that all parties, both public and private, have a clear understanding of their roles and responsibilities.

I want to welcome all of our witnesses. I look forward to their statements regarding the current state of maritime security, and hearing their recommendations pertaining to the needs still outstanding.

The CHAIRMAN. Senator Hollings, welcome back.

STATEMENT OF HON. ERNEST F. HOLLINGS,
U.S. SENATOR FROM SOUTH CAROLINA

Senator HOLLINGS. Thank you very much, Mr. Chairman. Let me welcome Admiral Collins and our Commissioner of Customs, Mr. Bonner. Let me do a little taking of stock, because, you know, the Committee itself, right after 9/11, went into an intermural on airport and airline security. We finally got that through and we took up and unanimously reported out a port security authorization, and within that authorization we provided monies. Specifically, Mr. Bonner, we put in a $15 million container fee, approximately $700 million overall, that would take care of at least the 55 major ports.

That's just a start. As Admiral Collins knows, the Coast Guard has estimated a total port cost of $7.4 billion. We had to make a start, and we made a good start. There was a unanimous vote in the U.S. Senate. It went over to the House side and into a dogfall of a year's wrangle.

Number one, they said that this was a tax, a tax, a tax. I finally got the House parliamentarian to rule that it was not a tax, it was a user fee. Then they went into a wrangle about, "Well, wait a

minute, this affects revenues under the Constitution. It ought to derive in the House of Representatives." I said, "Fine, let's get the conference agreement and get the money and you folks just introduce it and we'll take it ipso facto right on the Senate side." No, no, they didn't want to do that.

As of now, we have no money. Can you imagine that? 9/11/2001, 9/11/2002, that's two and a half years, and we're still wrangling. We finally agreed to ask the President to report on how he would fund the port security program. You know that's 15 months ago and we have yet to hear from the White House. We've heard from the White House otherwise. They've opposed it at every stand. I'm telling you right now, we put a small amount and two supplementals into the Homeland Security bill. I was able to get in $450 million, and that $450 million should be compared to the $7.4 billion that Admiral Collins says it would take for the ports.

But be that as it may, we offered an amendment in the 2004 budget resolution, of a billion dollars. We unanimously adopted the budget resolution. The White House demanded that we drop it in conference and it was dropped in conference, so we got nothing there.

Then again, we were trying our best, Admiral, you remember the money we received from the emergency supplementals in order to get these towers. We credit our friend, Senator John Breaux—he said we ought to have these transponders, to throw the ball to ships coming in. But we had no towers to throw the ball, or signal. And so we put in 50, and they cut it back, I think, to 24, if it—and you've done your best to control your budget, Admiral Collins. We're not fussing at you. I'm just trying to bring the Committee up to par here on just exactly what's been done. So we did that.

Now, in the 2004 budget, they finally requested some $46 million, but, you know, we still don't have the towers. We hope to get the transponders in there, and I think by the end of the year, Admiral Collins, you attest to the fact that the ships will be ready under Senator Breaux's initiative.

But what happens is that as of this morning, just 2 weeks ago—we always talked about Osama coming in there at Mombasa, the port of Kenya, and going to Nairobi and to Dar es Salaam and Tanzania and blowing up the two embassies. Well, they came into the port of Ashdod, in Southern Israel, just 2 weeks ago. They were trying to hit, as best we can tell, a chemical facility, and targeted it, but they were intercepted. Ten of them were killed, 20 were wounded there as they infiltrated the port there in Ashdod. But Lloyd's of London tells us that Osama owns ten vessels, and he has an interest in ten more.

And the best we can, after two and a half years of wrangling, and everything else like that, the Congress has been acting, but we have yet to get any more than a recommendation of $46 million for 55 major ports and 361 ports overall.

So I commend you, too. You all have been working, and we've been in the hearings with you. You've been responding the best you can. And, Mr. Chairman, I appreciate your indulgence, but I think we ought to take stock and see just exactly where we are when—we're all talking, "We're in there, we're doing this, we're doing that," and everything else, 9/11.

On rail security, they have not even taken up your bill and my bill that we reported out of this Committee. We can't even get rail security debated on the floor of the Congress. And they blew them up in Spain. On port security, we can't get any money. We passed the authorization, we asked the White House to give us their plan; 15 months later, they have no plan.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Hollings.

I mentioned, at the hearing yesterday, which you were unable to be here because of the funeral of your——

Senator HOLLINGS. Yes.

The CHAIRMAN.—your friend in South Carolina, that it would be my intention, with your agreement, that we would mark up another rail security bill, in light of additional information that——

Senator HOLLINGS. That would be terrific, Mr.——

The CHAIRMAN. Fine.

Senator HOLLINGS.—Chairman. I appreciate your leadership on that——

The CHAIRMAN. Fine.

Senator HOLLINGS.—because that's the only way we're going to get it done.

[The prepared statement of Senator Hollings follows:]

PREPARED STATEMENT OF HON. ERNEST F. HOLLINGS,
U.S. SENATOR FROM SOUTH CAROLINA

Mr. Chairman, I would like to thank you for convening this hearing today to allow this Committee to consider port security and examine where we are some year and a half after the enactment of the Maritime Transportation and Security Act of2002. While you don't have to much coastal water near you in Arizona, you have allowed us coastal members more than adequate opportunity to consider whether we have taken adequate measures to protect our ports and the people and citizens the live around and near them. However, port security is an issue that is much more than an issue that impacts just the people living on our coast. It impacts our whole economy and the health and strength of this Nation because of the importance of the maritime trade.

Almost all of the overseas retail goods that are sold here in the stores and the malls and the retail outlets comes from overseas destinations. U.S. manufacturers also rely on the maritime transportation system, for instance in my state of South Carolina, the car manufacturer BMW, gets many of the components that they put into their car from overseas ports. Most of our petroleum product comes overseas in tankers, as well as many of the chemicals and other bulk commodities we use. If our system of port security fails, I can assure that all of the industries that rely on it will also suffer tremendous losses, as will our Nation as whole, so port security really is an issue that impacts every citizen in the United States, whether they know it or not.

In my opinion we have been able to take some steps forward to better secure our ports and our system of maritime security, but we have a long, long way to go, and I do not feel that this Administration has dedicated the resources really to address this issue in a comprehensive fashion. Less than two weeks ago, in the Israeli port of Ashdod in Southern Israel, two suicide bombers allegedly with ties to the terrorist organization Hamas, infiltrated the port of Ashdod, killing ten and wounding twenty, according to press reports there is speculation that the suicide bombers had targeted chemical facilities within the port, including the chemical agent bromine. Currently, Israeli authorities are investigating how the terrorist got into the country, including whether they secreted themselves in marine containers in order to gain access. Prior to the incident in Israel, Al-Qaeda operatives had used small boats to blow up the USS Cole, and a commercial oil tanker. We also know that Al-Qaeda terrorist networks used Al-Qaeda owned and controlled vessels to smuggle in terrorists and explosives used in the attacks on the U.S. embassies in Kenya and Tanzania, and that Al-Qaeda owns a fleet of merchant vessels.

So this is a very real threat that we are talking about, and I have concerns that we are not currently positioned to prevent an attack utilizing means of access through maritime transportation or through our maritime system. I can tell you, that in the event that something does happen, we do not have a plan to reopen U.S. ports to commerce, without admitting that we will do so with very real risks that the same event could occur again. I can also tell you that in the event that we have to close our ports for any length of time, we will cause catastrophic economic impacts. For instance, when we had a labor-management impasse on the West Coast resulting in a closure of the ports, it is estimated that it cost the economy 1 to 2 billion dollars a day in revenues. I can assure that, closure of U.S. ports for any period of time would resonate throughout our entire economy.

While have taken some steps forward in the implementation of the Federal security planning requirements, there are many questions left, as to whether the security plans will be aggressive and effective tools to deter terrorism, or whether we have shell plans. My sense is that we will receive the minimum level of security necessary to ensure Federal compliance absent real resources that are dedicated to security enhancements. Otherwise, the ports will spend money on what they traditionally spend money, and that is making sure that they can move cargo as effectively as possible. I feel that the resources issues must be addressed, and I will be introducing legislation to ensure that, one way or the other, that we have funds in place that will be used to enhance port security.

When we passed the MTSA, the Senate took the position that it should be paid for through user fees, and ultimately the House opposed our position, and supported by the industry, who claimed that it would be funded through the government. Well, the Administration, until this year, when they proposed $46 million to be funded, has proposed nothing. Repeatedly, I have offered amendments that have been defeated on party-line votes, to increase the funds allocated for Federal port security programs. Something has to be done to rectify funding shortfall, or someday, we will all be sitting around here pointing fingers at each other.

I'll give you just one example of the problem. In the MTSA, we required all vessels to carry transponders in order to broadcast crucial shipping information and to allow governments to track the movements of these ships. Actually, it was Senator John Breaux, who led the charge on this particular issue. This will allow us to tracks ships to make sure they are not heading into the Golden Gate Bridge, or aimed to hit a nuclear reactor at Indian Point on the Hudson River. Every ship will have this equipment by the end of the year, but the Administration has in the past two years proposed $5 million dollars, not nearly enough to even start the system. This indefensible, this should be a crucial part of our system of port security defense.

The CHAIRMAN. Fine. Get it out before the Committee, before this next recess, and, if necessary, exercise the amending process in order to get this issue addressed.

Thank you, Senator Hollings.

Senator Breaux?

STATEMENT OF HON. JOHN B. BREAUX,
U.S. SENATOR FROM LOUISIANA

Senator BREAUX. Thank you very much, Mr. Chairman, again, for following up with this hearing with the one yesterday on rail security.

Over in the Hart Building right now, we are having some very high level and highly televised hearings on what happened on 9/11 and why we weren't better prepared, while we're having a hearing here today to find out how to get prepared so it doesn't happen again. This is where it really starts. They're looking at why we didn't do what we should have done when we should have done it, when today, I mean, we're really looking at what we need to do to prepare ourselves to make sure it doesn't happen again so there's not going to be another hearing sometime in the future to analyze why we weren't better prepared when a ship blew up in one of our ports and destroyed the lives of innocent individuals. So this is

where we solve the problems, and they're over there looking at the mistakes and what happened.

This is very, very serious. I mean, we've done a good job, I think, on airline security. We've spent four and a half billion dollars, we've got locks on the cockpit door; you have to go through metal detectors; and professional Federal inspectors in the airports. It's a whole new system with regard to aviation. But I fear that, in the area of rail security and in the area of port security, we're not nearly there yet. And if I were a terrorist, as I said yesterday—I mean, you can't think like they do, but you would assume that if they're going to attack another target, it's going to be the weakest target, not the strongest. And I think that when you look at weak targets, targets that are open for terrorist activities, you've got to look at the ports as one—and the rails—as one area that could have some very serious problems.

If you think about it, I mean, we had these hearings with the Chairman at that time, Senator Hollings, and we had hearings in Charleston, we had hearings in New Orleans, we had hearings in Houston, we had hearings on the East Coast, the West Coast, and I was really struck by the total lack of preparation because we had never considered, I guess, how vulnerable our ports are. If you think about a container ship as an example, they could have as many 3,000 containers on one ship, and each container carrying up to 60,000 pounds in each container, whatever they wanted to put into it.

And if you think about a ship with 3,000 containers being in a port that is located next to an LNG facility, which is located next to a chemical plant in the middle of a city, which we have in this country, you can imagine what one container filled with explosives could do to a city and a community if it was containing explosives and it was detonated. We've seen what a 35 foot vessel can do to a military naval ship. It blew a hole in it and killed innocent men and women, who were unsuspecting. And that was a 35 foot little boat that blew a hole in the USS Cole.

So this is a very, very serious problem. We've not done enough. Senator Hollings has said that. Money is the big problem, not your determination, Mr. Bonner and Admiral Collins; you all have done a terrific job, and will continue to do so.

We have, today, the Chairman—President of the Port of New Orleans, Gary LaGrange, who is up here. We invited him. It has been a port since about the 1700s down there. A ship sank in the port just a couple of days ago, stopped traffic for 4 days, just an innocent accident. And when you stop that, I mean, you stop commerce throughout the middle part of the United States of America. And that was, you know, not a terrorist activity, but it shows you what can happen.

The AIS system, the Automatic Identification System, is not in place, we said it should be, to track those vessels, where they are at every point in time. We know where every airplane is at every point in time, but we don't know where every ship is, and we've got some real holes in this system. And hopefully this hearing will be helpful in trying to fill the holes.

Thank you.

The CHAIRMAN. Senator Snowe?

STATEMENT OF HON. OLYMPIA J. SNOWE,
U.S. SENATOR FROM MAINE

Senator SNOWE. Thank you, Mr. Chairman. And thank you for holding this hearing this morning.

I want to welcome our witnesses, Admiral Collins, the Commandant of the Coast Guard, and Mr. Bonner and Admiral Stone. I thank you for being here, because obviously this is a key priority and a cornerstone of ensuring the integrity of our borders, and that is, of course, to secure the maritime transportation system.

As Chair of the Ocean, Fisheries, and Coast Guard Subcommittee, I certainly think that we have to do everything that we can to ensure that we are protecting our borders, in terms of what happens to the ships and the contents of those ships that come to this country. And some of the key port security priorities is to advance the acceleration of the Deepwater funding, which will provide the Coast Guard with updated capitalization, in terms of the assets.

And I'm concerned with also ensuring that ports, based on the Port Security Assessment Plan, have the adequate resources to implement those plans. That's another area for discussion here this morning. And also, making sure that staffing levels for the Container Security Initiative are high enough to ensure that the weapons of mass destruction never reach our shores.

Mr. Chairman, given the fact that only around 5 percent of the 6 million containers that come to this country from overseas are inspected each year, only 12 percent of all containers, whether it's air, land, or sea—and 95 percent of trade from outside North America comes into the United States by sea—it's absolutely vital that we focus on the security of our ports as a first line of defense.

Interestingly enough, there was a RAND report that was issued in August of 2003, and it stated that the maritime sector, and specifically the container transport sector, remain wide open to the terrorist threat, and the system is perceived to be poorly defended against misuse and terrorism due to its global and open nature.

So I think that is a stark assessment and characterization of where we stand today with respect to port security. I know the Coast Guard, the Bureau of Customs and Border Protection, and other Homeland Security agencies have made great progress in protecting our Nation against catastrophic terrorist attacks, but, as we, you know, know, we have a long ways to go in this process.

Last year at this hearing, I expressed concerns about the fact that Customs personnel were not equipped with personal radiation detectors. That now is not the case; everyone is equipped, as I understand it, with those detection systems, and that is very important, because that is central to our ability of protecting the maritime system from infiltration by weapons of mass destruction.

I do believe that we have to accelerate the Coast Guard Deepwater Project. The Coast Guard has been debilitated by degrading assets, and I'm concerned about the Administration's timeline for the 22-year project for the upgrade of the Coast Guard vessels. I think we have to accelerate that. In fact, I included a report last year in the Homeland Security Act that, in fact, underscored the necessity of accelerating that project, and that, in fact, that we would reap the gains and benefits of doing so. I do not believe that

we can wait any longer to acquire the necessary assets for the Coast Guard.

We're facing an ever-present danger, and the Coast Guard is facing extraordinary burdens in ensuring the security of our ports, and they need this capitalization and modernization of their assets sooner, rather than later, Mr. Chairman. And I hope that we're going to be able to turn that timeline around.

Second, it's funding. I know that's been indicated here this morning. Again, in order for the Coast Guard and others to comply with the mandates of the Maritime Transportation Security Act, I'm very troubled, again, that the Administration has requested $46 million in port security grants for Fiscal Year 2005, which represents a 63 percent cut, down from $150 million in Fiscal Year 2003, and $125 million in Fiscal Year 2004. That is a dramatic reduction at a time, I might note, ironically and coincidentally, that the Coast Guard has even indicated that it will take $5.4 billion on enhanced security grants over the next 10 years to comply with the mandates required under the Maritime Transportation Security Act. So clearly there is an enormous gap and discrepancy between our needs and that which is being requested by the Administration.

So, obviously, the funding is inadequate. I think we need to fight for additional increases in appropriations. And, finally, Mr. Chairman, we can't wait, or afford to wait, until the dangerous cargo is already in our port. I've been a strong supporter of the Containment Security Initiative. I think it's going a long ways to shoring up what comes into this country and securing—to make sure that those containers that might be identified as a high-risk threat do not enter this country. But, again, five-person teams deployed to the 17 CSI megaports is not adequate to do the job. Again, according to the CSI statistics, a five-person team in Singapore, which sent more than 400,000 containers to the United States from March 2003 to January 2004, reviewed only 63 percent of the cargo container's manifest. Obviously, that means that 160,000 container's manifests were not even reviewed to determine whether or not there was any risky cargo involved.

So we obviously have made strides, but we have a long ways to go, and I think we have to adopt a must-do attitude sooner, rather than later, Mr. Chairman, on all these fronts.

Thank you.

The CHAIRMAN. Senator Lautenberg?

STATEMENT OF HON. FRANK R. LAUTENBERG,
U.S. SENATOR FROM NEW JERSEY

Senator LAUTENBERG. Thanks, Mr. Chairman, for continuing to review the security concerns we have in our surface transportation as well as the ports that we're looking a little more closely at today.

When you think about it, and think about how quiet it seems in the port areas, it looks like we're kind of playing the "out of sight, out of mind" game here, not providing the resources that we need, and looking at departments that I think function very well in government—the Coast Guard, with its enormously expanding responsibility all the time. We always find, Admiral Collins, different things for the Coast Guard to do, even as we cut back on resources.

It has been a phenomenon that has been unpleasant to witness. I have great respect for the agency. And Customs people, I see them; they work very hard to do their job. And the volume of entries into the country, at airports and cruise ships, et cetera, is enormous.

When you look at it, if a terrorist organization is looking for a point of relatively easy penetration, just think about it, 55,000 ports of call are made each year. And where do these ships come from? They come from places that we know are not really necessarily friendly to the United States, and are usually fairly quickly accessible to those who would like to do us damage. So the task of securing our ports is enormous, but it won't go away by cutting back on the resources applied.

Recently, an official from the FBI testified before Congress that the agency has gathered intelligence suggesting that ports are a key vulnerability in our homeland defense. And, again, to be repetitive, terrorists know that, as well as we know it. Counterterrorism experts worry that terrorists could smuggle themselves, traditional weapons, nuclear, chemical or biological weapons into the country in these containers.

Robert Jacksta, Executive Director of the U.S. Customs and Border Patrol, testified last year that we inspected just 5.4 percent of the containers that arrived at our ports of entry. And despite that testimony, the Bush Administration's Fiscal Year 2005 budget proposes no Federal funds to help increase the number of containers being screened. Furthermore, Coast Guard officials have said, as we have heard from Senator Collins and Senator Hollings, that it will—Senator Snowe, rather, and Senator Hollings—will cost $1.4 billion in the first year, and $7.4 billion over the next 10 years, just to make the basic necessary physical security improvements in our ports. But the President, again, as we heard from Senator Hollings, is only asking for $46 million. That's the funding for this task in 2005. It's outrageous. But the President didn't mind using a seaport background, when he did some photographs for advertising, to suggest that he's concerned about a terrorist infiltration there.

It appears that the Administration expects port authorities and facility operators to comply with new security regulations with very little Federal assistance. Port security in my state is a major problem. The Port of New York and New Jersey is one of the biggest container ports in the world, handling over 16 million tons of ocean-borne cargo each year.

Hazardous materials move in and out of the port, through pipelines and over roads and freight line—and freight rail lines. And much of our vital surface transportation infrastructure in Newark Liberty International Airport are within a mile of the port. You can see from one to the other very clearly. Millions of people live near these facilities, which are vulnerable to terrorist attack. So it's easy to imagine what's at stake for New Jersey and New York and the Nation if the port's attacked.

Mr. Chairman, port security, one of those areas that makes me disappointed with the Administrations' homeland security effort, they don't put their money where their mouths are. The needs are out there. And rather than starting to address them, the Administration forces the good people at DHS to play budget games. And

we need them to have the resources they need to help secure our country against terrorism.

Last summer, we saw cross-training of air marshals and Customs employees. Yesterday, it was cross-training bomb-sniffing dogs. We've had requests to shift money from port security to pay for aviation security, where I think we are doing a pretty good job. But all we want is the security that comes with knowing our government is doing what it can to make our country safer from terrorism. That means we have to address the vulnerabilities that we know are there, particularly in our ports.

And, Mr. Chairman, I hope that this hearing will foster the attention and action that we need with regard to what we can do to secure our ports, and I greatly respect the fact that you're doing—following up yesterday's hearing with this one.

Thank you.

The CHAIRMAN. Thank you very much, Senator Lautenberg.

Senator Hutchison?

STATEMENT OF HON. KAY BAILEY HUTCHISON,
U.S. SENATOR FROM TEXAS

Senator HUTCHISON. Thank you, Mr. Chairman.

Mr. Chairman, I do appreciate your and Senator Breaux's and Senator Hollings' leadership in calling this hearing, along with Senator Snowe, who's the Chairman of the Subcommittee, because this is an area that I am very concerned that we have not put enough emphasis on in the past. You look at what happened in California, when there was a labor dispute that caused about, estimated, a billion-dollars-a-day in disruption to the economy, so you look at a disaster of some kind, and you are looking at the economic consequences that could be a huge impact on our fragile economic recovery. In addition, in my home state of Texas we have the largest chemical complex in America, the second largest in the world, sitting right on the port. So the kind of damage that could be done with a disruption in our system would be untold in terms of both lives and economic impact.

I believe it is time that we add to the Maritime Transportation Security Act that, frankly, our Committee took the lead on—and we were able to pass and have signed by the President, and it did a lot for port security—but I think we need to now add a second layer on that, and I am going to propose legislation in the near future, and look forward to having your input, because I want to do what we need to do to shore up the maritime container security, which will be the focus of my legislation.

It will do, first, the development of a national transportation security strategy to require the Department of Homeland Security to develop an overarching strategy designed to integrate the efforts of the Coast Guard as it develops its entire national security plan.

Second, to develop a container integrity initiative to build upon the Customs and Border Protection "smart box" concept, requiring, within 2 years, 50 percent of all containers coming into the United States to be in smart boxes.

Number three, start a point-of-origin security enhancement initiative. Building, again, upon the Customs and Border Protection Container Security Initiative, we would substantially increase the

number of U.S. Customs Service inspectors at foreign ports, just what Senator Snowe mentioned earlier needs to be addressed. I would have these inspectors phased in over a period of 2 years, so that we could have a real presence at the point of origin. If we don't have some capability to determine what is in those sealed-up containers at the point of origin, we will not have enough control when they get to our ports.

So I would welcome your input. I don't want to do something that would disrupt our trade and commerce. On the other hand, nothing could disrupt our trade and commerce more than a disaster at one of our major ports.

So, Mr. Chairman, I look forward to working with you and all the leaders in this effort to now take the next step in container security.

Thank you.

The CHAIRMAN. Thank you.

Senator Boxer?

STATEMENT OF HON. BARBARA BOXER,
U.S. SENATOR FROM CALIFORNIA

Senator BOXER. Thanks.

Mr. Chairman, I just want to take a minute to thank you and Senator Hollings, because I think Senator Breaux is right, everybody's over at the 9/11 hearing because of what happened; we're trying to do the work of making sure nothing else happens like that.

And yesterday, we had a great hearing—Senator Hollings, we missed you very much—on rail security, and I had a real problem with one of the Administration witnesses because I couldn't get a straight answer to a question, which was simply, "Where are you getting the money to do all these things that you want to do?" And they said they're taking it from other—from existing funds. Well, we never could get to the bottom of where they're taking the money from.

The bottom line is, if we're going to do this right, we'd better face the facts that we have to fund it some way. Whether it's a canine patrol or whether it's a high-tech way, like this Kevlar here, which I brought to show you, pass around—if we had containers made of Kevlar, they would be blast resistant, and we wouldn't cause damage. These are the things we have the ability to do.

I would like to put my statement in the record and conclude with a few points.

[The prepared statement of Senator Boxer follows:]

PREPARED STATEMENT OF HON. BARBARA BOXER, U.S. SENATOR FROM CALIFORNIA

Good morning. Mr. Chairman, I appreciate you holding this hearing today.

Two and a half years ago, the United States was caught unprepared when it came to aviation security. The results were devastating.

Since then, we have greatly improved our aviation security, and we have begun to improve our port security. We have a long way to go in both of these areas.

And clearly after the terrorist attack in Madrid, we must also address the vulnerability of our rail systems.

I was disturbed to read a quote by the Department of Homeland Security's Under Secretary for Border & Transportation Security Asa Hutchinson. He said that "it's very important that we do not simply react to an incident that happens anywhere in the world" and that the Administration was NOT seeking more funding for train

security. The Under Secretary said, "An aircraft can be used as a weapon. A train cannot be hurled through the air in the same fashion."

I believe that the terrorist attack in Madrid was a tragedy and I believe we act—even if the train cannot be hurled into the air.

In October 2001, this Committee passed a rail security bill. We knew that the United States must not be caught off guard when it comes to our passenger and freight rail systems.

However, the bill never became law.

This is extremely unfortunate when you look at the massive rail system in this country *(charts: passenger and freight rail systems).*

I am a co-sponsor of Senator Hollings's rail security bill introduced earlier this month. And, I am introducing legislation that will authorize funding for more police, canine dogs, and surveillance equipment on Amtrak and local transit systems.

I am also sending a letter to GAO asking for a study of the Department of Homeland Security's threat assessment of both the passenger and freight systems.

Both a threat assessment and Federal funding for everyday security measures are vitally important to our country, including California. California has the second highest Amtrak ridership in the country.

I look forward to hearing from the witnesses.

It is vitally important that we ensure that our Nation's entire transportation system is secure. And, it's our job to do that so thank you Mr. Chairman for this hearing.

Senator BOXER. And 40 percent of all the goods imported into the United States come through California. Senator Hutchison was so right in pointing out what happened when we had a strike, and how important it was to settle that strike, and the damage, the economic damage, that was done. Imagine if these ports were destroyed, God forbid.

So here's what we've got. The major cargo ports are Los Angeles, Long Beach, and Oakland. Other major ports are San Diego, San Francisco, and Stockton. I know so many of you know all these places, you've been to all these places. There are 12 major commercial harbors in California, and numerous other smaller ports that take the overload. I've been to Crescent City, down to San Diego. They need us. The Coast Guard is extraordinary, and the Coast Guard is stalwart. And you ask the Coast Guard, "Do you need anything else?" "Oh, we'll make do."

Well, I think we need to look at the GAO study. I guess Senator Lautenberg may have mentioned the number—$4.5 billion over the next 10 years is what GAO says is needed. And the Administration's asking for $42 million in this year's budget? I think, you know, we're in a Committee that's a can-do Committee, and this is an area that we must do.

I want to work with everyone. Congresswoman Millender-McDonald, from the L.A. area, has a very important bill that would call for major grants. We need to find a mechanism to pay for this. And we did have it, Senator Hollings, and then we couldn't get the bill—we got the bill through, but we didn't have a funding source.

Yesterday, I was on a TV program, on FOX, and the reporter said to me, "Well, don't you think we ought to do away with the gasoline tax? That'll bring down the price of gas." I said, "Yes, if you don't want to build roads. Yes, if you don't want to have transit systems." So, you know, we just have to be smart about this.

And I hope that, together, we can work across party lines—this is a great Committee to do that—so we can make sure that we're taking advantage of technology, that we have a funding source, that we avoid a 9/11 at our ports and our rail systems.

Thank you.

The CHAIRMAN. Thank you very much, Senator Boxer.

Our first panel is Admiral Thomas H. Collins, Commandant of the U.S. Coast Guard, the Honorable Robert C. Bonner, Commissioner of U.S. Customs and Border Protection, and Rear Admiral David M. Stone, who's the acting Administrator of the Transportation Security Administration.

And we'd like to begin with you, Admiral Collins. Welcome.

STATEMENT OF HON. THOMAS H. COLLINS, COMMANDANT, U.S. COAST GUARD

Admiral COLLINS. Thank you, Mr. Chairman, distinguished Members of the Committee, my pleasure to be with you today, and along with my Department colleagues, Commissioner Bonner and Admiral Stone, to update you on our Department's efforts to enhance maritime security, and the impact of those efforts on maritime commerce, and measures that we're taking.

The recent tragedy in Madrid clearly reminds us of the urgency of Homeland Security mission. We share the sense of urgency expressed by Senator Breaux.

Since 9/11, Secretary Ridge and all components within the Department, we've worked very, very hard to achieve the Department's strategic goals of awareness, prevention, protection, response, and recovery. And as part of that effort, we have developed a supporting maritime homeland security strategy consisting of four elements. And if I could indulge you just a minute, I will put up a chart that depicts the four categories—areas of interest, if you will—that dovetails with the Department's awareness, prevention, protection, response, and recovery strategies, all designed to mitigate maritime risk. That's what this is about.

Four major components, as you can see. One is to enhance what we call maritime domain awareness. That's to have visibility of threats and risks and things coming at us in the maritime. It starts there if you're going to make wise decisions about preventing things from happening. Building and administering an effective domestic and international security regime, it's increasing our operational presence and leveraging partnerships with state and local entities for success, and improving our response and recovery posture.

And listed under—detailed under each one of those major goals is all the individual—a partial listing, I might say, of the individual action items that we are taking, that we are investing in, that we're spending our collective energies in to move those goals along.

We are progressively and aggressively, each of our agencies, pursuing initiatives to support these strategy elements. And, again, all to mitigate risk.

The core of the maritime domain awareness effort centers on the development and employment of accurate information, intelligence, in targeting of vessels, cargo, crews, and passengers long before they reach a U.S. port. We want to understand the threat before it gets to Port Elizabeth. We want to understand the threat before it gets to L.A./Long Beach.

For example, the Coast Guard has made vessel notice of arrival reporting requirements much, much more rigorous, has instituted extensive screening procedures collaboratively with Customs and

Border Protection and the Office of Naval Intelligence, and is incorporating provisions for electronic submission of information. Customs, in turn, has requested earlier and more comprehensive cargo manifest information. All three of our agencies work collaboratively to fuse intelligence together to gain the clearest picture of risks.

The second element involves both domestic and international efforts to develop a new security framework, a security culture in the maritime—new standards of security, new processes, new procedures. It includes initiatives related to the implementation of the Maritime Transportation Security Act of 2002, the IMO—International Ship and Port Security Code Regulations that have been promulgated, as well as improving supply chain security and identity-security processes.

We published MTSA final rules in October of last year, the largest rulemaking in our history. These rules were jointly developed—jointed developed, collaboratively developed—between the Coast Guard, Transportation Security Administration, and Customs and Border Patrol. We are on schedule to implement the rule, effective 1 July of this year. And efforts also include, in terms of the security regime goal, very successful Container Security Initiative led by Commissioner Bonner. I'm sure you're going to have a few words on that, momentarily.

Our collective efforts to increase—in the third area—increase our operational presence in our ports and coastal zones focuses not only on adding more people, boats, and ships to our security effort, but making the employment of those resources more effective through the application of technology, information sharing, and intelligence support.

Several examples. Customs and Border Protection is employing nonintrusive inspection technology to screen shipments. Coast Guard is aggressively enforcing and exercising domestic and international security standards, equipping helicopters with airborne use-of-force capability and vertical insertion capability, adding boats and patrol cutters, and developing special safety and security teams to secure our ports, waterways, and/or vessels in the face of increasing risk. TSA, in coordination with the Coast Guard, is working with cruise-line operators to identify technology solutions for screening passengers and their belongings.

We are also aggressively working to improve our response capability and readiness to respond to security incidents that do occur in the over 26,000 miles of navigable waterways and over 361 ports. We will soon deploy the first segments of our Rescue 21, the Coast Guard's maritime 9/11 command, control, and communications system. We've also worked, within the Department and through the Department, to refine our Nation's emergency response plans and incident management systems. These will materially improve our overall response efforts. I know my colleagues this morning will add more descriptors on some of these action items that populate our overall strategy.

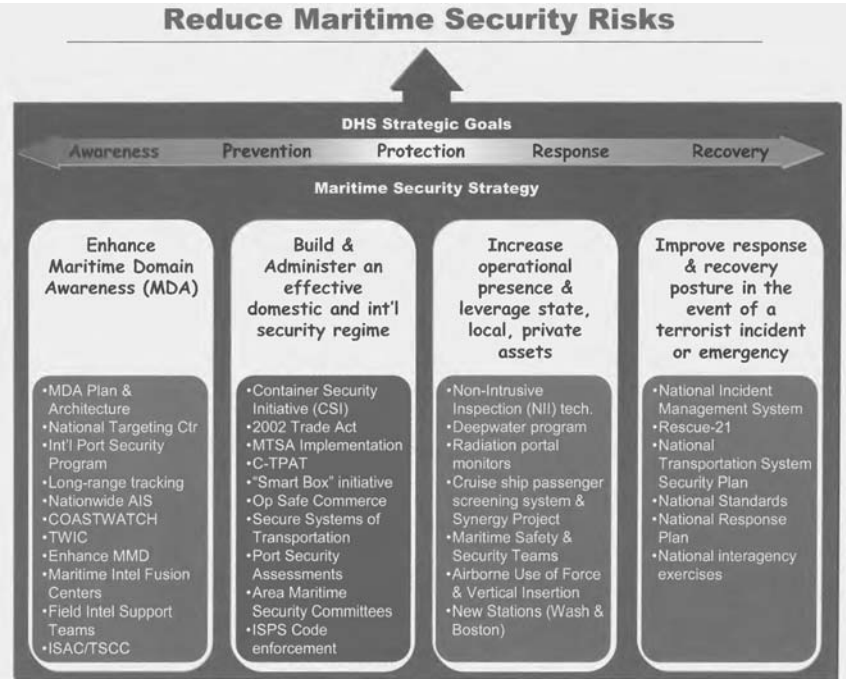
I should note that an essential feature of the overall Department's security strategy is pursuit of a layered defense approach, one that has been alluded to by the distinguished Members of this Committee this morning, but one that seeks to reach beyond our

borders, in partnership with other agencies and nations, to mitigate risk of the homeland.

Please, the next graphic.

I think this is a pretty good graphic that depicts how these various initiatives fold into a reaching-out type of approach well beyond our ports. You can see that there are a number of these initiatives, sorted by—geographically, if you will, in terms of a layered perspective that extends from our ports through coastal approaches, through open ocean, all the way to foreign ports. This is a comprehensive approach to deal with truly a global security challenge, because it is a global system that we're dealing with.

[The graphic referred to follows:]



Coast Guard's efforts for the Deepwater system is part of this layered defense. Senator Snowe mentioned that earlier in her comments. It is very, very important for us to have the presence, the operational presence, and the MDA, the maritime domain awareness, through this layered defense in the maritime. Indispensable for us to develop a network-centered approach to our systems, and that's what it's all about. It's a major priority within our budget.

You can see, Mr. Chairman, that we—the Department has a very full range of, I think, well thought-out and coordinated initiatives that will increasingly, as we work on all of these items, increasingly secure our Nation's ports, waterways, and infrastructure. These three agencies that are sitting here are committed to these efforts, committed to working together and develop many interagency working groups that are addressing things like cargo security standards, port security assessment, international port security assessment, and the development of associated plans in a fam-

ily-of-plans construct. We're under one roof now. We have great, intensive communication and cooperation amongst us, and I think there are a lot of great things we've done, and more coming.

Thank you for your attention, Mr. Chairman. I'll be glad to answer any questions at the appropriate time.

The CHAIRMAN. Thank you, Admiral.

Commissioner Bonner, welcome.

STATEMENT OF HON. ROBERT C. BONNER, COMMISSIONER, U.S. CUSTOMS AND BORDER PROTECTION

Mr. BONNER. Yes, thank you, Mr. Chairman and Senator Hollings and Members of the Committee. I want to thank you for this opportunity to testify regarding maritime and port security, and the progress that U.S. Customs and Border Protection has made since we last discussed this, back in September. I'm particularly pleased to be here with my colleagues, Admiral Collins and Admiral Stone.

I think I can report to this Committee that, with much of our government's terrorist prevention capabilities now under one roof—that is to say, within one department of government—and that department under the great leadership of Secretary Ridge, our country is better able to deal with the terrorist threat than we were before the Department of Homeland Security was created.

There are—three of the principal operational agencies of the Department are represented by the three of us that are sitting at this table before you. Customs and Border Protection is one of those operational agencies of the Department of Homeland Security that was created just a little over a year ago by essentially merging four different entities or agencies from three different departments and putting them into one agency, one agency for our borders.

The priority mission of our agency, of Customs and Border Protection, as a unified border agency, is nothing less than detecting and preventing terrorists and terrorist weapons from entering our country. That is, as we've discussed, we have twin goals here. One is to secure America's borders, to be sure; but to do it in a way that does not stifle the flow of legitimate trade, commerce, and people.

And those goals don't have to be mutually exclusive. We can, and we are, accomplishing them through the use of and obtaining advance information, through risk-targeting systems, through detection technologies, and by extended border strategies, like the Container Security Initiative.

In the maritime environment, we are, of course, concerned that cargo coming into our seaports could be exploited by al Qaeda, and al Qaeda-associated terrorist organizations. And clearly this is something of great concern to us and the Administration.

The use of containers to smuggle terrorists or terrorist weapons is, of course, by no means farfetched. Just last week, as reported in the Israeli newspapers, two Palestinian extremists detonated two suicide bombs in the Israeli port of Ashdod, killing 10 people and wounding 18 others. And, at first, the security officers in Israel were at a loss to explain how these suicide bombers were able to get into the port area, because they had. It now looks as though they infiltrated the port by concealing themselves in a cargo container.

This attack highlights two significant lessons on port security, it seems to me. The first one is the threat to our ports lies outside, and it lies in having unknown, essentially never before seen shipments arrive at our U.S. seaports. And it also is the lesson that we should conduct security screenings and inspections of high risk cargo at the earliest opportunity, before these cargo shipments and these containers arrive at U.S. seaports.

As the border agency for our country, Customs and Border Protection has a great responsibility, because every one of the eight to nine million sea cargo containers that arrive at our seaports annually have to be presented to and cleared through U.S. Customs and Border Protection. And CBP has the authority to search any and every container without cause or suspicion. Moreover, Customs and Border Protection could deny a carrier permission to unload or unload a container at U.S. seaports. And based upon that authority, has authority, essentially, to order no-load orders at foreign ports to prevent high risk or unknown cargo from being loaded onboard overseas onto a ship headed for the United States. And I can assure you and this Committee that Customs and Border Protection—by the way, I have used the no-load authority, and certainly would use it if there were any specific intelligence about any container anyplace in the world that was headed for the United States. And we've used that authority also to gain compliance with our 24-hour rule requirements.

Let me just say a couple of other things, and then I'll conclude, about our efforts.

One is the Container Security Initiative, which was mentioned by Senator Snowe. Customs and Border Protection is targeting and, with our foreign counterparts, screening targeted containers, those that pose a potential risk for concealment of terrorist weapons before they're loaded onboard vessels destined for the United States.

And I've just put up a chart here on the board which indicates that, to date, foreign nations representing 38 foreign seaports that ship directly to the United States have agreed to participate in the Container Security Initiative. And teams of Customs and Border Protection inspectors and targeters have been already deployed to 18 foreign seaports to target and screen containers destined for the United States for potential terrorist weapons.

By the end of 2004, I expect to have CBP officers operating in over 30, or perhaps as many as 32, foreign seaports. Now, these are hubs, strategic megaports that ship 80 percent or more of all containers to the United States, and through which containers originating in high-risk countries of North Africa, the Middle East, and South Asia ship and pass through or transship their containers.

The other initiative has been—that I want to mention is the Customs Trade Partnership Against Terrorism. The Chairman, Senator McCain, raised that. CBP has partnered, as you know, Mr. Chairman, with the private sector, with the trade community, to implement security standards and best practices that protect the entire supply chain against exploitation from terrorists, literally from the foreign manufacturers' loading docks to our ports of entry. And there are over 5,900 companies, C–TPAT members, that have joined C–TPAT, including many, many major U.S. importers. In

fact, U.S. importers, alone, represent 40 percent of all of the cargo that's shipped to the United States.

So they've agreed to implement security standards. And it's not just a matter of saying they're going to implement them. We are now rolling out, at Customs and Border Protection, supply chain security specialists, who literally are validating that the promises and commitments of C–TPAT members and their foreign vendors have been complied with.

And through C–TPAT, we continue to ask more from our partners, and continue to raise the bar. In January of this year, for example, five C–TPAT partners—these are major U.S. importers—agreed to enhance their supply chain security by using smart containers with an electronic container-security device that lets Customs and Border Protection inspectors know if that container has been tampered with. We'll continue to work with our partners, with TSA, with the Coast Guard, with the Department, and the Border and Transportation Security Directorate of the Department with respect to the question of how and whether to apply the smart box beyond C–TPAT, and what the standard should be.

In addition, by the way, we've done a lot at our own U.S. seaports—I know Senator Hollings knows this—in terms of deployment of large-scale X-ray imaging equipment. We've gone from—throughout the country, at our ports of entry, from 45 on 9/11; we now have 145 of the large, whole-container X-ray screening equipments at our ports of entry. This includes our land borders, as well as our seaports.

We have deployed, very quickly, radiological and nuclear detection equipment. We've acquired and deployed over 9,500 personal radiation detectors. And, Senator Snowe, you're right, every CBP inspector on the front line is equipped with, trained, and wears a personal radiation detector device.

We have deployed 325 radiation isotope identifiers to our ports of entry, and trained people to use them. These identify the nature of the material that's being—emitting radiation, whether it's U–235 or whether it's an innocent source. And we've deployed over 248 radiation portal monitors, highly sensitive portal monitors, including, by the way, not just at the northern border now, but for our first seaport, which is the Port of New York/New Jersey, that we deployed. Actually, just a couple of days ago I announced that we had deployed, as an additional layer, these sophisticated detection devices.

Let me just conclude, Mr. Chairman, by saying we have made some great strides. Clearly, we have a ways to go here, but we've made some great strides, and I appreciate the opportunity to point out a few of those to this Committee. Pleased to answer any questions after my colleague here, Admiral Stone, makes his statement.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Commissioner.

Admiral Stone?

STATEMENT OF REAR ADMIRAL DAVID M. STONE, ACTING ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION

Admiral STONE. Well, thank you, Mr. Chairman.

Mr. Chairman, Senator Hollings, and distinguished Members of the Committee, it is an honor to appear on behalf of TSA this morning to discuss maritime security. And I sincerely apologize for my late arrival.

As my colleagues have stated, Department of Homeland Security agencies are working closely together to maximize government resources, ensure consistency among agency initiatives and programs, and avoid potential overlap in carrying out our maritime security mission.

The Coast Guard, as the lead Federal agent for maritime security, has been tasked with developing the Maritime Transportation Security Plan. The Transportation Security Administration and U.S. Customs and Border Protection are assisting the Coast Guard in the development of this plan, which will be a component of the National Transportation System, Security Plan, and a subset of the larger National Critical Infrastructure Protection Plan.

TSA has developed a Web-based, no-cost maritime vulnerability self-assessment tool that is assisting port, vessel, and facility owners in completing vulnerability assessments required by the Maritime Transportation Security Act. TSA has implemented a synergy project designed to examine the feasibility of implementing a cost-effective, functional, and secure system to screen and transfer passenger baggage from seaport to airport, and reduce congestion at airport security checkpoints caused by the influx of large numbers of passengers disembarking from cruise ships. We are currently testing this program in Miami.

TSA will soon begin the prototype phase of the transportation worker identification credential. The prototype will test the feasibility of bringing greater uniformity to procedures for granting access to those who work in the most sensitive and secure areas of our national transportation system.

TSA personnel are also assisting the Coast Guard in developing the policies and procedures that will be used for their international port security program, and, to that end, have provided the Coast Guard with examples and lessons learned from the Foreign Airport Audit Program.

Key TSA Federal security directors from around the country, as well as headquarters, serve on the Coast Guard Area Maritime Security Advisory Committees. Working together under the leadership of the Border and Transportation Security Directorate, we are developing a more comprehensive framework for securing the maritime cargo supply chain. This initiative will also assist in meeting Maritime Transportation Security Act requirements for secure systems of transportation, emphasizing the intermodal aspects of maritime cargo transportation.

We are reviewing cargo programs, analytical tools, and other relevant resources in order to identify remaining supply chain vulnerabilities. The Department expects that the results of Operation Safe Commerce will also help shape this framework.

In closing, I would like to thank you, Mr. Chairman, for your strong support, and that of the Committee Members, and I look forward to answering your questions.

[The joint prepared statement of Admiral Collins, Mr. Bonner, and Admiral Stone follows:]

PREPARED STATEMENT OF ADMIRAL THOMAS H. COLLINS, COMMANDANT, U.S. COAST GUARD; ROBERT C. BONNER, COMMISSIONER, CUSTOMS AND BORDER PROTECTION, ADMIRAL DAVID M. STONE, ACTING ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION, DEPARTMENT OF HOMELAND SECURITY

Good morning, Mr. Chairman and distinguished Members of the Committee. It is our pleasure to be here today to update you on the Department's efforts to enhance maritime security, the impact of those efforts on maritime commerce, and the additional measures that may be needed to further enhance maritime transportation security.

Prior to the attacks of September 11, 2001, the primary focus within the maritime domain had been on safety, the environment, and vessel traffic management. Most national and international efforts revolved around the safe and efficient movement of waterborne commerce the interdiction of narcotics and illegal migrant, and trade compliance. However, after September 11, 2001, we have acted upon the realization that the maritime sector is one of the most valuable and vulnerable components of our national transportation system. The challenge is significant:

- Over 95 percent of overseas trade enters through U.S. seaports;
- Our seaports account for 2 billion tons and $800 billion of domestic and international freight each year;
- Each year approximately 9 million sea containers enter the U.S. via our seaports;
- 26,000 miles of commercially navigable waterways serving 361 U.S. ports;
- Seaborne shipment of approximately 3.3 billion barrels of oil each year;
- 6 million cruise ship passengers travel each year from U.S. ports;
- Ferry systems transport 180 million passengers annually;
- Waterways support 110,000 commercial fishing vessels, contributing $111 billion to state economies;
- 78 million Americans engaged in recreational boating;
- Some 8,100 foreign vessels making 50,000 U.S. port calls each year; and
- Domestic and international trade is expected to double in next 20 years.

While this Committee certainly needs no reminder, it is plainly evident that a terrorist incident against our marine transportation system would have a disastrous impact on global shipping, international trade, and the world economy in addition to the strategic military value of many ports and waterways.

The world's oceans are global thoroughfares. A cooperative international approach involving partnerships of nations, navies, coast guards, law enforcement agencies, and commercial shipping interests is essential—with all parties acting collaboratively to confront broadly defined threats to our common and interdependent maritime security. The Department of Homeland Security (DHS) recently marked its first anniversary and we are happy to report that operating with other Federal agencies sharing a common DHS mission perspective provides new benefits to our Nation's security daily.

We are committed to working with our partner agencies as one team engaged in one fight, and truly believe having one Department responsible for homeland security has made America more secure today. Events in Haiti over the past several weeks provide a recent example of the leaps forward we are taking with regard to interagency cooperation. Under the direction of the Secretary of Homeland Security, the Homeland Security Task Force Southeast was stood-up as part of OPERATION ABLE SENTRY. The Coast Guard (CG) led task force was comprised of many agencies chartered to plan, prepare, and conduct migrant interdiction operations in the vicinity of Haiti due to the escalation of violence in that country and the threat of a mass exodus of undocumented migrants. Within the first days of interdiction operations, the task force demonstrated impressive agility and synergy:

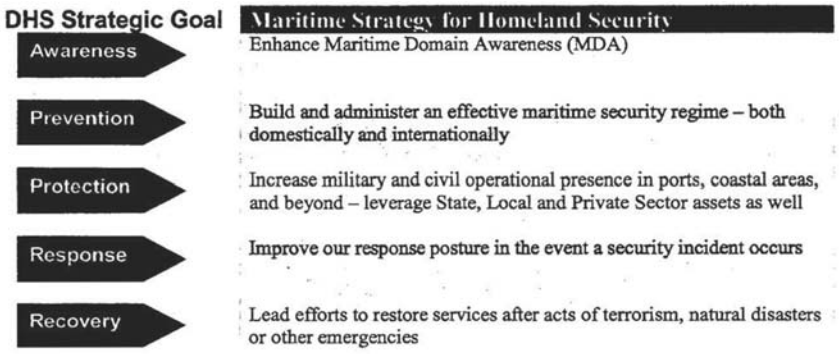
- CG cutters, with Citizenship and Immigration Service (CIS) asylum pre-screening officers and interpreters aboard, interdicted 18 Haitian vessels with 1,076 undocumented migrants;
- CG and Immigration and Customs Enforcement (ICE) aircraft patrolled the skies throughout the operating area; and CG, ICE, and Customs and Border Protection (CBP) conducted coordinated patrols off the Florida coast;
- CG and ICE conducted a coordinated boarding of a boat suspected of being hijacked off the coast of Miami; and

- Federal Emergency Management Agency (FEMA) also deployed three Information and Planning Specialists to the task force in support of contingency planning.

With our Federal Government's Awareness, Prevention, Protection, Response and Recovery capabilities now under one roof, in one department, the level of communication and cooperation among the sister agencies of CG, TSA, ICE and CBP is stronger than ever. CBP, TSA and CG are working together to support efforts to implement the Maritime Transportation Security Act (MTSA) through interagency working groups addressing cargo security standards, port security assessments, international port security and the development of the National Maritime Security Plan.

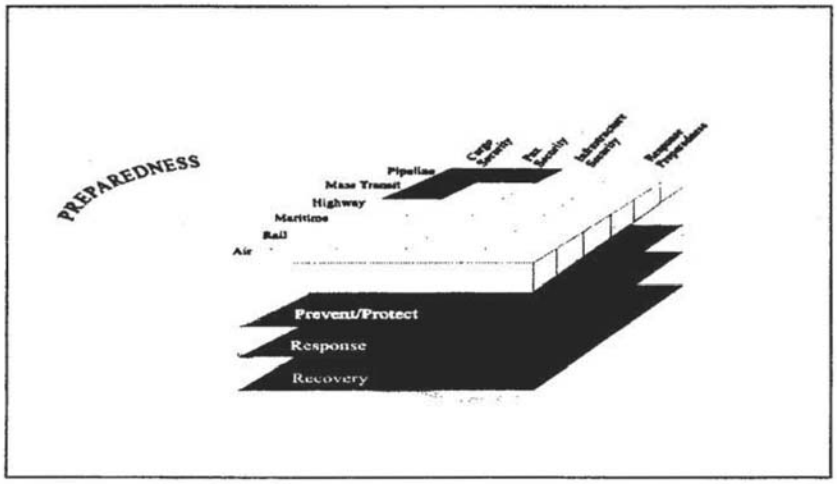
Maritime Strategy for Homeland Security

Since 9/11, Secretary Ridge and all DHS components have worked hard to achieve DHS's strategic goals of Awareness, Prevention, Protection, Response and Recovery. These strategy elements guide all that we do and likewise represent key pillars of the maritime homeland security strategy:



Given its unique blend of authorities, capabilities, competencies and partnerships (domestic and international), the CG has been charged with taking the lead on the development and implementation of a comprehensive Maritime Strategy for Homeland Security. The CG's *Maritime Strategy for Homeland Security* supports both the President's *National Security Strategy of the United States of America* and the *National Strategy for Homeland Security* and is responsive to near-term needs while maintaining a strategic outlook on the threats and opportunities of the future. The maritime strategy is built upon a layered defense; a time-proven means to enhance security in U.S. ports and waterways while concurrently facilitating the smooth flow of commerce. The collective result of our efforts is aimed at managing and reducing maritime security risks.

DHS is developing a National Transportation System Security Plan (NTSSP), designed to provide overall operational planning guidance on transportation security. The Transportation Security Administration (TSA), working with the Department of Transportation (DOT) and other Federal agencies, is coordinating the DRS's efforts on this initiative. The goals of the NTSSP are to reduce the risk of terrorism to the Nation's critical transportation infrastructure and operations and the people who use them. It will ensure that modal security plans are integrated into an effective concept of operations for management of the transportation sector's security and minimize the catastrophic consequences of any successful terrorist act. The NTSSP will be consistent with the Information Analysis and Infrastructure Protection (IAIP) Directorate's Critical Infrastructure Protection Plan. As the lead agency for maritime security, the CG is responsible for developing the National Maritime Transportation Security Plan (NMTSP), which will harmonize with the NTSSP and critical infrastructure protection plans and support our maritime strategy.



Below is an update on the Department's recent accomplishments in pursuit of each element of the maritime strategy with a particular focus on the joint and individual efforts of the CG, TSA and CBP.

Awareness—Enhance Maritime Domain Awareness (MDA)

The core of our MDA efforts revolve around the development and employment of accurate information, intelligence, and targeting of vessels, cargo, crews and passengers—and extending this well beyond our traditional maritime boundaries. All DHS components are working hard to effectively provide a layered defense through collaborative efforts with our international partners to counter and manage security risks long before they reach a U.S. port—when effectively deploying countermeasures becomes more difficult.

The goal is to know the difference between friend and foe, so that legitimate commerce can move through our coastal and port areas unimpeded while we interdict contraband cargo and illegal activities of all types at sea before it becomes a threat on our shores. The key to achieving this comprehensive domain awareness is our ability as a department to obtain, synthesize and analyze the context around the movement of goods and people. We are taking an interagency approach, leveraging information technology, multiple information sources and actively involving of the private sector. Our ability to achieve better MDA will allow us to better focus our protection and response efforts on those trade transactions, individuals, and activities of interest. A synopsis of our collective efforts is provided below:

- The CG is leading the interagency and joint Service effort to develop a comprehensive national MDA plan and system architecture.
- As directed by MTSA, the CG established an International Port Security Program (IPSP) that is currently working in concert with CBP, TSA and other Federal agencies to identify foreign ports identified by the Secretary as posing a potential security risk to international maritime transportation. TSA and CBP have provided extensive assistance in developing this program by sharing lessons learned and best practices from TSA's Civil Aviation Security Liaison Officer (CASLO) program and CBP's Container Security Initiative. The IPSP will begin visiting selected foreign ports in July 2004 to measure the degree of rigor with which foreign countries are administering the International Maritime Organization's (IMO) International Ship & Port Facility Security Code (ISPS).
- The CG is researching technologies and systems that are able to track vessels entering, departing or transiting U.S. waters and track vessels bound for the U.S. from overseas locations. The CG is currently working with IMO to develop functional and technical requirements for long-range tracking out to 2,000 nautical miles (approximate distance from shore a vessel owner must transmit their 96-hour notice of arrival, based on typical speed of advance). The U.S. will discuss and attempt to forward an amendment that has been proposed to IMO for this initiative in committee meetings over the next two months.

- The CG is establishing a network for receiving and distributing Automatic Identification System (AIS) reports (position, course, speed, cargo, etc.) from ships using existing Vessel Traffic Services in nine of our Nation's ports, waterways, and coastal areas. This initiative will progress to the other strategically significant U.S. seaports, and ultimately extend to nationwide coverage.
- The CG Intelligence Coordination Center, co-located with the Office of Naval Intelligence at the National Maritime Intelligence Center in Suitland, Maryland, established COASTWATCH. Through this process, notice of arrival reports from the National Vessel Movement Center are analyzed using law enforcement and intelligence information and vessels of interest are identified so that Coast Guard and other agencies can appropriately respond to board those vessels before they reach port, if necessary. The Coast Guard and CBP have exchanged personnel to enhance data sharing between the CG Intelligence Coordination Center's COASTWATCH (which gathers and analyzes information on ship notice of arrival reports on vessels, people, and certain dangerous cargoes approaching U.S. ports) and CBP's National Targeting Center (cargo tracking) process.
- CBP's National Targeting Center (NTC) is a 24x7 operation that supports the enforcement and regulatory missions of various agencies through a network of liaisons, which includes the TSA, CG, Department of Energy, and members of the intelligence community. CBP Officers and Field Analysis Specialists that are experts in passenger and cargo targeting for air, sea. and land operations in the inbound and outbound environments primarily staff NTC. The NTC staff develops tactical targets from raw intelligence in support of the CBP mission to detect and prevent terrorists and terrorist weapons from entering the United States. NTC also supports CBP field elements, including Container Security Initiative personnel stationed in countries throughout the world, with additional research assets for passenger and cargo examinations. NTC personnel are also currently engaged in the support of intradepartmental and interagency anti-terrorist operations, while simultaneously providing support to CBP targeting programs, policies, and initiatives. One example of CBP's commitment to collaborative targeting efforts is the Food and Drug Administration Prior Notice Center located at the NTC and operational since December 11, 2003. There, CBP and Food and Drug Administration personnel conduct joint targeting on a round the clock basis in support of the Bio-Terrorism Act.
- CBP is conducting national targeting and using automated targeting tools to screen advance information and other data to identify high-risk shipments. As a key component of the DHS maritime security strategy, CBP's Automated Targeting System (ATS) serves as the premier tool for performing transactional risk assessments and evaluating potential national security risks posed by sea. air, truck, and rail cargo.
- CG is using a risk management system to identify High Interest Vessels for follow-up security hoardings and when necessary, due to risk, vessel escorts and positive control hoardings to ensure the safety of vessels during their transit into U.S. ports.
- In partnership with the Chief of Naval Operations (CNO), the CG is establishing interagency prototype joint harbor operations centers in select Navy homeports improving both port security and force protection capabilities. Such prototypes have already been completed in San Diego, California and Hampton Roads, Virginia.
- TSA will soon begin the prototype phase in developing the Transportation Worker Identification Credential (TWIC), aimed at mitigating the threat of attacks to the national transportation infrastructure. The TWIC prototype and supporting measures will test the feasibility of bringing uniformity and consistency to the process of granting access to transportation workers entrusted to work in the most sensitive and secure areas of our national transportation system. The President's FY 2005 request includes spending authority to begin implementing the TWIC concept within parameters that will be defined by the Administration after completion of the prototype assessment.
- Complementing the TWIC, the CG will continue aggressive implementation of a Merchant Mariner Documentation (MMD) Task Force plan, which ensures positive identity of merchant mariners sailing on U.S. flag vessels and performs appropriate security/background screening. In 2004, the CG will provide for additional personnel support at Regional Examination Centers, centralized security screening and electronic fingerprinting capability.

- The CG has established additional Maritime Intelligence Fusion Centers on the east and west coasts for both military intelligence and law enforcement sensitive information. In addition, the CG established subordinate Field Intelligence Support Teams (FISTs) in key ports. These teams are actively engaged in Intel collection and first order analysis in coordination with federal, state, and local enforcement and Intel agencies. They are "joint" in the broadest sense providing a critical top-down and bottom-up information and intelligence.

Aside from the important initiatives above, we are seeing consistent and steady improvements in our ability to integrate and correlate information in the field such that we can effectively respond. For example, on March 13, 2004 the Coast Guard Pacific Area Maritime Intelligence Fusion Center advised CG Marine Safety Office (MSO)/Group Los Angeles/Long Beach that a 728-foot foreign flagged motor vessel with a cargo of crude oil was due into Los Angeles but failed to properly file an Advance Notice of Arrival. The MSO/Group responded and conducted a positive control boarding alongside ICE personnel while the vessel was at anchor. The crew was detained onboard due to improper visas. While we have much more work to do, our maritime domain awareness is improving every day.

Prevention—Create and Oversee Maritime Security Regime

This element of our strategy focuses on both domestic and international efforts and includes initiatives related to MTSA implementation, IMO regulations such as the ISPS Code, as well as improving supply chain security and identity security processes. Recent accomplishments and future plans include:

- CBP is expanding the Container Security Initiative (CSI). This is an effort by CBP to secure ocean-borne container traffic by placing CBP officials alongside host government Customs officers to ensure that potentially high-risk shipments are identified and inspected at foreign ports before they are placed on vessels destined for the United States. This program will be expanded to 14 additional foreign ports based on volume, location and strategic concerns, which will bring the total number of operational CSI ports to 31. Once implemented, nearly 80 percent of all cargo containers headed for the United States will be prescreened before they depart from abroad.
- In December 2003, DHS promulgated final regulations implementing the Trade Act of 2002, requiring advance, electronic manifest information for all modes of transportation. This information will augment that received and analyzed already at the National Targeting Center.
  - For vessel operations CBP is receiving complete cargo declaration information for all container vessels and non-approved break bulk shipments 24-hours prior to loading the vessel at the foreign port. With the implementation of the Trade Act, CBP now requires this cargo information in an electronic format via the Sea Automated Manifest System (AMS). On March 4, 2004 all container vessels must submit their cargo declaration information to CBP electronically.
  - The Trade Act also provides for all modes of transportation, inbound and outbound, to require cargo information electronically and in advance of arrival. On May 13, 2004 programming changes will be completed for the Air AMS application and a schedule for training and implementation was published in the Federal Register on March 1, 2004.
  - The outbound cargo electronic information is awaiting the publication of the Bureau of the Census final regulations before implementation can begin. The regulations are expected to become effective in late 2004 or early 2005. For the outbound portion of the Trade Act, a rolling implementation is not being considered. CBP is developing implementation guidelines that are being coordinated with outreach to the trade community.
- As a direct and immediate response to the terrorist events of 9/11, CBP challenged the trade community to cooperatively design a new approach to supply chain security that would strengthen U.S. borders against acts of terrorism while continuing to facilitate the legitimate flow of compliant cargo, conveyances and persons. The result was an innovative government/private sector partnership program—the Customs-Trade Partnership Against Terrorism (C–TPAT). C–TPAT is a cooperative endeavor covering all sectors of the international supply chain. The program calls upon the trade community to systematically establish procedures to enhance their existing security practices and those of their business partners involved in their supply chains. Currently, over

5,900 members of the international community have demonstrated their commitment to security by partnering with CBP through the C–TPAT program.

- DHS, DOT and the Department of Justice are working with business interests, the largest U.S. container load centers and the maritime industry to implement Operation Safe Commerce (OSC), an effort to develop and share best practices for the safe and expeditious movement of containerized cargo. The goal of OSC is to serve as a test bed to examine methods to increase end-to-end supply chain security, protect the global supply chain, and facilitate the flow of commerce.
- Under a BTS-led effort, TSA along with CBP and the CG are developing a more comprehensive framework for securing the maritime cargo supply chain. This initiative will also assist in meeting MTSA requirements for "Secure Systems of Transportation (SST)," by incorporating a systems-based approach to cargo transportation (*i.e.,* point of origin to point of destination). Agencies are reviewing cargo programs, analytic tools, and other relevant resources within the department in order to identify remaining supply chain vulnerabilities. The Department expects that the results of Operation Safe Commerce will also help shape this framework.
- Another part of this BTS-lead effort is CBP's recent partnership with five C–TPAT importers to initiative the development of improved security standards and performance criteria for the future maritime container—or "Smart Box". The Smart Box being tested through C–TPAT consists of the application and activation of an electronic Container Security Device (CSD), as well as the application of a mechanical seal meeting the ISO 17712 high security bolt seal standards. To date, approximately 215 containers meeting the criteria have been imported into the U.S. from various trade lanes. This first phase of the Smart Box initiative is designed to collect and analyze data relative to the performance of the technology being utilized and to help the Department develop more rigorous container security as part of meeting MTSA "Secure Systems of Transportation". Other efforts through TSA, the Science and Technology Directorate and Operation Safe commerce will also inform this process, which will result in the development of specific performance standards for cargo containers.
- The CG established Area Maritime Security Committees (AMSC), which assist in the development of Area Maritime Security Plans nationwide, as required by the MTSA. AMSCs will enhance maritime situational awareness and ensure integrated maritime prevention and response operations among the entire maritime community. CBP and TSA have designated representatives assigned to the Area Maritime Security Committees to assist CG Captains of the Port in addressing cargo security issues.
- The CG has completed Port Security Assessments (PSA) at 16 of the 55 most significant military and economic ports in the U.S. and will complete the assessments of all 55 strategic ports by the end of calendar year 2004.
- Final CG MTSA implementation Rules, drafted in cooperation with TSA, CBP and the Maritime Administration (MARAD), were published in October 2003 and security plans from approximately 9,500 vessels and 3,500 facilities were due on December 31, 2003. To date, approximately 97 percent have been received. The CG will continue to aggressively pursue 100 percent compliance, and has instituted a phased implementation of penalties to ensure that all regulated facilities have implemented approved security plans by the July 1, 2004 deadline.
- The Coast Guard is actively involved with MARAD in the development of maritime security competency standards and security training curricula under Section 109 of MTSA.
- The CG has met with nearly 60 countries representing the vast majority of all shippers to the U.S., reinforcing a commitment to the ISPS code. For vessels subject to MTSA, the Safety of Life at Sea (SOLAS) amendments and the ISPS Code, the CG is implementing strong Port State Control measures to aggressively ensure foreign vessels have approved plans and have implemented adequate security standards. The measures include tracking performance of all owners, operators, flag administrations, recognized security organizations, charterers, and port facilities. Noncompliance will subject the vessel to a range of control measures, which could include denial of entry into port or significant delay. This aggressive Port State Control regime will be coupled with the CG's inter-agency IPSP, comprised of representatives from the Department of State, Department of Defense, CBP, TSA, and MARAD, that will assess both the effec-

tiveness of anti-terrorism measures in foreign ports and the foreign flag administration's implementation of the SOLAS amendments and the ISPS Code.

Protection—Increase Operational Presence/Enhance Deterrence

Our collective efforts to increase operational presence in ports and coastal zones will continue to build upon the layered security posture established by the maritime security strategy. These efforts focus not only on adding more people, boats and ships to force structures but making the employment of those resources more effective through the application of technology, information sharing and intelligence support. Recent accomplishments and future plans include:

- CG's Deepwater Program: A multi-year, performance-based acquisition that will replace or modernize 90 Coast Guard cutters, 200 fixed wing aircraft and multimission helicopters and the communications equipment, sensors, and logistics systems required to maintain and operate them. Deepwater will greatly improve the Coast Guard's maritime presence starting at America's ports, waterways, and coasts and extending seaward to *wherever* the Coast Guard needs to be present or to take appropriate maritime action. Deepwater provides the capability to identify, interdict, board, and where warranted seize vessels or people engaged in illegal/terrorist activity at sea or on the ports, waterways, or coast of America. In FY04, the Deepwater Program:
  - Commences urgent re-engining of Coast Guard's fleet of short-range helicopters to ensure safe and reliable operations;
  - Accelerates the development of the Fast Response Cutter;
  - Begins construction of the first National Security Cutter (frigate-size vessel about 425 feet long);
  - Acquires an additional Maritime Patrol Aircraft (MPA);
  - Completes design and shipboard integration of Vertical Unmanned Aerial Vehicles (VUAV);
  - Commences conceptual development of the Offshore Patrol Cutter; and Delivers 4 Short Range Prosecutors (cutter small boats) for use on the 123' Patrol Boat.
- CBP is employing Non-Intrusive Inspection (NII) technology to screen shipments rapidly for anomalies. Deploying NII technology to our land borders and seaports has increased CBP's ability to detect conventional explosives, nuclear, weapons, and other terrorist weapons. N1I equipment includes large scale X-ray or gamma-ray imaging systems, portal radiation monitors, and a mixture of portable and handheld technologies to include personal radiation detection devices that greatly reduce the need for costly, time-consuming physical inspection of containers and vehicles.
- DHS's priority undertaking is preventing weapons of mass destruction from entering this country. The DHS goal is to screen 100 percent of all arriving containers, trucks, trains, cars, mailbags and express consignment packages with radiation detection equipment. To achieve this goal, CBP has developed a comprehensive risk management strategy for the deployment of radiation portal monitors (RPM) throughout the country.
- As of March 16, 2004, two hundred forty-seven RPMs have been deployed. The vast majority of the deployed RPMs are at International Mail Branches, Express Consignment Courier facilities and along major Northern Border ports of entry. Presently, CBP has begun deployment to our seaports. CBP has also deployed a large number of handheld radiation detection technologies. Currently, CBP has 321 radiation isotope identifier devices and over 9,418 personal radiation detectors to the field.
- Prior to the attacks of 9/11, the CG had committed less than 2 percent of its assets to active port security duty. Immediately after 9/11, the CG surged nearly 60 percent of its assets in immediate support of port security. Since then, the CG has rebalanced asset deployments to provide roughly 28 percent of its assets in coverage of port security—a significant and steady increase in operational presence.
- CG Maritime Safety & Security Teams (MSSTs) provide immediately deployable multiple boat, law enforcement capability that can be sustained over an extended period. Teams are equipped to deploy (via land or air) to any location within 12 hours of notification. To date, eight of thirteen MSSTs have been commissioned and the remainder will be operational by the end of CY 2004.

- CG is equipping helicopters with Airborne Use of Force (AUF) and Vertical Insertion (VI) capability. This will enhance the Coast Guard's ability to secure our oceans, ports, waterways, and coastal areas against illegal drug, migrant, and terrorist activity by providing capability to fire warning shots and disabling fire and rapidly/covertly deploying boarding teams aboard vessels at sea. The Coast Guard currently has 8-armed MH–68 helicopters operating out of Jacksonville, FL and will equip four HH–60J armed helicopters by April 2004.
- TSA in coordination with the CG is working with cruise line operators to identify technology solutions for screening passengers and their belongings for potential threats. TSA is also developing methods for inspecting passengers and vehicles utilizing established ferry transportation systems. Detection technologies and methods must be able to find threats without unduly impacting the flow of passengers and/or vehicles.
- TSA has implemented a Synergy Project designed to create a cost effective, functional, and secure system to screen and transfer passenger baggage from a seaport to an airport, thereby reducing the congestion at airport security checkpoints caused by the influx of large numbers of passengers disembarking from cruise ships. This program is currently underway at the Ports of Miami and Vancouver.
- Responding to threat assessments in and in support of the Maritime Homeland Security Strategy, CG Stations Boston and Washington, D.C. were created in Fiscal Year 2004.

Response and Recovery—Improve Response and Recovery Posture

Understanding the challenge of defending 26,000 miles of navigable waterways and 361 ports against every conceivable threat at every possible time, we are also aggressively working to improve our response capabilities and readiness. While the above increases in operational presence necessarily augment our collective response posture, additional accomplishments and future plans include:

- The Secretary announced on March 1, 2004 the approval of the National Incident Management System (NIMS). It is the Nation's first standardized management approach that will provide a consistent nationwide template to enable federal, state, local, and tribal governments as well as private sector organizations to work together effectively to prepare for, prevent, respond to, and recover from a terrorist attack or other major disaster. NIMS will ensure that all of our Nation's responders are working in support of "one plan, one team, one fight." For the first time, there will be standardized procedures for responding to emergencies across the Nation. A NIMS Integration Center will also be established to identify and share best practices on preparedness with state and local authorities, provide consistent training to first responders across the country, and conduct exercises involving many different localities.
- Continue deployment of Rescue 21—the CG's maritime 911 command, control and communications system in our ports, waterways, and coastal areas. Nationwide implementation continues during 2004. This system provides Federal, state and local first responders with interoperable maritime communications capability, greater area coverage, enhanced system reliability, voice recorder replay functionality, and direction finding capability. Rescue 21 represents a quantum leap forward communications technology.
- TSA is coordinating with CG, CBP, MARAD and other DOT modal administrations on setting national standards and policies for transportation security and is working with these agencies and the Office of Domestic Preparedness to coordinate the recovery of the transportation system in the event of a transportation security incident. For example, TSA is working with MARAD to study the impacts and lessons learned from the recent four-day closing of the Mississippi River caused when a barge sank from hitting the Greenville Bridge linking Mississippi and Arkansas.
- DHS agencies routinely lead or participate in national intermodal terrorism exercises, such as Operation Heartland, United Defense and TOPOFF2, designed to enhance our ability to prevent, mitigate, and respond to potential transportation security incidents.

DHS's response and recovery organization will be tested and further strengthened at the upcoming "California Spill of National Significance 2004" exercise (CAL SONS 04), scheduled for April 20–24. CAL SONS 04 is a CG-sponsored full-scale national exercise that will pose two major marine incidents off the coast of Southern California and require a coordinated response by local, State and Federal agencies, the government of Mexico, industry partners and volunteer organizations. CAL

SONS 04 will be guided by the Initial National Response Plan and National Oil and Hazardous Substance Pollution Contingency Plan and will involve the broad range of response and recovery functions, including rescue, mobilization of people and resources, multi., level incident management, tactical operations and testing of industry and agency contingency plans. The CG's National Strike Teams, which have been trained for Chemical, Biological and Radiological responses and were .instrumental in the response and recovery operations at the recent Ricin incident in the Senate Office Building, will also be deployed.

In summary, DHS is taking a comprehensive approach to the needs of maritime security. It cannot start and end at our maritime borders. Rather, it will take an integrated and coordinated approach that stretches from ports such as Miami and Los Angeles to Singapore and Rotterdam.

Service to the Public—Effect on Commerce

fu addition to Awareness, Prevention, Protection, Response and Recovery a sixth strategic goal of the Department of Homeland Security is *Service.* In this, we will strive to serve the public effectively by facilitating lawful trade, travel and immigration.

The Department is sensitive to the impact that increased security may have on commerce. The wide variety of security measures implemented to date has had no significant adverse impacts on the flow of maritime commerce. That said, we note that the cost to industry to comply with MTSA regulations is estimated to be $1.5 billion in the first year and $7.3 billion over the next 10 years. While we clearly understand that the cost of these security regulations to the maritime industry is not insignificant, a terrorist incident against our marine transportation system would have a devastating and long-lasting impact on global shipping, international trade, and the world economy. Based on a recent unscheduled port security closure incident, a maritime terrorist act was estimated to cost up to $2 billion per day in economic loss to the United States.

The Department understands there will be short-term costs, particularly for many smaller ports or companies with less existing security. Nonetheless, as the industry owns the infrastructure that is being protected, and benefits from that ownership, they should rightly be involved in protecting their infrastructure. We are engaged with the maritime industry to provide information on any available Federal funding. Thus far, the Department has awarded or made available a total of nearly $500 mil-

lion in port security grants over two years. There is also a shared cost burden by the government. The Department of Homeland Security, and its associated agencies, has spent hundreds of millions of dollars to improve our capability to protect the Marine Transportation System. However, the cost of securing America cannot be left exclusively to the American taxpayer.

In addition, we are continuously seeking out technology and procedural changes that will make our efforts not only more effective and efficient but also less onerous on the vast majority of maritime stakeholders who pose no threat to maritime security. As an example, the CG is incorporating an option in the 96-hour vessel notice of arrival (NOA) requirements to permit electronic submission of information. This e-NOA submission method will allow for importation of data into the CG's National Vessel Movement Center (NVMC) database, the Ship Arrival Notification System (SANS), eliminating all but minimal manual data entry. This will significantly enhance the processing and identification of security and safety risks posed by vessels entering our ports and move information to the field much more rapidly. By merging CBP and CG vessel and people information requirements into the e-NOA, the reporting burden on the maritime industry will be reduced. When the e-NOA system is fully developed, vessel owners and operators will have the option to use the e-NOA to satisfy CBP's Advance Passenger Information Service (APIS) requirements as well as the CG's NOA requirements.

The security requirements of the MTSA were developed with the full cooperation of the private sector. We have developed the security regulations to be performance-based, providing the majority of owners and operators with the flexibility to implement the most cost-effective operational controls, rather than more costly physical improvement alternatives. By establishing consistent national and international security requirements we will also be helping businesses by leveling the playing field. Consistency helps business—consistency amongst companies, states and countries. The Department will be vigilant in its Maritime Homeland Security mission and will remain sensitive to the impact of security measures on maritime commerce.

Conclusion

Our maritime security is first and foremost about awareness—gathering and synthesizing large amounts of information and specific data from many disparate sources to gain knowledge of the entire domain. Maritime Domain Awareness and the knowledge it imparts will allow maritime law enforcement and regulatory agencies to respond with measured and appropriate action to meet any threat. However, it will require the continued growth and development of strong partnerships not the least of which is among the CG, TSA, ICE and CBP, state and local agencies and our collective maritime stakeholders. No single maritime stakeholder whether it is government, industry, or private sector can do this alone. We must continue to work together to improve security. Tills is never more important than now in our collective national imperative to defend our Nation and win the war against terrorism.

The men and women of DHS have accomplished a great deal in the past year and we are each very proud of them. In the end, no amount of planning or strategizing is worth the paper it is written on without the dedicated effort of committed men and women who wake up every day with the safety and security of their nation on their minds. Thank you for the opportunity to testify before you today. We will be happy to answer any questions you may have.

The CHAIRMAN. Thank you very much.

Admiral Collins or members of the panel, has a vulnerability assessment of our Nation's maritime transportation system been completed?

Admiral COLLINS. The Port Security Assessment Initiative, Mr. Chairman, is underway. We've completed it in over 16 of our 55 major ports. There's three more that have just been started in the last month. And as we briefed in previous hearings and reports to both the House and Senate, we're on schedule to complete those by the end of this calendar year. That was the original timeline. We're still on that timeline to do those vulnerability assessments. And they become very, very important to the area maritime security committees in over 40 jurisdictions around the country as we build and refine our port—overarching port security plans, Mr. Chairman.

The CHAIRMAN. Admiral, I know you're aware that the responsibility for oversight of maritime security grants has been transferred to the Grants Policy and Oversight Office, an office that I understand, for the last year, has been staffed by one full-time employee. Is that sufficient attention to this issue?

Admiral COLLINS. Mr. Chairman, I don't know the staffing profile of that particular office. I know the intent here in the consolidation is to get some efficiency focus to facilitate the application of grants, sort of a one-stop shopping for states and localities. They can go to the Department—exactly how—I don't—I don't have the staffing profile, and we can provide that for the record.

The CHAIRMAN. Well, check into it. If it's true, you've not only got one stop, you've got one person.

[Laughter.]

The CHAIRMAN. Do you have adequate funding, Admiral, to meet the requirements being placed on the Coast Guard?

Admiral COLLINS. One of the—Mr. Chairman, obviously one of the big funding line items in our 2005 budget is over a hundred million dollars and over 700 people to implement the terms and conditions of the Maritime Transportation Security Act in the regulation that we promulgated last October. It's the first opportunity we've had to go on budget for this initiative. That will, in fact, give us the wherewithal to implement this particular regulation, to oversee it, to ensure compliance, to review the plans, to oversee the exercises, and all those types of things.

The CHAIRMAN. Admiral, this is a very tough question. And I understand that you may not—you may have difficulty answering it, and I appreciate that, because it's very difficult. But do you have adequate funding to meet the requirements that are being placed on the Coast Guard?

Admiral COLLINS. Yes, sir. I think the—yes, sir, we're pleased with the support——

The CHAIRMAN. Admiral Breaux says no.

Admiral COLLINS. We have, of course, our 2005 budget is a 9 percent increase, a pretty substantial increase in these—in this particular budget times. We're appreciative of the support that we've received within the Administration for that. Over the last 3 years, our operating expense budget, between 2002/2003 and 2004/2005 has gone up 51 percent. That's a substantial increase by—in anyone's estimation. So we're very, very pleased that we've been able to increase our force structure accordingly. And we're making progress, Mr. Chairman. It's the right direction.

The CHAIRMAN. It's a very excellent political answer, Admiral. And I understand the difficulty associated with the answer. We'd like to hear more about specific needs and specific requirements.

You and your staff are to be commended for spearheading the U.S. effort to establish international standards for maritime security and the international ship and port facility security code. We know all about that. But tell me, what happens to ships that are calling on the United States who have failed to meet those requirements on July 1?

Admiral COLLINS. There is a number of intervention strategies that are possible, that go all the way from denial of entry to additional inspection requirements and delayed departure and a whole

host of things. We, in fact, have a matrix developed of all those intervention strategies under our Port State Control hat is the term of art that we——

The CHAIRMAN. You would anticipate that there may be ships which have not met the criterion?

Admiral COLLINS. The way that we're going to deal with that, Mr. Chairman, is that, of course, every—under the terms of the ISPS code that 108 nations have signed up for, is that each flag state will issue security certificates to their vessels that certify, from the flag-state perspective, that they, in fact, compliance with the standards in this new international code. We will—our plans are—and effective 1 July—we're already doing interim inspections now—but 1 July, every foreign vessel coming to the United States will be—would be boarded, will be inspected to ensure compliance with international standards, 100 percent. And then we'll do that at least on a annual basis; and, in the interim, we'll do a 20 percent—review 20 percent of that population through the course of the year. So we're going to do a very, very aggressive Port State Control examination process to certify that they're meeting those standards, and we have, incidentally, developed fairly rigorous training programs for our inspectors, both for facility inspection, vessel inspection, and port inspection functions.

The CHAIRMAN. Gentlemen, we need more memorandums of agreement between your agencies, and I hope that you will make progress in that area.

Senator Hollings?

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

Admiral Collins, let get back to this chart here. Do you mind taking that down so we can see it?

Now, looking right at the chart you have submitted to the Committee, reduce maritime security risks, this is the responsibility of the Coast Guard, right?

Admiral COLLINS. Yes, sir.

Senator HOLLINGS. And if something wrong happened at a particular port such as a terrorist activity, the first person to be looked upon for either blame or commendation, depending on what happened, would be the captain of the port——

Admiral COLLINS. That's——

Senator HOLLINGS.—right?

Admiral COLLINS.—that's the Federal Maritime Security Coordinator, as defined in the——

Senator HOLLINGS. Well, the captain of the port, under law, is responsible. Now, these young officers are out there, and I see them, and I talk to them, and everything else, and I'm concerned about whether or not they are getting enough support from you?

Now, go to the first section, put a dollar mark by that. It's entitled "Enhanced Maritime Domain Awareness." How many billions of dollars is that?

Admiral COLLINS. They—we are—it depends which one item you're talking about, of course——

Senator HOLLINGS. I'm talking about the first red section, "Enhanced Maritime Domain Awareness."

Admiral COLLINS. That is—I can give you a breakdown of the money spent over the last——

Senator HOLLINGS. Well, just generally speaking, a ballpark figure.

Admiral COLLINS. Well, there's the $24 million, of course, that was appropriated last year for——

Senator HOLLINGS. You can perform all of that for $24 million?

Admiral COLLINS. No, that's for one element of that, Senator. That's for the——

Senator HOLLINGS. Yes, give me——

Admiral COLLINS.—start of the—the start of the———

Senator Hollings: Well, you see what I'm getting at. I want to put a dollar mark on each of the four. Now, under the first of the four, what dollar mark would you put?

Admiral COLLINS. I'll be glad to break that down and provide that for the record, Senator. There has been a considerable amount of money spent out of our base and out of——

Senator HOLLINGS. And generally speaking——

Admiral COLLINS.—appropriations.

Senator HOLLINGS.—your needs, you know what you need. You couldn't remember, perhaps, the exact figure, but you have a ballpark figure in mind. How much for the first?

Admiral COLLINS. There are a number of—both capital funds and operating-expense funds, and I would be—I would have to tabulate that for you, Senator. I don't have the number off the top of my head.

Senator HOLLINGS. And what about the second? You don't have a number for the second?——

Admiral COLLINS. I—well, I——

Senator HOLLINGS.—"Build and Administer Domestic and International Security Regime."

Admiral COLLINS. The MTSA implementation, in terms of the budget request in 2005, it's $100 million issue, and that's in our 2005 budget.

Senator HOLLINGS. And so 100 million would take care of number 2.

Admiral COLLINS. Not the entire—that it'll take care of the oversight in the compliance of the—in the terms and conditions of MTSA.

Senator HOLLINGS. Well, number 2—I'm just looking at your chart—is—$100 million your figure on that one?

Admiral COLLINS. It is—$100 million, Senator, is——

Senator HOLLINGS. You know, I'm always askance at all this chart nonsense. Man, I've been through it. I've got 38 years of charts.

[Laughter.]

Senator HOLLINGS. Now, give me the money. I'm trying to get down—it's a very simple question. The distinguished Chairman was more than polite in asking, and you've got no idea about 1, 2, 3, or 4, do you? Do you have an amount to give to the Committee?

Admiral COLLINS. I'd be glad to provide that to the Committee.

Senator HOLLINGS. For each one of those——

Admiral COLLINS. Absolutely. Yes, sir.

Senator HOLLINGS. And when you provide all of that, did you ask for that, of the Administration?

Admiral COLLINS. There is a good portion of these elements——

Senator HOLLINGS. No, don't give me "a good portion." Did you request that amount? These are simple questions and simple answers.

Admiral COLLINS. The—we requested the money, for example, for the MTSA——

Senator HOLLINGS. No, no. Did you request the money for the entirety of this?

Admiral COLLINS. They're all—these are——

Senator HOLLINGS. For one year. You can't do it all in a year. I mean, I'm trying to be——

Admiral COLLINS. The port-—the port-——

Senator HOLLINGS.—reasonable and practical, just like you.

Admiral COLLINS. The portion that we can build out and schedule in 2005 is included in our budget, yes, sir.

Senator HOLLINGS. Well, for how much?

Admiral COLLINS. Our overall home security portion of our budget is about 48 percent of our old entire base. And, again, I—I'll be glad to detail these, itemize these initiatives, and also show you the money that has been spent over the last 2 years——

Senator HOLLINGS. Yes, but I'm trying to get the authorization. This is an authorizing Committee, and we're at fault if we don't get you the authorization for the funds needed. All I can get out of you this morning, is charts and conversation, I would like an amount. I want to know how much—I know the $7.4 billion, because you've given me that amount——

Admiral COLLINS. Sir, the——

Senator HOLLINGS.—your predecessor, incidentally, Admiral Loy.

Admiral COLLINS. The $7.4 billion is the impact on the private sector of the MTSA regulation.

Senator HOLLINGS. Yes.

Admiral COLLINS. In other words, it's—that is not necessarily special program——

Senator HOLLINGS. I'm still getting conversation. Do you have any amounts in mind?

Admiral COLLINS. Yes, sir, and I'll be glad to provide that detail for the record.

Senator HOLLINGS. All right, sir. They are—because we know that—you know—you have $43 million. And if you have $86 million, that would be 100 percent increase. I mean, come on. The percentages mean nothing to this Committee. We've got to get going and get this job done.

With respect to the language, now, with—you say "one roof" and "layered" and "fused" and "comprehensive" and all. Where's the place to go for intelligence on port security? Is it your office or—where is that office? I know that Customs has an intelligence endeavor. The Coast Guard's an intelligence endeavor. The homeland security crowd has its intelligence—the FBI—the FAA—everyone has intelligence—where is the office, the one-stop shopping for intelligence on port threats?

Admiral COLLINS. For our Department, it's the Under Secretary at IAIP, sir, that is the node—Information Analysis and Infrastructure Protection—which is the informational node for our entire Department for not only maritime security, but the security across the board. We plug into that information intelligence fusion node, as

does other elements in the Department. Our particular part of the equation, we have a maritime—National Maritime Intelligence Center that's co-located with Office of Naval Intelligence, in Suitland, Maryland, that oversees the screening, and so forth, arrivals of ships coming inbound to the United States, vet that information through multiple national data bases in a coordinated way through FBI, CIA, and other national data bases, and with the targeting center at Customs, sharing that information collaboratively, and coming with the joint risk assessment on how to approach inbound ships, containers, and so forth, into our country.

Senator HOLLINGS. If you'd indulge me one more question——

The CHAIRMAN. I'd be pleased to indulge you.

Senator HOLLINGS. LNG containers. You know, right after 9/11, we were very disturbed by liquified natural gas. In fact, General Dynamics manufactures the containers in Charleston. And one ship contains enough liquified natural gas from Algeria to power 30,000 homes for one year. If they could ignite it, they said, it would be just like an atom bomb in the Port of Boston. I take it you're not going to allow one of those during our convention.

Admiral COLLINS. No, sir, and I—there's a—also, just a comment, there's a—in terms of the technology in the—what happened——

Senator HOLLINGS. Where are they coming in now? Do you——

Admiral COLLINS. Sir, they're coming in from multiple places. They're—ones going into Boston are from Trinidad and Tobago.

Senator HOLLINGS. So they are coming in from—coming into Boston now.

Admiral COLLINS. Yes, sir. And they're coming into Trinidad and Tobago. That's a loop from Trinidad and Tobago into Boston. We have a very, very strong oversight—security oversight program for that transit, including—we have been down in Trinidad and Tobago, we've inspected their facility down there from security, we've coordinated with the companies involved, we board every ship offshore, we provide escorts, we provide sea marshals on those vessels, layered defense, even air coverage all the way in and out of Boston. So I think we have been very, very detailed, very, very rigorous in dealing with that risk. And, of course, LNG comes into other parts of our country, as well—into the Chesapeake Bay, into Port Arthur. There is multiple applications in for LNG deepwater ports. And so——

Senator HOLLINGS. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Snowe?

Senator SNOWE. Thank you.

Admiral Collins, I wanted to go back to the Deepwater Program, because I do think it's essential to the Coast Guard major responsibility, in this instance, in enhancing port security and bolstering the maritime domain awareness. And I'm very concerned about the timelines that have been proposed and that we're adhering to, much to my objections, frankly.

As I said earlier, I did include, in the Homeland Security Act, a study that indicated that we could save more than $4 billion over the life of the program if we accelerated it by 10 years, and that's not even including the under-estimation, in my opinion—and I think I'm on track in saying this—of maintaining the current assets, whether it's, you know, the aircraft or the vessels, because, as

I understand, they're deteriorating even more rapidly—the costs are greater to sustain their readiness—and also the mandates under the law for enforcing maritime security.

So my first question is, Why aren't we pursuing a different timeline? Are you going to be able to perform your responsibilities with the existing assets?

Admiral COLLINS. Well——

Senator SNOWE. It deeply troubles me, as you know. And I—you know, I'm going to just keep insisting on this——

Admiral COLLINS. I share your—excuse me.

Senator SNOWE. Go ahead.

Admiral COLLINS. I share your concern, Senator. The current readiness status of our fleet, both air and surface, is my number-one concern, as the head of the Coast Guard. We are—we have a rapidly deteriorating readiness position because of the aging—some of our ships are eligible for social security, literally. They're older ships, and we're using them hard, in the national interest. So they are deteriorating in front of our eyes. And the conundrum that I'm faced with is that Deepwater has two basic pots of money in it. One is to maintain and enhance the capabilities of the legacy systems, or the existing system; one is to buy the replacement. But I'm stealing from the replacement money to keep the Band-aids on the—and so——

Senator SNOWE. Yes.

Admiral COLLINS.—it's a problem.

Senator SNOWE. Well, that's a serious situation, then. I mean, the bottom line is, Can you perform your mandate regarding homeland security missions with your current assets, either now or into the future?

Admiral COLLINS. I think——

Senator SNOWE. I mean, let's look into the next 5 years.

Admiral COLLINS. I don't think so. I think the timeline has to be addressed, and I think the 2005 budget—appreciative of the Administration's support that we've got in the 2005 budget—it increases that plus-up that we received in 2004, with the help of this Committee and others, that have acted to plus-up almost $200 million for Deepwater, and so it accommodates that, plus a modest increase. So it is showing a commitment to this requirement.

I think that, over the multi-year basis, we're going to have to rethink this timeline because of the—two things—because of the readiness condition, the material condition of the fleet, and, second, the Nation needs this capability now—that this brings a network-centric system to the maritime for this layered defense posture.

Just a couple of statistics on the material condition of our fleet. I had 670—over 670 unscheduled maintenance days for my major cutters. That's four of my major cutters, in a fleet of 12, that I was not able to lose—use last year because of unscheduled maintenance. That reflects their age and failing systems. Our 110-foot patrol boat is the workhorse of our fleet—does all our coastal search and rescue, our law enforcement, our interdiction of migrants, and so forth—suffered 20 hull breaches—yes, that's water coming into the hull—and required emergency dry-docking. Why? They're beyond their planned service life. The current schedule in Deepwater

for the replacement of that asset is not until 2018. I can't wait to 2018 to replace this asset.

Some are graphic examples of the current readiness posture, and why, looking at that multi-year plan and restructuring that multi-year plan is very, very important.

Senator SNOWE. Well, it sounds like we have to do this on an emergency basis, because it's going to take some time, obviously, just to replace the existing assets. I mean, this it not something that's going to happen overnight. But that's a dramatic situation that we're talking about, and it is going to encumber your ability to do what you need to do to protect, you know, our maritime domain awareness and pushing this threat out to sea——

Admiral COLLINS. Sure.

Senator SNOWE.—so that it doesn't reach our ports.

Well, does everybody understand that?

Admiral COLLINS. I mean, it all comes down to budget priorities and——

Senator SNOWE. Wow, it's——

Admiral COLLINS.—and so forth.

Senator SNOWE. I think this is a——

Admiral COLLINS. As we know——

Senator SNOWE.—major priority.

Admiral COLLINS. I am an advocate for a strong support of the integrated deepwater system.

Senator SNOWE. Well, I think that, obviously, we do have a urgent situation on our hands, you know, and it basically is undercutting your ability to do what you need to do, and I think that needs to be on the record. I think it has to be underscored, it has to be reinforced—we'll get everything on the table here—that these investments need to be made. And I think it's just—you know, your comments here this morning is illustrative of what we're facing. I mean, we can continue to ask you to do everything you need to do, but if you can't do it, you simply can't do it. Six hundred and seventy days? I mean, I hesitate to think about how much the costs are involved that takes away from the future modernization program. Do you have any estimate, currently?

Admiral COLLINS. Based on the current condition and the couple of data points that we have, that we could be, over the next 10 years, spending between 500 million to a billion dollars more on maintenance for our ships because of their current state. And, again, every dollar we spend is a dollar away from the modernization part.

So it's sort of this downward spiral phenomenon you get yourself into, and I—you know, if you talk to other service chiefs, whether it's the Navy, the Army—they're very familiar with this issue of current readiness and condition of the current assets, versus modernization and how to balance—do a balancing act on that, maintain the current operational capability and then get ahead with modernization.

But we're—I think we're reaching a critical stage. Again, we have some very, very old assets. If you compare our fleet with major navy fleets of the world, we are right down at the bottom, in terms of the oldest fleets in the world. And so this is a—I do have—again, I do have the sense of urgency, because I feel that it's

my responsibility to ensure that our men and women, who we put in harm's way every day, need to have the best equipment possible. And to do so, I would be irresponsible not to take any other position.

Senator SNOWE. I appreciate that, Admiral Collins.

Thank you.

The CHAIRMAN. Senator Breaux?

Senator BREAUX. Thank you, Mr. Chairman.

I'm sure Mr. Bonner and Mr. Stone are feeling neglected up there at the witness table, and just wished they were engaging in these questions that Admiral Collins is bearing the brunt of.

The thing—now, the chart's gone, but, I mean, on that reduced maritime security risk, I mean, I'm sort of like Senator Hollings, I'd—you know, the charts are great, and they're pretty, and they're multicolored now, and how we have them under the computer systems we get, but what is really lacking on all of this is—there are two things, at least. Senator Hollings pointed out that it's lacking about how much it's going to cost and where the money's going to come from. The second thing that I think is really missing is, What date goes right after each one of those? I mean, you know, it's a wonderful chart, but if the date is 2020 or 2030 or 2040, it doesn't give anybody much comfort. If it's within this year or next year or the next Fiscal Year, that's one thing.

Which leads me to the point of the questions I want to ask about the situation in the Port of New Orleans. And the Port Director, Gary LaGrange will be with us. But with regard to the automatic identification system, the requirement is that all the ships have the AIS equipment onboard so they can transpond to a central terminal to locate where all ships are at all times. That system is not in place in New Orleans, is it?

Admiral COLLINS. It's not finalized. It will—all our nine VTSs will be fully equipped and up and running by the end of this calendar year.

Senator BREAUX. Was the system in place the night and the morning of the ship crash that occurred in the mouth of the Mississippi River?

Admiral COLLINS. I don't believe the AIS—I'd have to get back to you. That's——

Senator BREAUX. The answer is, it was not. The AIS system was not operating. And the purpose of that system, obviously, is to track ships because of potential terrorist activity onboard one of these vessels, or because—also just monitoring the navigation, from a safety standpoint. In your opinion, had that system been in effect, would we have had better information about the locations of those ships?

Admiral COLLINS. I'd have to wait for the results of the investigation, which is ongoing right now.

Senator BREAUX. Well, that's not the question. My question was very careful. I mean, would—had that system been in place, would you have had better information on the location of the two vessels?

Admiral COLLINS. I think that system provides you a margin of information—improved margin of information wherever you would put it in. And I——

Senator BREAUX. If the system had been operating, you would have had an identification and location on the ships in the Mississippi River.

Admiral COLLINS. Absolutely. It gives you better visibility of the—of vessels. And clearly that's, you know, why we have been aggressive trying to push this system—AIS base VTSs. We think that's the way to go.

Senator BREAUX. Is the reason it is not in place in New Orleans and other ports around the country because of technology is not available, or is it because of the costs that we do not have the money to pay for?

Admiral COLLINS. I think it's a cost and schedule issue that it boils down to, and we're building it out as fast as cost and schedule allow. And, again, the game plan is to have it all—all the nine VTSs, Senator, by the end of this calendar year, is the current schedule.

Senator BREAUX. This goes back to the Chairman's question and then Senator Hollings question. My information is that you requested $1 million in the budget for the AIS system last year, and this year it's five million. That is woefully inadequate to accomplish what you're saying that you'd like to have done, isn't it? You can't do it with——

Admiral COLLINS. It really——

Senator BREAUX.—for $5 million.

Admiral COLLINS.—it really stretches it out, Senator. One of the——

Senator BREAUX. It does.

Admiral COLLINS.—one of the things we're looking for, for your information, in terms—to try to moderate the cost challenge is to look at existing structures in which to place—this is having AIS coverage beyond the immediate ports, beyond the VTSs. So we're looking at things like NOAA buoys and offshore platforms—you've very familiar with how many offshore platforms are in the Gulf—but to use those as structures by which to place AIS equipment.

Senator BREAUX. I understand that. But the problem is that you are not able to request sufficient funds in order to do these types of things. I mean, $1 million to do an AIS system nationwide is really not even close to getting it started. And this year, it's $5 million. Now, I think had that AIS system, in the—maybe the Coast Guard inquiry on the cause of that accident will reveal more information—but had that system been in place, clearly the central control system would have known where those ships were, what—the movement and what direction they were going in, and possibly could have avoided a very tragic accident. I mean, I can't say that. I mean, it's a tragedy for the families and for everything. But had that system been in effect, we would have had a great deal more information in order to warn the ships of an impending collision—which occurred and shut down a port for 4 days, not even to mention the tragic loss of life.

So, anyway, we don't have enough money to do what we should be doing. I mean, that's—I think that's pretty clear, particularly in this area.

Mr. Bonner, it seems to me—and we've had these discussions—that it's much more difficult to inspect 3,000 containers on a ship

when it arrives in port. It's much better to try and inspect the containers when they are loaded on the ship in the foreign port. And you say we now have about 38 ports around the world that are coordinating. I mean, I'd like to know a little bit more about that. Are you able, or is our government, to go in and say, "Look, you're going to have to have an inspection system that tells us what's being put on these vessels, or we're not going to allow you to call on our ports. It's just that simple?" And I guarantee you, with everything we're importing into this country, other countries would put it into effect lickety-split, because they're not going to be able to say, "We're not going to ship to the United States." What's the status of all that?

Mr. BONNER. Well, first of all, there are—they're countries that represent 38 foreign ports that have agreed to implement the Container Security Initiative.

Senator BREAUX. Is that our——

Mr. BONNER. We——

Senator BREAUX.—is that our Container Security——

Mr. BONNER. It's our——

Senator BREAUX.—Initiative?

Mr. BONNER.—Container Security Initiative. And it means, Senator Breaux, that they've agreed that they will—first of all, we will have targeters there. We will be using, and are using, our automated targeting system to identify, based upon strategic intelligence—not just specific intelligence, but strategic intelligence—as well as anomaly analysis, the containers that pose, in our judgment, a potential threat for terrorist exploitation. The host nation that—joint CSI agrees that when we then, based upon our targeting and any information, additional information, they can give us—and, by the way, being there, our targeters being there, there is an exchange of information that takes place with the host nation customs authorities—but if we say, "Look, we're concerned about this container or this group of containers," because of where they're coming from and other things that go into our targeting rules, we request them to actually do the minimum security inspection. And the minimum security inspection is running that container through the large-scale X-ray imaging machines—so to be in CSI, you've got to have at least one of these machines at your foreign seaports—and run it for radiation detection. Now, obviously, if there is a concern then, it gets a physical inspection, but relatively few do. So we select out—that's the agreement, that's what CSI is. And we have deployed that now to 18 foreign seaports where we have Customs and Border Protection inspectors, targeters, working with the host nation to identify high-risk containers and see that they're screened overseas before they're loaded onboard vessels headed for the U.S.

And 18 foreign seaports, by the way—we just—the first foreign seaport was just 18 months ago, so we've deployed one every month since September of 2002. And we're continuing. I mean, we're not stopping with those 18. As I indicated, we're going to expand this. I believe we'll hit over 30 by the end of the—at least 28 to 30 by the end of the Fiscal Year, and another four by the end of the year, and to expand it out.

So this gives us a system in place, with respect to many of the major ports of the world—the megaports, the hub ports that ship most of the containers to the United States. And, by the way, these are also placed in areas where—you know, nothing comes directly from Karachi to the United States. I can tell you that right now. It comes through Singapore, or it comes through Hong Kong. And we have CSI there. So it's a hub using targeting and target analysis and information to identify high-risk containers, and then doing it there.

Now, we're ramping this up. We've—you know, there's no question that we've made good progress, but we have ways to go. We probably need to increase, to some extent, the numbers of targeters that are working in particular countries, like Singapore, because of volume, but we've made good progress so far in expanding the Container Security Initiative. And it has been well received and widely accepted by every—virtually every country that we've approached to join in with us with the Container Security Initiative.

Senator BREAUX. Thank you.

The CHAIRMAN. Senator Lautenberg?

Senator LAUTENBERG. Admiral Collins, we all are very fond of the Coast Guard, the work that it does, and the relationship that we have within the coastal states particularly to the Coast Guard, the number of functions that it performs. But yet, in response to the Chairman's inquiry about whether or not you have enough funds, you were more than gracious, I think, with the Administration by saying, "Don't worry about it, we've got plenty."

But if I look at the GAO report that recently came out, in March of this year. The total Coast Guard resource hours have increased substantially, 39 percent, over pre-September 11 levels in Fiscal Year 2003; but, not unexpectedly, homeland security is the greatest beneficiary of the increased hours, as more vessels devoted to homeland security have been added to the fleet. Conversely, the resource hours for most non-homeland security programs have decreased as many more resources are now generally devoted to protecting the Nation's ports and waterways.

For example, resource hours for several programs that the Coast Guard has traditionally conducted, such as living marine resources, search and rescue, declined by 26 and 22 percent, respectively. And if we look at the various categories of activity—illegal drug interdiction, down 44 percent. And this morning, there was a drug bust of 29,000 pounds of cocaine off the West Coast, so there still are plenty of drugs out there, we know that.

How do you square, Admiral, this minimal increase in funding with all of these activities that you are responsible for? It's terrific to see the enhancement of the security concerns being attended to, but these other functions are important functions, traditional Coast Guard functions. What happens with them?

Admiral COLLINS. Clearly, homeland security and the security of our ports and waterways is priority number one. You know, the Secretary believes that, I believe that, I think Commissioner Bonner and Administrator Stone believes that. And that—because the consequences are very, very substantial. So we have to maintain, I think, an aggressive posture. Most of our budget plus-ups over the last couple of years have been devoted to building up

our—to be just confident—the Coast Guard to be just as confident in the homeland security part of our business as we are traditionally in search and rescue and servicing aids to navigation and breaking ice and so forth. I think if you look at our performance in all those missions, along with activity levels, that—activity levels give you one perspective. Look at our performance and outcomes, and I think you'll see, in all the non-homeland-security areas, that we've met every standard, we've exceeded every performance goal in those particular non-homeland-security missions, if you will. We have not backed off our search and rescue standards one bit. We're meeting our search and rescue standards. We saved over——

Senator LAUTENBERG. Was that a bloated budget that you had before that we should have——

Admiral COLLINS. I think——

Senator LAUTENBERG.—reduced the——

Admiral COLLINS.—I think that you'll see ups and downs of those numbers in any given year, based upon the risks that we're dealing with in that year. Our whole allocation of our cutters and our boats and our people is all risk based. You know, we're allocating resources day in, day out to the greatest risk at the time.

Senator LAUTENBERG. Well, how about something like the foreign fish enforcement, the living marine resources? These things don't have an immediate response to attention, but they will—in years ahead, suddenly we'll find ourselves with—over-swamped foreign fishing fleets that rape the bottom of our oceans and leave nothing there for us to harvest. I think, honestly, you're—I would have normally said "you're a good soldier," but you're not a soldier. The fact is that you are certainly loyal to those who make the decisions, but we know how seriously the Coast Guard takes its responsibility. And you can't make the case that we can constantly do more with less, unless we want to change the mission of the Coast Guard altogether and say Coast Guard is another part of the intelligence or anti-terrorism organization, and leave the nautical part to something else.

Admiral COLLINS. Part of the—Senator, part of the challenge of this thing, again, is to manage to the greatest risk at the time. I mean, understanding that we're not optimally resourced for every one of our missions simultaneously, and so to mobilize our—to be multi-mission, in terms of our resource, multi-task capability we embed in every one of our resources. They can surge to those issues, and we've done that, and I think we've done that very, very effectively, and that's a good story. The second is to be—to grow. And I think if you look at our budgets over the last 3 years, we are growing. We've added—our workforce has grown by over 12 percent, our budget's been increased by the Administration——

Senator LAUTENBERG. But it has been absorbed by functions.

Admiral COLLINS. It——

Senator LAUTENBERG. More than absorbed. And when you say that the American Coast Guard is near the bottom of the list with the kind of equipment that we need to do our job, it's distressing to hear that, and that has to come from some pot of resource that is being used otherwise.

And, Mr. Chairman, the conclusion is that we cannot maintain all of the functions that we need to maintain, those that take care of now and those that take care of the future, without supplying the resources.

And I'll conclude with this very quick question for Admiral Stone. Mr. Bonner, I don't mean to leave you out, as Senator Breaux said before, but the fact of the matter is, I have a question for you about the radiation detection, because that's like the second line of defense. The first line of defense is what we do at those ports of embarkation, and how do we control it, and can we effectively stop those ships from coming here if those ports look like they're particularly dangerous places for us? Is that——

Mr. BONNER. Well, first of all, you know, one thing that I think is not often recognized, but if we had a specific concern from intelligence that we received from IAIP through the intel community about a specific container that posed a terrorist threat, we have information, under the 24-hour rule, of all containers, wherever they're moving, if they're heading for the United States, before they leave foreign ports, Senator—before they leave the foreign ports, 24 hours before they're loaded onto our vessels to leave. So we literally can instruct the carrier to "do not load that container" until we are satisfied that it doesn't pose a threat.

Now, if we're at a CSI port, we obviously are in a position to make sure we do the security screening, because we have—we're there, and we also have the commitment from the host nation to work with us to get it done.

But we have some means here to prevent a container that poses a risk, if we have the intelligence, to prevent it from going onboard. And then, at CSI ports, it's beyond just the intelligence; it's the strategic intelligence, if you will, that there are a group of containers that were—we have sufficient concerns about that we want them to be inspected before they're loaded onboard——

Senator LAUTENBERG. Yes, but referring to Senator Breaux's earlier question, could we assign a different status to those ports that we expect problems coming from—could we simply embargo that port and say the only ports that are going to be allowable are those—you described some as hub-ports—can we do that if we choose to do that? Or——

Mr. BONNER. I actually think we're—in essence, as we expand out the Container Security Initiative and the standards that Senator Breaux was referring to, where we've got a much broader coverage, then you have the possibility of simply saying, let's say, at level orange, or where there's a higher threat level, that all containers, if they're moving to the United States, have to move through those ports. But you don't want to do this, in my opinion, until you have——

Senator LAUTENBERG. Commerce——

Mr. BONNER.—much broader coverage of the Container Security Initiative than we have with just 18 ports. But, yes, I think that would be a direction. And, ultimately, of course, the Coast Guard, under MTSA, will be certifying the security at the foreign ports themselves that are shipping containers to the U.S. and so——

Senator LAUTENBERG. So we're working from the beginning—before it begins——

Mr. Chairman, I wanted to say to Admiral Stone that we've been more than perplexed, frustrated, et cetera, about the slowness of DHS's—slowest—terribly late response to our inquiries in this Committee, and I want to leave you with a question.

If you could provide us with some identification of the directorate's resources that are devoted to port security tasks, and those that have been assigned to rail security. And I wonder if you could just tell us how long it might take to get that information.

Admiral STONE. Yes, sir. Would you—you'd like that from the Department perspective, or just TSA-specific, or the overall Department?

Senator LAUTENBERG. No, from the Department's perspective.

Admiral STONE. Yes, sir. I'll go to work on that immediately and get that to you as soon as possible.

Senator LAUTENBERG. But we won't need a year for that.

Admiral STONE. No, sir.

Senator LAUTENBERG. OK. Thanks very much.

Senator BREAUX. [presiding]. Senator Nelson, any questions?

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. Thank you, Mr. Chairman. Mr. Chairman, I always knew you wanted to be Chairman of the Commerce Committee before you retired.

[Laughter.]

Senator BREAUX. Now I'm leaving.

[Laughter.]

Senator NELSON. Admiral, you have a big job. And it's a big job to comply with the law that says all of these ports have to be ready to meet the standards for port security by July 1. And the fact is that a lot of the foreign ports that do business with the United States, especially the 14 deepwater ports that almost half of the Florida commerce originates from, will not be able to comply by July 1. How are ports in the Caribbean and Central America, such as Puerto Cortez, Honduras, 350 miles south of Cancun, going to be compliant, according to the law, by July 1?

Now, tell us what in the world you are going to do. You have my full support, but I just don't know how you can get ten pounds of potatoes in a five-pound sack.

Admiral COLLINS. It is—Senator, you've hit the nail on the head. That particular part of the regulation is—it's going to be a challenge.

Just to echo your concern, I went down and visited, in Costa Rica, about 3 weeks ago, and several other countries. The reason for my trip was basically building counter-drug agreements, bilateral agreements, with those countries. But I did use the occasion to talk about the MTSA and the ISPS code and how they were going to be meeting core standards. When I visited Costa Rica, that wasn't even on their scope, and there were not—didn't have any overt act—they do now, by the way. I talked to the president of Costa Rica, and they are moving on sharply.

We're going to have to work closely with each one of those countries through regional groups and affiliations, and slug through those issues.

For Florida, there are already regulations in the book. There's a special reporting requirement into the ports in Florida for any vessel coming from the Caribbean, and we're going to have to scrutinize it. We're going to have to pay special attention to every one of those vessels coming in.

That's, I guess, the short of it, is that we're going to have scrutinize each one of those vessels. We're going to have to look at all—if there's a—for instance, Costa Rica doesn't—it's not a flag state, but it—but there are third-party vessels, Panama flag or whatever, that call in this port, pick up the pineapples or whatever it's carrying en route to the United States. So the fact that it takes on cargo from a port not—they're not even a signatory to the ISPS code. So they're not a signatory to the ISPS code, so we're going to have to look at alternative security plans, help them along, have very close oversight, scrutinize them from a risk perspective, and take intervention measures for each and every occasion until we bring that, you know, "tide rising, all ships" type of phenomenon, we bring them up, from a standards perspective.

Senator NELSON. Well, let me suggest to you what's going to happen. We're only talking about three and a half months from right now. When it dawns on everybody that commerce is going to grind to a halt because you are either going to wave off a ship coming from a port that has not complied with the security requirements, or you're going to impound the cargo until it's inspected, to be released, commerce is going to grind to a halt. And that is going to cause an outcry. And the pressure is going to be on you to release and ease up on your security requirements under the law. How are you going to deal with that pressure?

Admiral COLLINS. Carefully, Senator. No, you're absolutely right. No to be flippant about this. It's absolutely a challenge. We're going to have a lot of pressure on that. And one of the reasons we're working in the interagency process with the State Department and others, so that we will have—and coming—developing what we call an intervention matrix of Port State Control. What control actions will we take if this vessel meets—doesn't meet this issue, doesn't meet that issue, and so forth?

But I think for smaller infractions, you don't—you know, for smaller infractions of the code, you don't ignore them—you hold them accountable, but you don't deny—you may not deny entry. It doesn't call for denying entry, it doesn't call for detainment; it calls for having corrective action before the next port of call, or whatever. It depends on what the serious nature of that infraction is. So we'll have a menu—menu of the Port State Control—the most severe of which would be detaining or denial of entry, but that would have to be for a higher-risk issue.

But our intent was to fully hold these ships accountable, and owners accountable. As you know, for safety, we publish a bad-guys list for classification societies, for ship owners, for ship operators, and so forth. And based upon past performance on safety and environment issues, you get on this list or don't get on the list. And if you're on the list as a, what we call a priority one, we are all over you on the inspection regime every time you come in. We're going to do the same—and it's, by the way, produced incredibly good results, in terms of driving substandard ships, from a safety

perspective, out of the U.S. trade—we're going to do the same thing on security.

There's going to be a report card on every vessel. We're going to publish that worldwide. We're going to exchange that information worldwide, so there'll be security accountability, safety accountability, and marine environmental protection accountability for every ship that comes in. So it's a strong oversight inspection regime from a Port State Control to ensure we—and this is about managing risk, and we're going to try to identify risks, sort the risks, and act appropriately. Denial of entry is the last resort, of course. But if the risk is high enough, then you deny entry if the vessel is not complying.

Senator NELSON. Well, I want to suggest, also what's going to happen is that there are those, such as myself, that have been raising Cain about increasing the amount of money appropriated for port security in this country. I mean, what we've been addressing is the port security in these other countries. I assume a port like Rotterdam's got enough financial resources that they're going to be compliant. But you get into some of these—like this port in Honduras and other Caribbean nations, they're not going to be compliant. And yet here in our own country, I have been raising Cain that we're not putting enough money into our port security.

Now, you know, the National Port Council wants something like $5 to $7 billion more. I've been trying to get $2 billion more. And I can't get any support out of the White House for that. As a matter of fact, there is, in the budget submitted by the President in this coming year, it's $46 million. Now, they say it's $1.9 billion, but a huge part of that is actually for you, which—you have to do a lot of other things, other than port security, such as interdiction on the high seas, search and rescue, and so forth.

Admiral COLLINS. Yes, sir. There's basically—this approach that we're taking with this regulation is shared responsibility for this rollout, and shared financial responsibility. The Federal Government is certainly underwriting a major part of our operational presence, maritime domain awareness, and all these other things we're doing, to the tune of the dollars that you mentioned. Commissioner Bonner's work force, my workforce is paid by Federal dollars. We're involved in the security business. That's a Federal investment in the security of our maritime. The figures that have been quoted earlier about the—initially $1.5 and $7.3 billion over 10 years, that's the cost estimated of this regulation, obviously, to state, local, private sector, in meeting the terms and the standards of the regulation. There is almost $500 million that's already been, in terms of grants, distributed to ports, based on their application. As you noted, there are 46 million dedicated funds within the 2005 budget.

But I might add that there's also the ability for ports to apply to ODP within the Department for a larger pot of money. The total amount of grant money available in 2005 through the Department, close to 3.5—I think it's 3.4—billion that'll be administered through the central processing and grant application to ODP, with the Coast Guard and others still the expert witness, if you will, on maritime applications. So a dedicated 46, plus the ability to apply for that larger pot through general application to ODP.

Senator NELSON. Well, if I may be clairvoyant, my job, of getting additional money for American port security, is going to be a lot easier come July 1 because of the outcry that's going to occur, and that outcry will be translated into legislative action because of Members of Congress suddenly hearing about this problem. And not all of the Members of Congress have districts that are on the coast of the United States.

A final question. I have the three largest cruise ports in my state. Now, I know you all have already addressed, here, the issue of security, the metal detectors, and so forth. But I can tell you, from having talked to constituents and others that have recently come on and off of a cruise, that there is not much checking of the luggage, and particularly not so with regard to the kinds of plastic explosives that could be put in luggage and create the same kind of effect that occurred in Spain on the railroad cars. So this is just another little headache that you're going to have to address.

Admiral COLLINS. The cruise—clearly, the—and you're referring to Port Everglades and obviously the Fort Lauderdale area and Miami and so forth, that every Friday that's a pretty busy—those are pretty busy ports as they change out——

Senator NELSON. Miami, Everglades, and Canaveral.

Admiral COLLINS. Yes, sir. And, of course, that was the one segment of the maritime industry that, before 9/11, had comprehensive security plans, by the way—past history of Achille Lauro and other issues that—that was the one part that had more robust—that did have a security regime, and the only—really the only part of the industry that had that type of a security regime. And right at 9/11, of course, we elevated the security condition, and there has been 100 percent screening of baggage and people since 9/11 for the cruise industry.

We're also working with TSA to see what kind of technology enhancements and procedural enhancements, based upon their expertise in screening, needs to be imported——

Senator NELSON. OK, now, on that 100 percent screening, is that just for metal, or is that for all kinds of explosives?

Admiral COLLINS. I don't know the answer to that—I might—maybe——

Senator NELSON. I will tell you the answer.

Admiral COLLINS. Maybe Administrator——

Senator NELSON. I'll tell you the answer.

Admiral COLLINS.—Stone would have——

Admiral STONE. I'll partner with Admiral Collins, sir, and make sure we get you a comprehensive answer on——

Senator NELSON. OK.

Admiral Stone—whether it's just metal or——

Senator NELSON. That's what I'm saying, you're not screening for——

Admiral STONE. Yes, sir.

Senator NELSON.—plastic explosives. And it's an accident waiting to happen.

Thank you, Mr. Chairman.

Senator BREAUX. Are you not X-raying luggage that comes onboard cruise ships? I mean, I've visited the cruise ship terminal, and we looked at what you all were doing, and——

Admiral COLLINS. It has been a lot—the sophistication of the equipment at—on the marine terminal is not on the par as the sophistication at the airports.

Senator NELSON. That's correct.

Admiral COLLINS. And that's the observation that the Senator is making.

Senator BREAUX. So you could detect if they brought a pistol onboard, but not if they brought plastic explosives. Ugh.

Admiral COLLINS. I'll confirm that, but I'm sure the Senator is correct——

Senator BREAUX. That's not too comforting.

Admiral COLLINS. The overall level of sophistication and investment in equipment has not been the same.

Senator BREAUX. That's like when they took my little red Swiss army knife, about this long, away from me when I went into the Superdome Stadium in New Orleans, but if I could have walked in with plastic explosives, they never would have caught it, but they sure caught that one-inch little red knife. I don't know what I could have done with that.

All right, let me—so you said 145 container screeners now, Mr. Bonner? What are—can you tell us, what are the container screeners picking up? I mean, can they pick up anhydrous ammonia being loaded in a container? That wouldn't really show up——

Mr. BONNER. Well——

Senator BREAUX.—would it? I mean, I don't want to get into——

Mr. BONNER. They can——

Senator BREAUX.—something you don't want to talk about, but——

Mr. BONNER. They scan—go ahead, Senator.

Senator BREAUX. I mean, what do you—what are you picking up in container screeners that you now have utilized, 145 of them?

Mr. BONNER. The main thing we're picking up are illegal drugs, but we—but it has the capability—the X-ray screening machine, and we use this on a targeted—risk-targeted basis, but it has the capability of picking up lead-shielded materials. It has the capability of detecting an anomaly. If you had a certain—by the way, we're getting advance information on what's supposed to be in these containers, so if it says "ladies apparel," and it doesn't look like ladies apparel, that's anomaly in itself. So it gives us an extra measure of detection without doing, essentially, a physical inspection of every container we think poses a potential risk, for certain kinds of things. I mean, it doesn't—you know, that's why you have a layered detection strategy, because it—you know, it wouldn't detect against every possible, let's say, weapon, particularly if it were relatively small and wasn't—didn't contrast, let's say, with the density of——

Senator BREAUX. It's a——

Mr. BONNER.—in the background of what's in the——

Senator BREAUX.—it's a huge——

Mr. BONNER.—what's in the container.

Senator BREAUX. Yes, it's a huge problem. I think we've made some real progress with these container screeners, and—but like Senator Nelson was talking about, there are some things that may not even show up on these screeners. I don't want to talk about it

too much in the public; it may give people ideas about what they can bring in. But, I mean, obviously this is a concern I hope you all are trying to address.

Mr. BONNER. Well, we are, and there are layers to this. And one of the things is—if you're talking about just explosive materials—of course, is that we have some other technologies. One is canines that we have trained. As you know, we've had an excellent canine program at Customs—now it's Customs and Border Protection—with respect to dogs that sniff out drugs and even cash. But we've trained, and are training, more canines that are capable of detecting both potential chemical weapons, as well as explosive materials with respect to cars or vehicles or containers that may be crossing our borders. So——

We also have itemizers and some other materials, where we can take swabs of containers or shipments, and run them, and very quickly identify whether they have explosive materials in them.

Now, all of this, by the way, is based upon managing risk and targeting containers or shipments or vehicles that pose a potential risk, and identifying that either in advance or at—when a person or thing presents itself at our ports of entries into the United States.

Senator BREAUX. Well, we want to thank you. We've kept you all here a long time. There have been a number of requests from Members about information that we need to have forwarded. Mr. Stone and Admiral Collins, you both have had requests, and I would hope that you would be able to promptly respond to those Members' requests as quickly as you can. And we thank you very much for being with us.

I'd like to welcome up the next panel. We have, Mr. Chris Koch, who is President and CEO of the World Shipping Council; Mr. Gary LaGrange, who is the Executive Director and CEO of the Port of New Orleans; Dr. James Carafano, who is Senior Research Fellow for Defense and Homeland Security at the Heritage Foundation; and Mr. Mike Mitre, who is Director of Coast Port Security, with the Longshore Division of the International Longshoremen and Harbor—and Warehouse Union. We're delighted to have all of you with us and are pleased to receive your testimony.

Mr. Koch, we have you listed first. Welcome back to the Committee.

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

Mr. KOCH. Thank you, Mr. Chairman.

We appreciate the Committee's looking into maritime security, because it is so important, because so much maritime commerce is moved by this country—about 200,000 importers a year are moving their goods through maritime commerce. There are a comparable number of exporters, all using this industry. So your oversight is very appreciated.

Just to give you a little framework here, we're talking about $750 billion worth of goods being moved in and out of U.S. ports from international commerce. About two thirds of that is moved by the liner industry in containers. That's about $1.4 billion worth of cargo a day going through U.S. ports. That keeps retailers' and gro-

cers' shelves filled, but it also provides markets for U.S. exporters, and keeps factories supplied with the components they need.

There are various facets of how the government is trying to deal with maritime security, and let me just try to identify them very quickly.

The first is ships. As Admiral Collins described, by July 1 all ships arriving at U.S. ports will have to be compliant with the ISPS code. In surveying our members, our expectation is that all our members' ships will be compliant by July 1.

Senator BREAUX. I'm sorry to interrupt you. Is that the AIS system?

Mr. KOCH. AIS is one component of the ISPS code. So all the ships will have that equipment on it, although, as has been discussed earlier, the Coast Guard has yet to be fully equipped to receive AIS transmissions at all ports across the country.

As to ports, the ISPS code also requires, by July 1, that all port facilities have compliant security plans. It's our understanding that all U.S. container terminals should be ready by that period of time, but, as also discussed earlier, we do expect problems in some foreign ports, that not all foreign ports will be compliant by July 1.

One of the unanswered questions we hope to work with Customs and Coast Guard on is: After a compliant vessel has called at a port that is not compliant, what happens to it? And what happens to the cargo that originates at a noncompliant port when it arrives in the U.S.? There aren't crystal clear answers on that. We know we're not suspending trade with those countries on July 1, and it's going to be an iterative process. They're going to put pressure on the industry to keep pressure on these foreign ports. We understand that, too. But we'll need to work through how that's going to be handled.

There's also a people security piece to this, which we recognize. TSA is developing a transport worker identification card for shore-based maritime employees, and other transport modes. As to seafarers, the U.S. Government's cleaned up its seafarer list. As to foreign seafarers, they've suspended the use of crew list visas. Now every seafarer has to get an individual visa. Vessels are also providing the government advanced notice of all crew members 96 hours before the vessel even arrives at U.S. ports, so all crew members are screened through the various intelligence and information systems that the government has.

The final piece of this is really the cargo security. And from the liner industry perspective, that's the more complicated piece of it, particularly containerized cargo. There's a lot of cargo, about seven million containers a year coming into U.S. ports. If we inspect every container, we obviously have gridlock for commerce. So, as discussed earlier, the strategy here is that you screen 100 percent of all containers through the Automated Manifest System, or the Automated Targeting System, using the 24-hour rule. You deploy radiation portal screening, so you can screen 100 percent of all containers for radiation, and we understand the objective is to have that in place by the end of the year. And then you physically inspect everything that the Automated Targeting System says should be inspected. And that's a key component of this strategy——getting the Automated Targeting System to be more robust and more

effective, because it's the lynchpin in the strategy. You want to inspect everything that gets kicked out by ATS.

And then, finally, very importantly, is the CSI initiative. What we would like to point out is that the Coast Guard had the advantage of dealing with the IMO, an existing international organization which can create international rules for ships and ports.

Commissioner Bonner didn't have the advantage of an international organization that sets cargo security rules, so Customs has had to create this through the bilateral agreements forming the CSI network. And in diplomatic terms, they've done a great job. They've got 38 ports signed up: 18 are operational. And it's obviously a work in progress, but a very essential part of the strategy. So the strategy is good. There's a lot of hard work going on, at both government and industry levels, to make it work. A lot of people should get a lot of credit for where they are. But the challenges now are to keep going, because we're still at the foundational level—making ATS more robust, making sure the equipment is there to inspect not only U.S. ports, but at foreign ports, and to encourage international cooperation. We should not fall into the trap of thinking we can solve all problems in the U.S. and that, everything's going to be done here. This is international trade, and we need international cooperation and international standards with our trading partners if we're really going to get our hands around this.

So there are a lot of issues, including good contingency planning, which we discuss a little bit in our submitted testimony. But we think the government's at least on the right track. It's a question now of keep going and keeping focused on dealing with what increasingly become more difficult parts of the challenge.

Thank you.

[The prepared statement of Mr. Koch follows:]

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

Introduction

Mr. Chairman, I would like to thank the Committee for the opportunity to comment on the state of maritime security enhancements. My name is Christopher Koch, and I am the President and CEO of the World Shipping Council (WSC). The Council is a non-profit association of thirty companies that operate forty-four international shipping lines. WSC's members include the full spectrum of vessel-operating ocean common carriers, offering containerized, roll-on/roll-off, car carrier, and other international cargo transportation services. WSC's members carry approximately ninety-three percent of the United States' imports and exports transported by the international ocean liner shipping industry.

International commerce is a huge and economically vital part of our economy, and liner shipping is an essential facilitator of that trade. In 2002, approximately 202,800 U.S. importers received goods from more than 178,200 foreign exporters via liner shipping. The combined value of U.S. exports and imports of goods moved by international waterborne trade in 2002 was approximately $728.4 billion. Close to $500 billion, or two-thirds of that, was containerized cargo carried on liner vessels. On average, roughly $1.4 billion worth of goods are moved through U.S. ports by the liner shipping industry each day.

The Council has strongly supported the various efforts of the government to enhance maritime security, and it will continue to do so. Whether it has been the Coast Guard's efforts as the lead agency for vessel and port security, or Customs and Border Protection's efforts as lead agency for cargo security, the Council has fully supported the government's strategies in both domestic regulation and in international fora.

Enhancing maritime security, while maintaining the efficient flow of commerce, is a very large, complex and multi-faceted task, and this Committee's oversight of that effort is very appropriate. In my remarks this morning, I would like to address several different components of the overall maritime security objective, including enhanced ship security, port facility security, personnel security, and cargo security.

I. Ship Security

The Maritime Transportation Security Act instructs the Coast Guard to establish regulations requiring all vessels calling at U.S. ports to have vessel security plans. With an upcoming July 1 effective date, all vessels arriving at U.S. ports will have to be fully compliant with the new International Ship and Port Facility Security (ISPS) Code and the amendments to the International Convention for the Safety of Life at Sea (SOLAS). The Coast Guard deserves considerable credit for simultaneously and successfully partnering with domestic and international industry stakeholders, the International Maritime Organization and other governments, other Federal agencies and the U.S. Congress to accomplish this. The Coast Guard's approach to the implementation of the ISPS Code and SOLAS amendments, not only faithfully implements this new international regime that the Coast Guard played a key role in creating, but it enhances maritime security through the use of a consistent, uniform international approach for an industry, which operates within the jurisdictions of all the maritime trading nations of the world.

Vessels that are not compliant with the Code by the July 1 effective date will be denied entry to U.S. ports. The Coast Guard regulations will ensure that every vessel has an approved security plan, designated and trained personnel responsible for defined security actions and communications, procedures for communicating with ports and other vessels, procedures for monitoring and controlling physical security and access to the vessel, and the installation of Automated Identification Systems transponders.

While a substantial amount of work is being done to be compliant by July 1, our Member lines' representatives have identified no significant problems regarding lines' expectations that their vessels will be compliant by that time.

We would note that the new rules require most ships to have AIS transponders installed and operational by July 1,[1] but that Coast Guard receiving stations will not be operational by that time in a number of U.S. port regions, especially along the Atlantic and Gulf coasts. We believe that the Coast Guard should be given the resources to make a nationwide AIS system fully operational as soon as possible.

Finally, we note that while these vessel security plans will improve internal vessel security and preparedness as intended, they may be of little defense against an organized, external terrorist attack of a merchant vessel, such as the attacks on the *Limburg* or the *U.S.S. Cole.*

II. Port Security

The regulations established by the Coast Guard to implement the requirements of the Maritime Transportation Security Act and the ISPS Code also require port facilities to be compliant by July 1st. As with vessel security plans, compliance with these requirements may involve considerable effort, but, as with vessels, we are unaware of any U.S. container terminal that does not plan on being compliant by that date.

It would appear likely, however, that not all foreign port facilities will be compliant on July 1. This may be of particular concern in some developing countries. It seems clear that the U.S. will not stop trade with such countries in July; however, the issue is: How will ISPS compliant vessels be treated by the U.S. Coast Guard and other nations' maritime authorities when they arrive after having called during their voyage at a foreign port facility that does not have an ISPS compliant facility security plan? Vessels calling between such ports and the cargo on those vessels are caught in the middle. It is not yet clear what a vessel can expect in these situations.

Similarly, it is currently unclear what consequences shippers should expect for their cargo that passes through noncompliant facilities. For example, it is possible that Customs' Automated Targeting System may assign a higher security risk to cargo containers transiting through non-ISPS Code compliant facilities, and thus make it more likely such containers will be held up for inspection. While the government may be highly reluctant to stop trade with such countries, we expect it is likely to undertake measures designed to impose pressure on such ports and governments to comply, and those consequences may become more substantial as time

[1] All vessels larger than 50,000 gross tons are required to comply by July 1,2004. Vessels less than 50,000gt but larger than 300 gt must comply not later than the first safety survey, but not later than December 31.

passes and the government becomes less tolerant of foreign ports that are not compliant with the Code. In short, while we fully recognize that the U.S. and other ISPS Code compliant nations are likely to take actions that will affect carriers and shippers that move cargo through a non-compliant foreign port facility, and that such actions are likely to be designed to ensure, inter alia, that all parties strongly support efforts by all port facilities to become compliant as soon as possible, it is unclear at present how these situations will be addressed.

III. Personnel Security

The Transportation Security Administration is developing a Transport Worker Identification Card for all domestic transport workers in each transportation mode, which will require government background checks and biometric identifiers. This system will apply to shore-based, domestic maritime workers. It is unclear when this system will become operational, but several pilot projects are underway.

Regarding U.S. and foreign seafarers, the government has undertaken a number of changes.

First, it reviewed all U.S. seafarers and revoked the licenses of a number of persons who raised security questions.

Second, for foreign seafarers, effective last August, the use of crew list visas has been terminated. Each seafarer is required to obtain an individual visa from a U.S. embassy or consulate, and undergo a personal interview. If a seafarer does not have an individual visa, he will be unable to sign on or off the vessel in the U.S. or obtain shore privileges in the U.S., and the vessel operator may incur additional costs of posting guards at the vessel gangway.

Third, today information on all crew members is transmitted electronically to the Coast Guard 96 hours in advance of a vessel's arrival in a U.S. port, and is provided separately to Customs and Border Protection (CBP) and is screened through government information systems. Both agencies and the industry agree that there should be a "single window" for the advance electronic filing of such information that can be shared among government agencies. One of the positive manifestations of effective coordination within the new Department of Homeland Security is the recent agreement by the CBP and Coast Guard that the Coast Guard's electronic notice or arrival (e-NOA) system will soon be an acceptable "single window" system for this purpose and will be used by both agencies, thus eliminating duplicative filing requirements. We would like to commend Undersecretary Hutchinson, the Coast Guard and Customs and Border Protection for their continued efforts in this regard.

IV. Cargo Security

One of the most complex challenges is the enhancement of cargo security, especially containerized cargo. The vast majority of liner cargo is containerized—that is, it is carried in sealed metal containers from point of origin to destination. These containers come in standard sizes (typically 20', 40', and 45' in length) and may include various specialized technologies, such as refrigeration units for chilled and frozen foods, or internal hanger systems for carrying garments. Over 20 million TEUs (twenty foot equivalents) of containerized cargo are imported or exported through U.S. ports per year. Containers serve, in essence, as a packing crate and in-transit warehouse for virtually every type of general cargo moving in international commerce.

Physically inspecting every container is not practicable. Commerce would be severely disrupted.

A. Cargo Screening and the Automated Targeting System

As a result, Customs has developed and implemented a strategy to enhance the security of containerized cargo by:

- Requiring carriers to provide the agency with advance cargo manifest information for *every container* imported into the U.S. (or stowed aboard a vessel that calls at a U.S. port even though the cargo may be destined for a foreign country), 24 hours before vessel loading in a foreign port,
- Analyzing such information via the agency's Automated Targeting System (ATS),
- Inspecting any container about which ATS raised significant questions, and
- Developing close cooperative working relationships with the governments of our trading partners through the Container Security Initiative.

The ATS is thus a central feature in determining which containers get inspected and in the working relationships that Customs is establishing with other Federal agencies and with other trading nations' Customs administrations.

It is noteworthy that with international liner shipping, unlike the other transportation modes, the government strategy is to perform cargo security screening before the cargo is even loaded onto the transportation conveyance coming to the U.S. The "24 Hour Rule" has been implemented without major incident, and Customs has worked closely and cooperatively with industry to address those issues that have arisen. The Rule's importance is obvious to the security strategy described, and ocean carriers have supported Customs' strategic initiative and the Rule.

Today ATS is populated with carriers' cargo manifest or bill of lading data, and it utilizes other government data. A significant pending question is whether the current 14 cargo manifest data elements are sufficient for the security task at hand. Earlier this year the complexities of this issue became obvious in the context of Customs' Trade Act cargo documentation regulations. Customs amended the cargo manifest regulations' regarding who the carrier should name as the "shipper" on its bills of lading that are filed with the agency, out of a desire to capture information about the identity of an importer's "foreign vendor, supplier, manufacturer, or other similar party". This particular approach to obtaining such information presented serious problems.[2]

The agency recognized the problem that the regulations created, suspended enforcement of that portion of the regulations, and announced that it would work with the industry to review these issues. In short, it acted in a most professional and responsible manner. What remain to be addressed, however, are some hard issues. While it appears clear that information about importers' "vendors, suppliers, and manufacturers" is not appropriately obtained by trying to change who should appear as a "shipper" on a transportation contract—a bill of lading, it is not so readily apparent how such information is best obtained by Customs if it is to be used in the ATS for security screening before vessel loading in a foreign port.

Because this is an important issue that is likely to be addressed this year, I would like to offer some preliminary observations.

One should start by recalling the terms of the law. Section 343 of the Trade Act requires:

> "In general, *the requirement to provide particular information shall be imposed on the party most likely to have direct knowledge of that information.* Where requiring information from the party with direct knowledge of that information is not practicable, the regulation shall take into account how, under ordinary commercial practices, information is acquired by the party on which the requirement is imposed, and whether and how such party is able to verify the information."

In short, the information of interest—an importer's vendors, suppliers or manufacturers—is clearly information within the "direct knowledge" of the importer, not the carrier. In fact, the importer today provides this information to Customs in an existing Customs data system in the merchandise entry process. The difficulty is that this information is not currently filed before vessel loading in time to be useful to ATS.

When Customs wanted carriers' manifest information earlier than the formerly required time of vessel arrival at the U.S. port, the government established the 24 Hour Rule and required carriers to change their systems and processes to comply. The same logic might be applied by requiring shippers to provide Customs with their data before vessel loading. Although importers may not relish the idea of doing so, such a process is used for U.S. export cargo.

The threshold issue is whether Customs needs the information about an importer's suppliers and vendors before vessel loading in order for ATS to become more effective. There is in fact an over-arching and broader question that underlies this issue and the effort to make ATS as effective a cargo security screening system as possible, namely: *What* information does the government need, *from whom, when,* filed into what information system? Clarity and agreement on this difficult but fundamental question will be important to understanding what gaps exist, what the objectives are, and how we can all determine how best to make the continued progress.

The Trade Act regulations make it appear probable that shippers are going to be involved in measures to provide the government and the ATS more advance information about their cargo shipments before vessel loading. It is also apparent that carriers should not be made into conduits for transmitting to the government information they don't know, cannot verify, and could be penalized for if inaccurate.

---

[2] For a complete explanation of all the issues created by this proposal, the Council's petition that was submitted to Customs on February 2 can be found on the Council's website. *www.worldshipping.org.*

In addition to the language of the Trade Act, which indicates carriers should not be the parties filing this kind of information, there are other aspects of this issue that all sectors of the industry will need to consider. First, there is the issue of confidentiality. Do shippers want their supplier and vendor lists given to carriers, and filed in the public manifest system? Second, early carrier manifest filing requirements are becoming more prevalent with Customs administrations around the world. For example, Panama will soon be implementing an advance cargo manifest filing system very similar to U.S. Customs' system for every container transiting the Canal, regardless of whether Panama is the cargo's origin or destination. The measures taken here in the U.S. on this issue could easily become a precedent for other nations. Do shippers want their supplier and vendor lists broadly distributed via carrier manifests? Third, would such requirements apply to foreign-to-foreign cargo shipments that move on ships that call U.S. ports or are relayed in bond through U.S. ports? Because it is highly unlikely, for example, that a European importer of Latin American goods is going to supply the U.S. government with a list of its vendors and suppliers just because the ship calls at the Port of Miami, such a measure applied to such goods could have a substantial effect on vessel deployments, vessel calls at U.S. ports, and other service related issues.

In short, Customs has addressed the immediate problem that existed in the drafting of the existing Trade Act regulations, but the agency and the industry have yet to determine how the underlying issues will be addressed.

B. Container Inspections

Today, Customs uses the ATS system to screen 100 percent of all containers before they are loaded aboard a vessel bound for the U.S. It then has the ability to inspect, via physical de-vanning of a container or use of Non-Intrusive Inspection technology (gamma ray or X-ray), every container that raises a security question. As Customs has refined ATS, ocean container inspection rates have increased, from less than 2 percent before September 11 to 5.4 percent according to the most recent reports. That means that Customs is now inspecting almost 400,000 ocean containers a year. We expect container inspections are likely to continue to increase. We believe that a numerical objective, however, should not be the goal. The goal should be to inspect 100 percent of all containers that ATS says warrant inspection, plus some random process designed to monitor and verify the selectivity techniques being used.

How many of these inspections will be performed at U.S. ports and how many at CSI foreign ports of loading we cannot tell at this time.

Finally regarding container inspections, Customs has stated that its goal is to establish radiation-screening portals that will perform radiation screening on 100 percent of all containers transiting U.S. ports. The implementation of this will be challenging, including addressing the screening of containers that are loaded onto on-dock rail cars and do not pass through the terminal gate, but the goal is clear and appears logical. We also note that some foreign ports are undertaking similar measures to protect international commerce and that the Port of Rotterdam is implementing a similar radiation screening system.

C. Container Security Initiative

I began my testimony by discussing the Coast Guard's implementation of the new vessel and port facility security plan requirements, which the agency was instrumental in creating at the International Maritime Organization. The Coast Guard's strategy and its execution, as well as its communication and efforts working with the industry, have been excellent.

Customs, however, has not had the benefit of a comparable international regulatory organization to work with, so Commissioner Bonner and his organization have worked with Customs administrations in other trading nations to develop the Container Security Initiative—a set of bilateral agreements designed to foster closer cooperation and more effective security screening of international commerce. It is also significant that the Department of Homeland Security has reached an agreement with the European Commission that can promote trans-Atlantic cooperation and coordination of container security initiatives in conformity with the CSI approach and objective. We welcome this development. The importance of CSI should not be underestimated. Protecting international trade requires international cooperation, and the Council hopes that all participating governments will implement these CSI agreements effectively and cooperatively. Of the 38 CSI ports, 18 are currently operational.

CBP deserves a lot of credit for where it has taken this initiative, and while we recognize that many details of CSI have not been spelled out, we would urge the Committee to consider that the program is still in its developmental stage. Ocean

carriers are fully supportive of these initiatives. In the event governments need to respond to a terrorist event in this industry, it seems likely that trade would be irreparably harmed if CSI agreements are not operational and well implemented

D. Technology and "Smart" Containers

As discussed earlier, technology is being improved and deployed more extensively to enhance container security through non-intrusive container inspection technologies and through radiation detection.

Government and industry also continue to examine technology that may be appropriate for application to containers themselves. Operation Safe Commerce continues to fund projects reviewing such possibilities. Customs and the Department of Energy continue to review these issues, as do technology manufacturers, shippers and carriers.

The objective of this exercise is generally stated to be to make sure that containers are effectively sealed and that one can reliably detect if they have been tampered with in transit.

The "sealing" portion of this exercise does not really involve sophisticated technology. It requires shippers to seal a container immediately upon securely stuffing the box with a high security seal. Electronic seals (e-seals) do not provide any more security in this regard than a high security manual seal, but they may have a role in enabling a more efficient way to verify seal integrity.

Consideration of e-seals usually involves the application of Radio Frequency Identification (RFID) technology, and in fact many of the products and platforms being marketed as enhancing container security also rely on that technology. Recent announcements by the Department of Defense and major retailers concerning the usage of RFID tags on products have also spurred significant interest in the technology.

It is important to keep in mind, however, that no international standard exist today for the application of RFID-based e-seals or for active, read/write RFID tags. Nor has a clear and appropriate delineation been drawn between the possible usage of RFID technology to address container security requirements and the possible usage of that technology to address supply chain management objectives. These are not trivial issues. The issues, the challenges, and the requirements involved in addressing the two are not the same. The purposes and the use are not the same. The technology, operational and information implications are different. A failure to clearly distinguish between security requirements and commercial supply chain management objectives will create confusion; will impede progress on these issues; and may in fact create significant security vulnerabilities.

There is also the issue of selection of frequency or frequency bandwidth. It simply would make no sense to select a radio frequency for RFID platforms that is not publicly available in all major trading nations. And it would be of little value to the government and industry if the frequency that is eventually selected were deficient in terms of operational characteristics, such as requiring line of site to be read, producing false positives, etc.

The WSC is actively participating in International Standardization Organization (ISO) working groups tasked with developing standards for RFID e-seals and tags, and has submitted several papers to the ISO identifying user requirements for e-seals and a proposed framework for the optional usage of RFID e-seals and tags.

We have also presented this framework to CBP in response to its Request For Information (RFI) for "Smart and Secure Containers". We commend CBP for having reached out to affected parties to solicit their input in this first stage of what we hope will be a comprehensive and coordinated analysis of the issues involved in trying to identify technology's role in enhancing container security.

One of the more important and difficult issues in this regard is understanding and analyzing the information infrastructure and systems issues necessary to support a technology, whether it be RFID, wireless or satellite based, including:

- What information is generated, who is authorized to generate it, and is that information necessary for security purposes?
- Who collects the information?
- What supporting infrastructure the technology requires, where must it be located, and who operates it?
- Who has access to the information?
- What is done with the information?
- What actions are to be taken, by whom, with respect to the information?
- What are the costs of the technology and its use, and who incurs them?

- How does the technology affect the operations of shippers, carriers, and the relevant government agencies?

The deployment of any such technology would involve many international supply chains, international operating systems, the need for cooperation in other national jurisdictions, and substantial costs. Consequently, it is essential that government and industry analyze all the issues to be sure that appropriate and clearly understood requirements are being defined and met, and that the requirements and technology are not going to be replaced and the necessary capital wasted in efforts to implement technology that is really not the best approach to the issue.

Finally, there is the issue of how "sensors" might be applied to containers. Clarity will be needed on what should be sensed, and where. For example, is sensing more appropriately done at the port of loading through centrally operated sensing devices (as is done for radiation detection as discussed earlier) rather than equipping the world's 16 plus million sea containers with individual sensors, which might be disabled by a terrorist loading the container?

For devices installed on containers, there is also the issue of what kind of reading and information infrastructure is needed for these devices to work.

For example, some question RFID-based technology platforms for container security application because of their dependence on an array of ground based readers at multiple yet-to-be defined points in many facilities, in many different countries, controlled by many different parties. Increasingly such RFID skeptics are considering whether satellite and/or wireless technologies may be a potentially superior way than RFID-based technology to address security requirements as they are developed. We do not yet know the answer, but these issues need to be addressed before decisions are made on the deployment of technologies, which will have significant cost and operational implications for customs administrations, shippers, carriers, and terminal operators around the world.

In this regard, Undersecretary Hutchinson recently announced a significant and important change in the Department of Homeland Security. Responsibility for the issues of smart and secure container technology and systems has been moved from the Transportation Security Administration to the Border and Transportation Security Directorate, with Customs having a major role in implementation and with TSA having an advisory role. The BTS Directorate has also announced that it will soon be establishing a new consultative process with the industry to help consider and address the issues involved. It is not entirely clear at this time how the ongoing "smart" container analysis within Customs and within Operation Safe Commerce will be integrated into this process, but it presumably will be. We look forward to working with BTS, Customs and TSA on these issues and such a process.

E. Customs Trade Partnership Against Terrorism (C–TPAT)

Secure container loading is the starting point, and arguably the single, most important point, in the container security process. It is also the most difficult to address because it involves millions of containers being loaded and sealed at tens of thousands of different locations in every country in the world. An ocean carrier is like the postman; it receives a sealed container for transportation with all the necessary cargo documentation regarding the shipper, the consignee, and the cargo, but it has no first hand knowledge of what has been loaded inside. Unless the carrier is aware of information that arouses its suspicion about a particular container, it has little choice but to trust what shipping documents state is in the container and that the loading process was secure.

The Customs Trade Partnership Against Terrorism (C–TPAT) program is one way to try to effect improvements in this regard, but this is a substantial challenge. We expect that the Bureau of Customs and Border Protection (CBP or Customs) will continue to try to expand the voluntary C–TPAT program into an initiative that includes manufactures and suppliers outside the United States, and that it will continue its efforts to validate compliance.

F. Export Cargo Regulation

Later this year, the Census Bureau is expected to issue new regulations requiring U.S. exporters to file an electronic Shipper's Export Declaration (SED) for export vessel cargo directly to the government via the Automated Export System (AES) no later than 24 hours prior to vessel departure. Once those regulations are in place, a carrier may not load export cargo without first receiving from the U.S. exporter either the electronic SED filing confirmation number or an appropriate exemption statement. There are expected to be several exemptions from the advance SED export cargo filing requirement depending on the value of the shipment, the size and nature of the U.S. exporter, and possibly also the types of cargo.

G. Imported Food Security

The United States imports approximately $50 billion worth of food products per year. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 requires food facility registration and requires that prior notification of certain imported food be provided to the U.S. Food and Drug Administration (FDA) before its arrival in the United States. The implementing regulations require facilities throughout the world that produce or hold FDA-regulated food products shipped to the United States to register with the FDA and have a U.S. agent. Second, they require every FDA regulated food shipment to file detailed information about the product prior to its arrival in the United States, and they identify carriers as the parties through whom the government will stop cargo that is not compliant with the new rules.

This is a complicated and extensive new regulatory system that is being developed, and we would like to commend Customs and Border Protection for their extensive efforts to assist FDA in making these new regulations as workable as possible.

V. Contingency Planning

The Department of Homeland Security is now one year old, and is dealing with a very substantial number of issues. One of the issues that we hope will be high on the list of priorities for the Department is the unpleasant topic of contingency planning, or how would trade be allowed to continue in the event of a terrorist attack on the industry? The issue first requires clear, agreed and practiced role definition within and among the various U.S. government agencies. Second, it requires clear understandings and practiced scenarios with the governments of our trading partners who presumably will have just as significant an interest and need to address the continuation of commerce as the U.S. government. Third, the implementation of any response scenario would also involve substantial activity by the private sector—importers, exporters, carriers, brokers, terminal operators, and others. Having some kind of dialogue and road map of expectations and requirements would be very helpful to the private sector. The World Shipping Council's members are fully prepared to support and participate in any such endeavors.

VI. Conclusion

Mr. Chairman, the above is a brief description of the major security enhancement initiatives as they affect international liner shipping. While liner shipping is the largest component of our maritime commerce, it is important to recognize that there are many other maritime sectors that are not addressed herein, including the passenger cruise industry, the bulk and tanker shipping sector, the inland waterway industry, break-bulk cargo, and small vessels calling at small facilities. Each sector has its separate and distinct security challenges.

In the liner shipping sector, enhancing the security of America's commerce has, in many respects, brought carriers, shippers, intermediaries and government closer together in addressing a common threat and dilemma. Simply hoping you are not the victim cannot be the approach, because a successful terrorist attack would make us all victims. It would affect every supply chain, every carrier, every port, and every nation's trade and economy.

While trade and commerce, like many aspects of our society, remain vulnerable to premeditated criminal, terrorist activity, significant progress has been made in the last year to enhance the protection of international trade from the risk of terrorist attack. But this is a work in progress that must continue. Each of the initiatives discussed above, involving ships, port facilities, people, cargo security, cargo screening, inspection, and risk assessment capabilities is an important part of a multi-layered effort to enhance the security of international commerce. It is a complex and multi-faceted security infrastructure that is being built, but we now live in a world where it must be built, and all sectors of industry and all trading nations must work together to help create it.

We should also recognize that the security infrastructure we are trying to build to prevent terrorists from using or attacking international maritime trade needs to be robust enough to function as the security infrastructure that will be used to keep trade flowing in response to a transportation security incident.

The security infrastructure thus must not only be effective in design, but all the players' roles and responsibilities in that system should be clear. Ambiguity in the face of difficult questions is quite understandable, but it neither advances effective security, nor helps government or industry understand what it needs to do to adapt to meet these evolving needs.

We are making substantial progress in enhancing the security of international trade. The system is certainly more secure now than it was two years ago. It will be even more secure next year. We fully recognize that it is a difficult challenge,

and that industry and government must work closely together to meet the challenge. There are no good alternatives to open, constructive dialogue and the joint development of effective solutions to shared challenges. We would like to state for the record that the agencies responsible for maritime security, particularly the Coast Guard and Customs and Border Protection, have consistently worked closely with the industry in these efforts. The international liner shipping industry fully understands and supports working as closely as possible with the government to make commerce more secure in a way that is sustainable and does not unduly impede trade.

Senator BREAUX. Thank you, Mr. Koch.

Mr. Gary LaGrange, Gary, welcome, glad to have you here.

STATEMENT OF GARY P. LAGRANGE, EXECUTIVE DIRECTOR AND CEO, BOARD OF COMMISSIONERS, PORT OF NEW ORLEANS

Mr. LAGRANGE. Thank you, Mr. Chairman, it's a pleasure, indeed, and to all the other Members of the Committee.

And, Senator Nelson, I assure you, in Louisiana, at the Port of New Orleans, we share the same sentiments with you about Cortez and Limon and all of the other many Central American and Caribbean ports.

My first day on the job at the Port of New Orleans as CEO was September 10, 2001, and I can assure you that, on that day, when I showed up in New Orleans to take the job, security—port security, in particular—wasn't on the top 20 list of anything that we needed to accomplish. Since that time, all of our lives have changed in many respects and in many ways.

Senator Breaux, I was fortunate enough to sit in and to testify at a Committee hearing that you had at the Port of New Orleans early on in this venture. And since that time, I do have to admit much has happened. But not enough has happened, and that's for the simple reason that adequate wherewithal has not been provided, and we basically have been playing centerfield on one leg as best we can, and I think that's true from the top all the way down to the bottom.

The implementation aspects of things that we have—have occurred not so much from a Federal level, where we've received approximately $8 million in the first two rounds out of a need for $60 million identified in our vulnerability assessment; an assessment, which, by the way, was ongoing at the time of 9/11, copycatting the Florida Ports Council, if you will, who had done an excellent job in taking a leadership role of what to do and what to identify.

Where it has happened and where it has occurred is really in providing more of a coordinated role, more of a vigilant role, more of a role of being acknowledged and aware of what's going on around you. There have been a number of agencies, a number of groups that have been formed, which we participate in on a weekly basis. The United States Coast Guard Area Maritime Security Executive Committee, the Region 1 Area Security Initiative membership, the FBI Joint Anti-Terrorism Task Force membership, all of those groups meet at least on a twice-a-month basis, and we're actively involved with our 90-plus harbor policemen and our security department, and working in a coordinated vein with them.

As I said, much has happened; however, not enough has happened. The $8 million that we have received from the Federal level

is tantamount to receiving a tube of toothpaste, but no toothbrush. Basically, we have a situation where we've had four perimeter gates, as an example, to our new uptown docks and our new container terminal that's just been completed at a cost of $120 million, and those four gates, which were partially funded are absolutely meaningless to us at this point, because we, in essence, got the funds that we needed for approximately one third of each gate. One third of each gate just simply doesn't serve the purpose that we need.

Much of our activities are self-funded. Twenty-five percent of the Port of New Orleans budget now is dedicated strictly to maritime safety and security, anti-terrorism efforts. We've sent officers to anti-terrorism school in Georgia. They've come back. We've created an anti-terrorism division, which is performing quite well, within the port. But all of that is not without—it's not free. Five and a half million dollars a year has been added to our budget from an operational standpoint alone, as well as another million to a million and a half in operational expenses for equipment and so on and so forth on an annual basis.

Where does the money come from? It's not coming from the Federal Government. It comes from our ability to build future infrastructure that we need to placate the original meaning and idea of a port, to facilitate commerce and the movement of commerce. And in doing that, it's a significant part, much like Florida, at the Port of New Orleans, which is at the mouth of the Mississippi River, it serves 32 states. Sixty-two percent of the consumer-spending public in the United States is represented via the Mississippi River and its tributaries. Along with that, 62 percent of all grain exported out of the United States goes through the Port of New Orleans, and 19 percent of all petrochemical products that come into the United States come into the Port of New Orleans, on the import side.

Senator as you have mentioned and alluded to earlier, on Mardi Gras weekend, on February 21, Saturday morning, 6 a.m., in a fog-shrouded Mississippi River, there was a collision with a container ship coming in and an oil fuel supply boat on the outbound side. The supply boat cut across the bow, unfortunately, of the container vessel, immediately sank; and, unfortunately, five lives were lost in that collision.

That is something that possibly could have been prevented. I, for one, believe that it could have, with the completion of the VTS. That VTS system is in progress, and it's being completed, and only two radar sites remain to be completed with it; and, of course, all of affiliated tests that go hand-in-glove with it.

In the Mississippi River, over 5,000 ships a year come in to the river, and there are over 400,000 barge movements, which go hand-in-glove to placate the inland ports at Pittsburg and Louisville and Chicago and St. Louis and Memphis and Tulsa.

All of that said, 2 days after the river reopened, Secretary Ridge was in the Port of New Orleans office commemorating the first anniversary of him becoming Secretary of Homeland Security. And the question begged by the Secretary—that was only a small 140-foot vessel; what if it was a 3,000-passenger Conquest-size cruise ship instead? What would the ramifications have been? Or, better yet, as we gazed out of my office at the Crescent City Connection,

the bridge that connects—goes over the river in downtown New Orleans—what if some bird shows up and decides to bring these bridges down? What happens to the movement of commerce into inner-America, mid-America and up into the Northeast? Those are questions that are yet today unanswered, and I'm not sure that we really want the answer.

As I said, it's an integral role. We feel as though New Orleans is in an integral position. But so is every other port. The port director from Long Beach, California, just mentioned to me yesterday at a meeting, two private airplanes collided over the entrance to the Long Beach Harbor. Thank God it didn't stop traffic. Thank God it didn't stop the waterways and the movement of commerce. But at any given port anywhere—your port in Miami, Everglades, Canaveral, Tampa, any other them—you close that harbor, and you've shut off a significant amount of commerce to a lot of people.

Senator NELSON. [presiding]. The Skyline Bridge——

Mr. LAGRANGE. Yes, sir.

Senator NELSON.—over the mouth, coming into the Port of Tampa.

Mr. LAGRANGE. Exactly. How well we recall.

[The prepared statement of Mr. LaGrange follows:]

PREPARED STATEMENT OF GARY P. LAGRANGE, EXECUTIVE DIRECTOR AND CEO, BOARD OF COMMISSIONERS, PORT OF NEW ORLEANS

I want to thank Chairman McCain and Senator Hollings for calling this hearing and continuing to shed light on the issues of port security. I also would like to thank Senator John Breaux for his tireless support of the Port of New Orleans and the maritime industry throughout the United States. We will deeply miss Senator Breaux's advice and counsel when he leaves the Senate at the end of this year.

Since reporting to the Committee two years ago, the Port of New Orleans, along with many other U.S. ports, has made significant port security enhancements. The Port has accomplished all previously enumerated goals and objectives that could be undertaken administratively by its staff. The following security enhancement and/or regulatory compliance requirements have been completed:

- Increased Security to Heightened MARSEC/National Alert Levels
- Federal Grant Application Initiatives
- Federal Grant Project Award Management
- Port Vulnerability Assessment
- Harbor Police Department Anti-Terrorism WMD Manual
- Increased Cruise Terminal and Waterside Security
- U.S. Coast Guard Area Maritime Security Executive Committee Membership
- Region One Urban Area Security Initiative Membership
- FBI Joint Anti-Terrorism Task Force Membership
- Immigration and Customs Enforcement (ICE) "Operation Check Down" Initiatives
- MTSA Facility Security Plan
- Metal Detection Equipment Enhancements

The Port has completed or is in the process of completing necessary infrastructure enhancements with funding assistance made available by the Federal Government. The Port has dutifully absorbed all personnel, operations and maintenance costs related to security improvements, including overtime for heightened level alert periods. The impact of increased security costs on port authorities is significant and must be addressed. It is the primary reason that Federal funding assistance must not only be continued, but increased to meet the level of funding needed to address security concerns demonstrated by the Port Vulnerability Assessments completed by ports throughout the United States and submitted to the U.S. Coast Guard. These assessments document U.S. ports' numerous areas of weakness and, consequently, their susceptibility to criminal and terrorist activities. The preparation, distribution

and review of these assessments, albeit as protected SSI (Security Sensitive Information) documents, may actually result in increased port vulnerability, if the steps required to mitigate identified weaknesses are not taken within a "reasonable" period of time. Therefore, Congress and the Bush Administration should act immediately to provide funding at levels sufficient to enable port authorities to meet the increased financial burden associated with increased security costs as well as the mandates of the Maritime Transportation Security Administration which become applicable on July 1, 2004.

As stated, during the past two years, the Port of New Orleans has accomplished many of the goals listed in its previous report. To date, the Port has applied for more than $33 million in Federal grant funding. The following awards have been received

TSA I	Upriver Gate Access	$3.5 million	Project ongoing
TSA I	Cruise Terminal Fencing	$184,450	Project completed
TSA II	Cruise Terminal Lighting/Monitoring	$600,000	Project ongoing
TSA II	Signs, barricades, barriers	$50,000	Project ongoing
TSA II	Metal detectors	$15,000	Project completed
DHS	Upriver Perimeter Enhancements	$3.4 million	Project ongoing
DOJ/Tech.	Video Teleconferencing	$52,000	Project completed
DOJ/COPS	Hiring Grant	$212,351	3 Officers over 3 years
DOJ/COPS	Overtime Grant	$37,500 Req.	-0- Award
TSA II	8 Projects	$5.5 mil. Req.	-0- Award

The Port of New Orleans anticipates contributing matching funding for these projects totaling approximately $1.2 million. (This is in addition to an annual Safety and Security Division operating budget of $ 5.5 million and a capital equipment budget of $275,000.) The Port intends to apply for additional funding through the Round III Federal grant initiative. However, the President's proposed Fiscal Year 2005 budget of $46 million for port grant funding is not sufficient to meet port security funding requirements. It is worth noting, that this figure represents a significant reduction in available grant funding because infrastructure improvements or new construction projects, which were included in previous rounds, are now listed as "ineligible" in the Round III guidelines. Nearly $5.4 million in security enhancements were not funded in the Port's previous grant application. This amount alone comprises eight percent of the President's proposed budget. None of the grant projects included in Round III attempts to address the prohibitive costs of providing infrastructure improvements and associated equipment, maintenance and staffing costs (as opposed to installation or replacement enhancements) which result directly from elevated security requirements.

The American Association of Port Authorities estimates that $400 million in funding is called for in FY '05. The latest U.S. Coast Guard forecast estimates the cost for total MTSA compliance to be $1.125 billion for the first year and $5.4 billion over the next 10 years.

Numerous administrative or procedural MTSA mandates must also be addressed and clarified. The most glaring example is the TWIC (Transportation Worker Identification Card) concept for ports. Information concerning the status of the TWIC initiative is all too often illusive, sketchy and most of all inconsistent. The Port of New Orleans, like many ports, has deferred initiating a card access project because the "start-up" (staffing for processing, distribution, enforcement and administration); equipment; and software costs are extremely high and this is without the assistance of a paid consultant. A recent article in the Winter, 2004, *Port Illustrated* discusses the TWIC pilot program in Wilmington, Delaware. The pilot program began in July, 2003, and is scheduled to run for 15 months, extending beyond the July, 2004, MTSA compliance deadline, and leaving ports without firm guidelines. To date, no directives or guidelines which address the need or requirement for a biometric component of TWIC have been issued. As a result, ports will be forced to purchase more expensive card access systems which will be able to accommodate features which, ultimately, may not even be required.

The Port of New Orleans will submit a grant application for all eligible unfunded security initiatives, ranging from training and exercises to communication system upgrades and patrol vessels used to supplement Coast Guard patrols and response. The price tag for these initiatives is currently being estimated at approximately $50 million dollars.

Port executives remain committed to securing additional funding for security initiatives from both self-generated revenues and Federal funding sources. Now, more than ever, port executives truly understand that the safety and security of our Nation's waterways will forever be a paramount component of port operations.

The vessel collision that occurred at the mouth of the Mississippi River on February 21 of this year provides a poignant example of the potential economic havoc that could be visited upon this Nation by a terrorist act. In this unfortunate inci-

dent, the sinking of a relatively small vessel in the busy Southwest Pass resulted in a four-day closure of the main international shipping channel into the Mississippi River and the delay of 158 ocean-going vessels. The closure was absolutely necessary to conduct search and rescue and recovery operations followed by removal of the vessel. Our thoughts go out the families of the five seamen who lost their lives.

After removal of the sunken vessel, the backlog of ship traffic was cleared and shipping returned to normal within three and a half days. Estimates are that this incident caused approximately $17 million in direct losses and $68 million in overall negative economic impacts. Not only were ships delayed, but three container cargo ships and three cruise vessels had to be diverted to other ports. Thousands of passengers were bussed to other Gulf Coast ports which were ill-equipped to handle them on such short notice. The cruise lines incurred thousands of dollars in ground transportation costs and reimbursements to passengers for the loss of their vacations.

With more than 5,000 ocean-going vessel calls on the Mississippi River annually, the importance of this waterway system to the Nation's economy is readily apparent. The nation's economy would experience severe consequences from a prolonged closure of the Mississippi River to deep draft navigation. In 2002, the ports of the Lower Mississippi River from the Gulf of Mexico to Baton Rouge handled 227 million tons of foreign waterborne commerce valued at nearly $40 billion and representing 18.1 percent of the Nation's international waterborne commerce. American producers exported 27 percent of total U.S. exports out of lower Mississippi River ports.

Included in this total are agricultural products from 17 midwestern states exported from the 10 grain elevators located on the lower Mississippi River, making up more than 62 percent of total U.S. Grain Exports. More than 92 million tons of petroleum and petroleum products are imported to Louisiana facilities on the Mississippi River system, comprising nearly 16 percent of all U.S. waterborne imports of petroleum and related products.

This collision and its consequences clearly demonstrates the need for the timely completion of all elements of the of the Vessel Traffic Service (VTS) on the lower Mississippi River to facilitate safe and secure vessel operations. Ports and industries along the lower Mississippi are poised to reap the considerable benefits of the new state-of-the-art VTS being implemented by the U.S. Coast Guard. All facets of the maritime community have been involved in this unprecedented multi-year cooperative venture with the Coast Guard. The system, for the most part, is up and running on a test basis out of the Coast Guard's Vessel Traffic Center on the river front in New Orleans. Two more radar sites must be installed and the system must be subjected to formal testing procedures, involving both the computer simulation and real world tests with a large number of vessels on the waterway equipped with VTS transponders.

VTS New Orleans will enhance both safety and security of the largest port complex in the world. The Coast Guard will be able to identify and track the movements of all ocean-going vessels and most other commercial vessels moving on the lower Mississippi. Tracking will begin prior to a ship's entrance to the river and will extend up river beyond the limit of deep draft navigation at Baton Rouge. Mariners will be given a powerful new tool to assist safe navigation in the busiest waterway in the Nation. Existing radar only provides a very limited view of the river and is particularly hampered by the river's twists and turns. Mariners depend on extensive use of radio communication with other vessels to determine navigation conditions, but radio communication, as seen in the recent vessel collision, is not always reliable. VTS will provide a detailed, real-time picture of vessel movements on the waterway, including vessel identification, as well as provide a method for communicating waterway conditions and special alerts to all mariners. VTS will not be blinded by bends in the river or by fog or darkness.

We have to thank the Coast Guard for its perseverance in bringing VTS to our ports and waterways, and Louisiana Senator John Breaux for his tireless championing of VTS, especially for his insistence on expediting VTS carriage requirements for vessels. A final notable attribute of VTS is that as currently programmed it comes at no cost to the Port. The Port's emergency response vessel, which assists the U.S. Guard and responds to every level of waterway emergency and service, is scheduled to be have the system installed at no cost to the Board.

In conclusion, now is not the time for Congress to lose its zeal in the war against terrorism on the domestic front. Extending the deadline for compliance with security measures without providing necessary additional funding is not the answer. The nation's ports, like its airports, simply cannot by themselves bear the financial burden of added security costs, especially during these volatile economic times. From the beginning of this regulatory process, port executives have pleaded that no security

mandates be issued without the proper funding. The mandates are here. Please ensure that adequate funding is too.

Senator NELSON. Thank you, Mr. LaGrange.
Mr. LAGRANGE. Thank you, sir.
Senator NELSON. Dr. Carafano?

STATEMENT OF DR. JAMES JAY CARAFANO, SENIOR RESEARCH FELLOW, DEFENSE AND HOMELAND SECURITY, THE HERITAGE FOUNDATION

Dr. CARAFANO. Thank you. I have a lengthy statement, which I've submitted for the record, which I'd just like to briefly summarize.

The Heritage perspective of our research agenda is to always look at the strategic problem, because we think this is going to be a long, protracted war. And I actually think we could take a lesson from the Cold War here. You need the same kind of strategy, and it's got to have three parts, and you have to have offense and defense—one, because, you know, you've got to take the initiative; two, the bad guys are always going to get through, so you have to deal with the leakers. But, at the same time, you have to continue to grow the economy. And so if you have a strategy that doesn't promote economic growth, then you have a failed strategy, because that's what enables you to endure and win in a protracted conflict while you ride the other guy into history. And the third is, you have to protect civil liberties and privacy at the same time, because that's the foundation of stability of the country. And, in essence, that's what you're fighting for.

And our agenda says, basically, our research looks at it, and if you don't have a solution, a security solution that does all three—security, economic growth, and protect civil liberties and privacy—then you have the wrong answer. Go back and start over.

And so with that in mind, what I tried to do was to briefly look at the different efforts in the maritime security area, up against the national security strategy, and look and see where there were questions, concerns, or problems that I wanted to highlight to the Committee.

Before I do that—by definition, these are negative kind of comments, because I'm looking for gaps and holes. And I don't want to belittle or neglect the great work that DHS has done. I think they've made remarkable progress in the last year. I think the guys on the ground are terrific. I mean, in all the ports I've been to—I was in Miami recently, and I walked the line at the cruise-ship terminal with a young Coast Guard officer, and every place you went, every person that we talked to, no matter what their badge was, no matter what patch they had on their shoulder, he knew every one of those guys by their first name. And it's clear that on that pier, those people are working together and cooperating and are concerned about security.

And I'd also—I think—don't think we can neglect the great work that this Committee has done. I think the MTSA act has been a great foundation for establishing a homeland security program.

I'd just like to very briefly highlight some of the points that I identify in the testimony. One of the components in the MTSA act was a requirement for—within the Department of Transportation,

to examine and certify a means of providing secure commerce and transport. That doesn't necessarily mean regulatory means. It could be alternatives to the structure that we have with CSI and C–TPAT and these other things. And that's not to say that they're bad, but I think that we ought to have something in the Department that's looking at alternative ways for—to secure intermodal transportation.

First of all, it's going to take years for the whole CSI system to be put in place. And even then, we don't really know if it's going to work. Second is, you know, we're not—there's no—we have no confidence that regulatory systems are going to keep up with economic and technological developments. Other people could come up with better, faster, and cheaper ways to do this. And, third, I think we really have to think about the day that something catastrophic does happen, because we'll do exactly what we did with the airlines; we'll close every port in the United States down, and commerce will grind to halt. And if we don't have plans and programs and public/private plans in place to figure out how we can get Wal-Mart goods going again, not just to get the economy rolling, but to get people the confidence that this Nation is still going on, then we're going to have a problem. So I do think that we need to look at alternatives for secure intermodal security that the private sector could propose, that DHS could validate, and that could either be used or put on the shelf for times of emergency.

Another area that we need to look at is law enforcement. How can we buildup law enforcement capacity in the maritime domain? And just one issue I'd like to point out very quickly is some great initiatives in the Coast Guard. Sea marshal program, great initiative. Also, if you look at their Maritime Security Office, they've done a lot more, in terms of using their investigators for counterterrorism and security issues. But, in either case, they have human capital programs. There aren't development programs, there aren't ways to grow and maintain these people. And there's no plan on how they really integrate with the other law enforcement activities in DHS. You know, for example, for a maritime security officer—investigative officer, you have to be in place 20 months. But you don't have to be an investigator for 20 months; you could be a safety officer for 19 months, and an investigator for one. Only 5 percent of the investigators do a follow-on assignment, so all the expertise that they gain is really lost. So I do think that there is work to be done, in terms of looking at the law enforcement capacity that we have available in the maritime realm, and how we could expand that.

Another area is unity of effort at the ports. The port captain, the port authority director, and the Customs enforcement person all have clear responsibilities. In most of these ports, they all have different command posts, so I'm not really sure how we have unity of effort. I'm not really sure we have a plan that really looks at, Do we need to bring these guys into one command post? Do we need to have redundant command posts? Do we need to have virtual command posts? And have we really looked at how we could enhance that?

And the final point I'd just like to make is on organization. I mean, when we created Department of Defense, what became the

Department of Defense in 1947, I mean, everybody knew we weren't going to get it right. You know, we went back in 1949, and we passed a law that kind of cleaned up the bill—the Department a bit. We missed some of the hard issues, like jointness. And it only took us 50 years to get it right after that. I think everybody should have an expectation that we need to go back at some point and rethink the Department of Homeland Security and see if we really have it right. And I think the area of maritime security is clearly one that should be looked at.

I mean, one of the issues that I've found is, one of the reasons why I think the pieces all don't quite come together, is, we don't really have a true national maritime security strategy. And you need a national strategy to really help you make the hard choices. Do I need to put more money into the port security grants, or is that money better spent on Deepwater? And I don't think it's—unless we have that, that we really can move forward in a very proactive and systematic way.

And to the question of—we have TSA, we have ICE, we have Coast Guard and Department of Defense. All potentially have a big role here. Do we really have the roles and missions right? Do we really have somebody who we can put our finger on and just say, "You're in charge of making this happen?" That's a tough thing, but I think that eventually that's an issue we need to go back and revisit.

Thank you.

[The prepared statement of Mr. Carafano follows:]

PREPARED STATEMENT OF DR. JAMES JAY CARAFANO, SENIOR RESEARCH FELLOW, THE HERITAGE FOUNDATION

Mr. Chairman and other distinguished Members, I am honored to testify before the Committee today.[1] Appraising the status of national efforts to enhance maritime security is a vitally important task. In my testimony, I would like to assess the progress that has been made in each of the areas related to implementing the national homeland security strategy, examine organizational issues that will affect the long-term development of a national maritime security regime, and reconsider the need for standards and metrics to evaluate preparedness and guide future efforts and investments.

The Challenge—Consequences, Size, and Scope

There are three reasons why the subject of maritime security requires national attention.

- *First,* the importance and vulnerability of the maritime domain cannot be overestimated. As you well know, 95 percent of U.S. overseas trade traffics the mar-

[1] The Heritage Foundation is a public policy, research, and educational organization operating under Section 501(C)(3). It is privately supported, and receives no funds from any government at any level, nor does it perform any government or other contract work. The Heritage Foundation is the most broadly supported think tank in the United States. During 2003, it had more than 200,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2003 income came from the following sources:

Individuals 52%
Foundations 19%
Corporations 8%
Investment Income 18%
Publication Sales and Other 3%

The top five corporate givers provided The Heritage Foundation with 5 percent of its 2003 income. The Heritage Foundation's books are audited annually by the national accounting firm of Deloitte & Touche. A list of major donors is available from The Heritage Foundation upon request. Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own, and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

itime domain. In addition, many major population centers and critical infrastructure are in proximity to U.S. ports or accessible by waterways. Maritime security also has a critical national security dimension.[2] The economic, physical, and psychological damage that might result from a significant terrorist attack targeting maritime commerce or exploiting America's vulnerability to strikes from the sea[3] is difficult to estimate. The September 11 terrorist attack on New York incurred well over $100 billion in losses to the U.S. economy alone.[4] Given the Nation's overwhelming dependence on ocean-going commerce, a similar sudden, unexpected attack in the maritime domain might easily exceed these costs. The United States lacks sufficient means to respond to maritime attacks with catastrophic consequences.

- *Second,* the size of the maritime security challenge is as daunting as the terrible consequences of a serious attack. The figures often cited are well-rehearsed: maritime security involves hundreds of ports, thousands of miles of coastline, tens-of-thousands of commercial and private craft, and millions of shipping containers. Even these figures, however, do not describe the magnitude of the maritime domain, which is truly global in nature, encompassing every ocean and the peoples and property of many nations.[5] Current initiatives, even when fully implemented, may be inadequate to address the global challenges of maritime security.
- *Third,* maritime security is truly a complex strategic problem encompassing a physical domain, land-based critical infrastructure, intermodal means of transportation, and international supply chains that covey goods, services, and passengers. The National Strategy for Homeland Security, issued by the Bush Administration in July 2002, identified six critical mission areas. These areas were established to focus Federal efforts on the strategy's objectives of preventing terrorist attacks, reducing America's vulnerabilities to terrorism, and minimizing the damage and recovering from attacks that do occur. The components of maritime security cut across each of these functions.[6] Only a strategic solution can provide the comprehensive regime required to address such a complex strategic problem. The United States still lacks such an adequate, overarching approach to the challenges of maritime security.

While these challenges are indeed daunting, I would like to start off by commending Secretary Ridge and the entire Department of Homeland Security (DHS) on the work that has been done over the last year in the area of maritime security. The war on terrorism is likely to be a long, protracted conflict, and the DHS has the difficult task of being on watch right now against possible terrorist threats and

---

[2] The overwhelming bulk of American military power is still moved around the world by ship. Most military supplies and hardware move through only 17 seaports. Only four of these ports are designated specifically for the shipment of arms, ammunition, and military units through DOD-owned facilities. For an overview of the military's reliance on ports and associated security risks, see U.S. General Accounting Office, "Combating Terrorism: Preliminary Observations on Weaknesses in Force Protection for DOD Deployments Through Domestic Seaports," GAO–02–955TNI, July 23, 2002. See also U.S. General Accounting Office, "Combating Terrorism: Actions Needed to Improve Force Protection for DOD Deployments Through Domestic Seaports," GAO–03–15, October 2002, pp. 5–10.

[3] For a discussion of threats, see James Jay Carafano, "Budgets and Threats: An Analysis of Strategic Priorities for Maritime Security," Heritage Foundation *Lecture* No. 791, June 16, 2003, at *www.heritage.org/Research/HomelandDefense/HL791.cfm.*

[4] Estimates of the damage wrought by the 9/11 attack vary depending on the criteria used. Insurance Information Institute set the initial cost at $40 billion. Insurance Information Institute, *Catastrophes-Insurance Issues-Part 1 of 2,* January 9, 2002, np. A study by the Federal Reserve Bank of New York put the cost at $33–36 billion. The Federal Reserve Bank's estimate included only immediate earning loses, property damage, and clean-up and restoration costs through June 2002 and did not cover long-term productivity and tax revenue losses. Jason Bram, *et al.,* "Measuring the Effects of the September 11 Attack on New York City," *FRBNY Economic Policy Review,* Vol. 8, No. 2(November 2002), p. 5. The City of New York Comptroller set the total economic impact on the city at between $82.8 and $94 billion. Comptroller, City of New York, *One Year Later: The Fiscal Impact of 9/11 on New York City* (New York: City of New York, September 4, 2002), p. 1. The U.S. General Accounting Office reported that it believed the most accurate assessment places the total direct and indirect costs at $83 billion. U.S. General Accounting Office, *Impact of Terrorist Attacks on the World Trade Center,* GAO–02–7000R, May 29, 2002, p. 2. In addition, Wilbur Smith Associates estimated the long-term costs of the 9/11 attacks resulting from reduced commercial aviation range from $68.3 to 90.2 billion. Wilbur Smith Associates, "The Economic Impact of Civil Aviation on the U.S. Economy—Update 2000," (2002).

[5] See, for example, Daniel Y. Coulter, "Globalization of Maritime Commerce: The Rise of Hub Ports," *Globalization and Maritime Power,* ed. Sam. J. Tangredi (Washington, D.C.: National Defense University Press, 2002), pp. 133–142.

[6] White House, National Strategy for Homeland Security, 2002, pp. 15–46.

building a robust homeland security system that must stand for decades. While the Nation's current maritime security regime is inadequate to meet long-term U.S. strategic needs, it represents a significant improvement over the pre-9/11 state of preparedness. The DHS has achieved a lot given the short time frame of its existence and the magnitude of the task it faces. Likewise, Congress has performed yeoman's service as well. The Maritime Security Act (MTSA) of 2002 produced major changes in the Nation's approach to maritime security and, I believe, provided much of the legislative foundation required to implement robust national programs. But, there is more work to be accomplished. Rather than dwelling on what has been done well, I believe it is more important to focus on what can be done better.

A Strategic Assessment

One of the most important actions taken by President Bush's administration in the wake of the September 11 attacks on New York City and Washington was establishing a national homeland security strategy. In turn, the strategy defined the six critical missions required to protect U.S. citizens from transnational terrorism. I would like to review each in turn, highlighting where cautions or questions are in order.

Intelligence and Early Warning. The first critical mission area is intelligence and early warning. It includes activities related to detecting terrorists and disseminating threat information and warning. It is widely recognized that promoting intelligence sharing across the public and private sectors is the greatest challenge in this critical mission area. Effective intelligence sharing is a prerequisite for exploiting the full potential of national capabilities to respond to potential terrorist threats.[7] The emerging national maritime system certainly faces this challenge. However, intelligence and early warning in the maritime domain faces an additional obstacle. The United States lacks adequate situational awareness of activities in U.S. coastal waters and waterways.

While the U.S. Coast Guard recognized the critical importance of maritime domain awareness even before the 9/11 attacks,[8] current plans for enhancing domain have matured little. For example, the Vessel Traffic Service (VTS) was established in 1972 to improve navigation safety by organizing the flow of commercial maritime traffic. There are 10 VTS areas scattered throughout the United States. These provide limited coverage of the maritime domain. In 1996, Congress required the Coast Guard to reassess future VTS requirements. This initiative resulted in the development of the Ports and Waterways Safety System (PAWSS), which is now in the process of being employed. MTSA requires most large commercial craft and vessels on international voyages to have Automatic Identification System (AIS) tracking devices that will be monitored by PAWSS. PAWSS–VTS is intended to automatically collect, process, and disseminate information on the movement and location of ships in ports and on waterways using a network of radars and onboard ship transponders.

Unlike the U.S. air traffic control system, PAWSS–VTS will never be able to provide a complete picture of traffic in the maritime domain. PAWSS–VTS faces three major drawbacks. First, it will not be a national system. According to a report by the General Accounting Office, as currently envisioned, "for the foreseeable future, the system will be available in less than half of the 25 busiest U.S. ports."[9] Second, PAWSS–VTS was intended to support maritime safety and environmental protection missions, and has been pressed into service to support homeland security responsibilities. In this regard, PAWSS–VTS will be inadequate to meet emerging security threats. It will, for example, be of virtually no use in providing early warning of small boat threats such as the craft used to attack the USS *Cole* in October 2000

---

[7] Among the recent initiatives by the DHS to improve information sharing is the announcement of the establishment of the Homeland Security Information Network (HSIN). HSIN will link states, territories, and major urban areas to the Homeland Security Operations Center through the Joint Regional Information Exchange System (JRIES). Initially, the system will be limited to sensitive-but-unclassified information, but in the future it is intended to carry secret information to the state level. A collaborative tool such as HSIN is essential for effective information sharing. Extending HSIN to major ports within the United States as a priority might significantly speed efforts to enhance public-private information sharing in the maritime domain. For a discussion of major challenges in intelligence sharing see, James Jay Carafano, "The Homeland Security Budget Request for FY 2005: Assessments and Proposals," Heritage Foundation *Backgrounder* No. 1731, March 5, 2004, at *www.heritage.org/Research/Homeland Defense/bg1731.cfm.*

[8] Bruce B. Stubbs, "The Coast Guard and Maritime Security," *Joint Force Quarterly,* No. 26 (Autumn 2000), pp. 95–99.

[9] U.S. General Accounting Office, "Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, But Concerns Remain," GAO–03–1155T, September 9, 2003, p. 7.

or large commercial vessels that might be hijacked or converted into covert weapons carriers. Third, PAWSS–VTS does not provide coverage "between the ports." Terrorists could well mimic tactics of drug smugglers and employ non-commercial vehicles such as small, fast, private boats with concealed compartments capable of storing 30–70 kilograms of material.[10]

Currently, the DHS has only two, very expensive and unattractive options for significantly expanding maritime domain awareness. It can direct additional investments in the land-based equipment and other infrastructures required to expand PAWSS–VTS and require additional craft to carry AIS tracking equipment, or it can rely on the surface and aviation assets of the U.S. armed forces (including the Coast Guard and the U.S. Navy) to cover the large remaining gaps. Neither option appears particularly cost-effective nor sufficiently useful or flexible to ensure preparedness in a protracted conflict against an unpredictable foe.

Proposals to create a maritime-NORAD, might offer the basis for developing more practical alternatives.[11] Such an approach would probably require three elements to produce more promising alternatives to the long-term challenge of enhancing maritime domain awareness: (1) joint cooperation between the Department of Defense (DOD) and the DHS both in research and development and operational monitoring of U.S. waters, (2) close cooperation of the United States' northern and southern neighbors, (3) new and innovative technical solutions.

Border and Transportation Security. Protecting border and transportation systems includes managing the border and ports of entry, ensuring aviation and maritime security, and developing guidelines and programs for protecting national transportation systems. The key principle guiding Federal investments in this area should be ensuring the adoption of a layered security system: a combination of effective, mutually supporting initiatives that simultaneously provide useful counterterrorism measures, protect civil liberties, and do not encumber the flow of travel and commerce.

Unlike many strategic challenges, overall, adequacy of resources for implementing new initiatives is not the most significant challenge in this critical mission area. Funding for the DHS role in one layer of the maritime component of border and transportation security, however, is an issue of major concern. In particular, the appropriation for the U.S. Coast Guard's Integrated Deepwater acquisition program—long-term modernization effort to recapitalize the service's fleet of cutters, aircraft, sensors, and command and control—is inadequate.

The Coast Guard's fleet is old, expensive to operate and maintain, and poorly suited for some homeland security missions.[12] Deepwater was to be funded at $330 million (in 1998 dollars) in the first year and $530 million (in constant dollars) per year in the following budgets, but no annual budget before FY 2004 matched the required rate of investment. Meanwhile, the Coast Guard's increased operational tempo and expanded mission requirements since 9/11 have been wearing out the fleet faster than anticipated, putting the modernization program even farther behind schedule.

In the Administration's FY 2005 budget, Deepwater would receive $678 million, an increase of $10 million.[13] This level of funding is totally inadequate to support rapidly building up an essential component of the Nation's homeland security system. Dramatically increasing the budget for Deepwater would not only establish the capabilities needed for a long-term security system sooner, but also garner significant savings (perhaps as much as $4 billion) in lower procurement costs.[14] Reducing life-cycle expenses by retiring older and less capable systems would realize additional savings.

While funding should be expanded there are aspects of the Deepwater program that should perhaps be revisited in light of how the U.S. maritime security structure has evolved since September 11. Among the issues that might be reconsidered is whether coordination of requirements and leveraging of research and development between the Coast Guard and the U.S. Navy's littoral combat ship (LCS) program

---

[10] *Measuring the Deterrent Effect of Enforcement Operations on Drug Smuggling,* p. 1.

[11] James Jay Carafano, "Shaping the Future of Northern Command," CSBA *Backgrounder,* April 29, 2003, at *www.csbaonline.org/4Publications/Archive/B.20030429.NORTHCOM/B.20030429.NORTHCOM.pdf.*

[12] Ronald O'Rourke, "Homeland Security: Coast Guard Operations—Background and Issues for Congress," Congressional Research Service, RS21125, November 22, 2002, p. CTS–2, and Independent Assessment of the United States Coast Guard, "Integrated Deepwater System," Acquisition Solutions *Issue Brief,* July 14, 2001, p. 6.

[13] U.S. Department of Homeland Security, "Budget in Brief: FY 2005," February 2004, p. 33.

[14] See the recommendations for the costs and benefits on accelerating the Deepwater program in U.S. Coast Guard, "Report to Congress on the Feasibility of Accelerating the Integrated Deepwater System," at *govt-aff.senate.gov/presslinks/031203cgreport.pdf.*

is adequate and properly synchronized.[15] Likewise, both programs should be assessed to see if they provide an adequate set of capabilities to respond to the small boat threat. Currently, the United States simply lacks an adequate capability to deal with an attack similar to the strike on the USS *Cole* (In particular, it is unclear if they have sufficiently exploited emerging non-lethal technologies that might be available). Additionally, it is not clear that short-range unmanned aerial vehicle (UAV) and manned aviation requirements of the Navy, Coast Guard, and Immigration and Customs Enforcement Air and Maritime Operations have been adequately rationalized.[16]

Another issue that might be addressed is the requirement for Deepwater systems to provide security on the waterside of the ports. Most security plans acknowledge that security on the landside of port facilities is the responsibility of the port. There is often, however, an assumption that security of the water around the port should be the responsibility of the U.S. Coast Guard. While the Coast Guard has traditionally had responsibility for protecting defense-related port facilities, particularly during times of war, it is not clear that service assets should be the primary responders to security incidents in proximity to the ports. Over the long term, it might be more effective if close-in security needs are met by local port authorities[17] and Deepwater assets were focused to an even greater degree on extending depth and redundancy in the U.S. maritime security zone.

In contrast to funding for Deepwater, other initiatives in the border and transportation area are programmed to receive significant additional funding. However, of concern here is whether, even with adequate funding, they will provide the redundancy and overlapping security required for an effective layered defense system. Of principal concern are the initiatives intended to secure the supply chain that crosses the maritime domain including the CSI—Container Security Initiative (a program designed to target high-risk cargo for additional screening); CTPAT—the Customs-Trade Partnership Against Terrorism (an initiative for encouraging the private sector to enhance supply-chain security); ACE—the Automated Commercial Environment (which will facilitate Customs oversight of lawful international commerce by streamlining data entry and information exchange between Customs and the trade community and facilitate cargo inspections and clearances); the inspection teams and technologies employed in domestic and foreign ports to screen high-risk cargo; and the shipping and port security measures mandated in MTSA and the International Maritime Organization's International Shipping and Port Security Standards (ISPS). While all these initiatives are worthwhile, each addresses only a portion of the challenge of providing security of maritime commerce and interdicting terrorist threats before they reach their intended targets. We will only know if they actually provide comprehensive security once they are all up and running in concert and appropriate metrics are developed to measure their effectiveness. This effort will take years and in the end may not prove effective. Nor is it clear these initiatives will be flexible enough to keep with the rapid changes demands and technological innovations of the 21st century marketplace.

It may not be strategically prudent to pursue the current combination of measures alone. Layered security, after all requires not placing all the eggs in "one security basket." The MTSA required the Secretary of Transportation to establish a program to evaluate and certify secure systems of intermodal transportation. It did not direct that these programs would have to necessarily be conceived or implemented by the Federal Government. In order to reduce risk, as well as exploit the capacity of the marketplace to create innovative and effective solutions, the DHS might consider establishing mechanisms to allow the private sector to develop and implement its own alternatives to the CSI/CTPAT regime.

Domestic Counterterrorism. This mission area comprises law enforcement efforts—principally by the FBI and U.S. Immigration and Customs Enforcement (ICE)—to identify, thwart, and prosecute terrorists. The guiding principle for enhancing this critical mission area should be adopting programs that expand the capacity to conduct counterterrorism operations without impinging on civil liberties or detracting from other law enforcement priorities.

---

[15] For issues related to LCS development, see Robert O. Work, "Naval Transformation and the Littoral Combat Ship," Center for Strategic and Budgetary Assessments, February 2004, pp. 129–153, at *www.csbaonline.org/4Publications/Archive/R.20040218.LCS/R.20040218.LCS.pdf.*

[16] Bruce B. Stubbs, "Fitting In," GovExec.Com, October 1, 2003, at *www.govexec.com/features/0903hs/HS0903s2.htm.*

[17] One alternative, for example, might be build-up state naval guard forces to fulfill this role. See James Jay Carafano, "Citizen-Soldiers and Homeland Security: A Strategic Assessment," The Lexington Institute, March 2004, pp. 20–21.

The addition of the U.S. Coast Guard to the DHS provides another additional tool for expanding the Nation's capacity to conduct domestic counterterrorism in the maritime domain. Several initiatives are noteworthy. Since 9/11, many of the local investigation and inspections arms of the Coast Guard's Marine Safety Offices have significantly shifted their focus to supporting domestic counterterrorism efforts. In addition, the Coast Guard created the sea marshals program to create a cadre of specially trained law enforcement officers to escort high-risk vessels into port.

While the Coast Guard law enforcement initiatives are a positive effort, there is little sign that the service is creating a comprehensive human capital plan, including the leader development training and education that are needed to fully exploit the potential of these programs. Likewise, it is not clear that Coast Guard and ICE law enforcements programs are being developed in tandem to create the objective law enforcement corps needed for maritime security. In fact, it is not apparent that the DHS has defined its long-term strategic needs in this area and that they dovetail with other ongoing Federal and state efforts to expand the national capacity to conduct domestic counterterrorism.

Defending Against Catastrophic Threats. This critical mission area includes developing better sensors and procedures to detect smuggled nuclear, radiological, chemical, and biological weapons; improve decontamination and medical responses to such weapons; and harness scientific knowledge and tools for counterterrorism efforts. The guiding principle for investments in this mission area must be to focus funding on developing new means to prevent, respond to, and mitigate the unprecedented dangers posed by catastrophic threats.

The DHS Science and Technology Directorate is to be commended for developing mission portfolios to address the most critical technology needs for the DHS.[18] On the other hand, it is unclear whether the DHS portfolios, which has not yet been publicly released, adequately reflect the needs of maritime security. Nor has the directorate forged a relationship with the science and technology community in the DOD that can conduct the joint development and acquisition of major programs that might benefit both the defense and homeland security community.

In addition, greater consolidation of research and development efforts in regards to supply-chain security is required. For example, the Administration proposes to phase out Operation Safe Commerce in FY 2005. Launched in November 2002, the program was in-tended to use pilot projects in the ports of Seattle-Tacoma, Los Angeles–Long Beach, and New York–New Jersey to test technologies and practices, including cargo tracking, anti-tampering "Smart Containers," information protection, and real-time data reporting.[19] However, it has shown only limited results, and the research and development effort could be performed better and more efficiently under a development program in the DHS Science and Technology Directorate.

As the DHS consolidates these programs in the directorate it should reevaluate whether they are consistent with the department's research priorities. It is not clear, for example, that "Smart Containers" are a worthwhile program for Federal research. Any solution to implement smart containers should come from the private sector, which is in a better position to evaluate the utility of added security information as measured against the added cost. The DHS effort in this area might be more profitably focused on leveraging the security that might be provided by new commercial products and practices rather than developing and mandating standards and technologies to the marketplace.

Protecting Critical Infrastructure and Key Assets. This critical mission area includes national efforts to secure public and private entities. Since virtually all of the Nation's critical maritime infrastructure and key assets are not federally owned, developing programs to ensure responsible, efficient, and cost-effective cooperation between the public and private sectors should be the principle guiding investments in this area.

Making the challenges of critical infrastructure protection in the maritime domain particularly pressing is that U.S. ports must comply with new security provisions detailed in MTSA and ISPS. However, in developing a funding strategy to improve port security, the Administration should not become overly "port-centric." Addressing all the critical infrastructure concerns at U.S. ports could well require many bil-

---

[18] James Jay Carafano, "Strategy and Security in the Information Age: Grading Progress in America's War on Terrorism," Heritage Foundation *Lecture* No. 824, March 14, 2004, at *www.heritage.org/Research/HomelandDefense/hl824.cfm.*

[19] Alex Fryer, "Port-Security Project Endangered Murray Claims," *Seattle Times,* February 12, 2004, at *seattletimes.nwsource.com/html/localnews/2001856193__homeland12m.html.*

lions of dollars.[20] On the other hand, the DHS awarded only $245 million in port grants in FY 2003 (albeit the largest amount of any year to date). According to an unpublished analysis by Dr. Joe Bouchard, implementing MTSA at current funding levels (about $50 million a year) would take 112–162 years.

Yet, the current restraint in Federal funding may be very appropriate. Addressing the considerable vulnerabilities of maritime infrastructure does not necessarily require a dramatic infusion of Federal dollars. For example, effective intelligence and early warning, domestic counterterrorism, and border and transportation security programs can help to reduce risks to critical infrastructure by limiting the opportunities for terrorists to reach U.S. ports. With limited resources available in the Federal homeland security budget, it is not apparent why a multi-billion-dollar port security initiative would be a superior strategic choice to a more balanced maritime security program.

In addition, the overwhelming preponderance of maritime infrastructure is in private hands. It is not clear that full-federal funding would be either appropriate or sustainable. Excessive funding would more likely create a condition of dependency with security declining as soon as the infusion of Federal dollars ended. Initiatives that enable and encourage the private sector to take a more expansive and proactive role should be central to any protection program.

Federal port grants should used sparingly, as a tool to promote appropriate public-private sector solutions. More important than simply spending more money to help facilitate the development of maritime security programs, the Federal Government should help create a predictable business environment with (1) multi-year authorizations so that states, local governments, and the private sector would have a clear grasp of what funds will be available over the long term; (2) national performance standards so that they know what the Federal Government expects state and local governments and the private sector to contribute to critical infrastructure protection; and (3) a clear system of national priorities so that the preponderance of Federal investments support the most critical strategic needs.

Emergency Preparedness and Response. This critical mission area includes preparing for, responding to, and mitigating the effects of terrorist attacks. The overarching principle that must guide funding is that Federal resources should be used to assist in creating a true national preparedness system, not merely to supplement the needs of state and local governments.

Currently, the major challenges affecting an effective response to a maritime incident are the same as those affecting other types of domestic emergencies: interagency coordination, organization and communications, and convergence.[21] Establishing unity of effort is central to addressing all of these concerns.

The Coast Guard should be commended for its announcement in January 2004 to consolidate all its regional activities under sector commands, so that captains of the port will have all the assets available to support maritime security under their control. This initiative, however, does not ensure proper unity of effort at the port. In many ports, the Coast Guard, ICE, and port authorities, each with critical specific duties and authorities in regard to port security, have their command posts in different facilities, undercutting efforts to ensure effective integration of their efforts in times of crisis. The DHS should review the requirements for command and control at the ports and determine the needs for unified command posts, redundant command facilities, and virtually integrated command posts to ensure unity of effort for emergency response.

It may also be worth reviewing whether national plans are adequate to deal with the consequences of catastrophic or multiple attacks on geographically disparate maritime targets.[22] For example, in the immediate aftermath of the 9/11 attacks,

---

[20] In August 2000, the Interagency Commission on Crime and Security in U.S. Seaports estimated that the costs to upgrade security infrastructure at the Nation's 361 ports ranged from $10 million to $50 million per port. Congress funded $93 million for security improvements with the passage of the Maritime Security and Transportation Act (MTSA) in 2002 but received grant applications for as much as $697 million in the first year of the program alone. U.S. General Accounting Office, "Transportation Security: Post-September 11th Initiatives and Long-Term Challenges," GAO–03–616T, April 1, 2003, pp. 5 and 16. The Coast Guard has estimated that it will require at least $1.4 billion in the first year and $6 billion over 10 years for private port facilities to meet the baseline security mandates required by the MTSA. Other estimates of total cost range from $5.8 to $7.8 billion. James Jay Carafano, "Budgets and Threats: An Analysis of Strategic Priorities for Maritime Security," Heritage Foundation *Lecture* No. 791, June 16, 2003, at *www.heritage.org/Research/HomelandDefense/HL791.cfm.*

[21] These are described in James Jay Carafano, "Homeland Security and the Trouble with Training," CSBA *Backgrounder,* October 3, 2002, at *www.csbaonline.org/4Publications/Archive/B.20021003.Homeland__Security__/B.20021003.Homeland__Security__htm.*

[22] For more discussion on multiple and catastrophic attack scenarios see the discussion on emergency response in James Jay Carafano, "Budgets and Threats: An Analysis of Strategic Pri-

the Federal Aviation Administration halted all civilian aviation. In the aftermath of a maritime attack, similar concerns might call a halt to U.S. maritime traffic. In this event, mechanisms to rapidly reestablish confidence in the supply chain and resume the flow of commerce in order to minimize economic disruption and restore public confidence will be vital. If adequate public/private sector plans do not exist to address such contingencies, they must be rapidly developed.

Organizational Issues

While the issues raised in each of the critical mission areas deserve attention, together they still do not address the core issue of how well the Nation is doing in preparing a maritime security system that will protect us during a protracted conflict against threats that will surely change and evolve to test the defenses we throw up to frustrate them.

We will not be able to depend on the terrorists to provide us measures of success. The fact that al-Qaeda operatives took five to seven years to plan and execute the September 11 terrorist strikes is a cause for concern. It could well be a half-dozen years before the DHS faces its first great test.

For now our metrics of success must rely on measuring our capacity to implement strategy. The first task should be revisit the basic organization and missions of the DHS. Here a lesson from the Cold War is instructive. The National Security of Act of 1947 created what became the Department of Defense and the Central Intelligence Agency, the Nation's two premier weapons for defending against the Russian bear. Yet, it soon became apparent that in the enabling legislation neither organization had been crafted perfectly to match the Nation's emerging strategy of containment. Two years later it was necessary for the Congress to revisit the organization and missions of the departments. At the same time, some of the most difficult and obvious challenges, such as how to promote jointness (operations involving more than one of the military services), were ignored. As a result, organizations and practices became institutionalized, and it took over 40 years to resolve some of the obstacles to effective operations.[23]

Congress can help the DHS avoid a similar fate if it begins now to assess how well the department is organized to implement the emerging national strategic priorities. One area that should be addressed is assigning responsibility for directing national maritime strategy. Clearly, emerging strategic requirements call for an integrated system of layered security initiatives. Yet, there is no single over arching strategic concepts that defines how ongoing initiatives will be forged into a coherent system or makes the hard choices for prioritizing scarce resources. In part, the lack of unifying maritime strategy is understandable—four major organizations play prominent roles (DOD, and within the DHS, the Coast Guard, ICE, and the TSA—Transportation Security Agency) and arguably their roles and missions overlap. Congress might profitably look at the prospects for consolidating missions, assigning one entity within the DHS the role of providing overall strategic planning and operational control of maritime security and responsibility for coordinating with DOD. At the same time, Congress might revisit the regulatory functions of the components in the DHS to see if the Departments of Transportation or Commerce might more appropriately perform them, allowing the DHS to focus more of its resources on homeland security. Finally, a crosswalk needs to be performed between the performance metrics established by each agency for measuring progress to ensure that they are integrated and complimentary.

Another area that deserves further attention is an examination of how we will train the next generation of leaders that will be responsible for implementing the future national maritime security system. Currently, the Nation lacks an overall homeland security training and education strategy. Training is not only essential to prepare leaders for the difficult and complex decisions they will face in a crisis, but also to evaluate readiness, determine the effectiveness of programs, and identify needed improvements. Meanwhile, education is critical in preparing leaders to respond to long-term challenges.

The advanced degree program offered by the DHS through the U.S. Naval Post-Graduate School is one admirable initiative, but it is not enough. Other professional

---

orities for Maritime Security" Heritage Foundation *Lecture* No. 791, June 16, 2003, at *www.heritage.org/Research/HomelandDefense/HL791.cfm.*

[23] For example, see David Jablonsky, "Eisenhower and the Origins of Unified Command," *Joint Force Quarterly,* Vol. 23 (Autumn/Winter 1999–2000), pp. 24–31. See also Shepherd, "Evolution of Security Agencies and Departments," pp. 161–165, and William W. Epley, Roles and Missions of the United States Army: Basic Documents with Annotations and Bibliography (Washington, D.C.: Center of Military History, 1993), pp. 299–310. Additional major revisions were made by the Goldwater-Nichols Defense Reorganization Act of 1986. See also James R. Locher III, *Victory on the Potomac* (College Station: Texas A&M University Press, 2002).

development opportunities for emerging senior leaders are also needed. The Massachusetts Institute of Technology, for example, conducts a program called Seminar XXI for the Federal Government. Seminar XXI provides a year-long series of lectures and workshops for mid-grade professionals on international affairs. A similar program targeted on homeland security might be equally useful. In the same manner, the national community might benefit from the establishment of a national homeland security university modeled on the military's war college system.

Finally, any national leader development effort will have to include a plethora of state and local leaders and private sector leaders. The nation's network of junior colleges, which have become the hub of continuing adult education throughout the country, may provide the best venue for offering appropriate leader development opportunities.

Congress might consider guiding the DHS training and education effort by creating mandatory training, education, and experience requirements similar to the provisions established in the Goldwater-Nichols Act to foster jointness among the military services.

Over the long term, the capacity of the national maritime security system to exploit the initiatives currently being put in place will be more dependent on the quality of the decisions made by its leaders and the programs they implement than on the structure of the system itself. The nation would be well served if we gave equal attention to both sides of the equation.

I, again, thank the Committee for the opportunity to testify on this vital subject and I look forward to your comments and questions.

Senator NELSON. Thank you.

Mr. Mitre?

STATEMENT OF MIKE MITRE, DIRECTOR, COAST PORT SECURITY, LONGSHORE DIVISION, INTERNATIONAL LONGSHORE AND WAREHOUSE UNION (ILWU)

Mr. MITRE. Good morning. I would like to thank the Chairman, the Ranking Member and the Members of this Committee.

My name's Mike Mitre, and I've been a member of the ILWU for almost 30 years. I've worked on and around the terminals for about 29 years, and my specialty is container terminals. I'm a crane driver, and I used to be a foreman running what they call the "dock and ship" on the terminals.

I'd like to thank everyone for allowing us to speak here today. Some of my constituents are really excited by the fact that, hey, we finally had a—got a chance in Washington to get up and say our piece and say what we really feel is happening with security within some of the marine terminals on the West Coast, and especially because we live and work within L.A./Long Beach, which is the largest two ports in the country. And with 12 million containers, that's where the numbers are. That's the numbers game, and that's where they're coming.

Most of my remarks will be aimed at practices that occur there. I'd like to also thank the International Longshoremen's Association and the teamsters for their assistance in a combined that we put together in trying to attack some of the tougher issues regarding port security.

First of all, I'd like to say that we really appreciate the commitment that Congress, and this Committee in particular, have made to the goal of protecting our ports, but, more importantly, to protecting our port workers, which is our members, and they're the guys that work there. The men and women that are—they're our first line of defense. We handle containers when they come off the ship. And if something should happen, it's our workers that are going to get hammered first, and most of our families live and

work, themselves, within five miles of the port. And if we're talking any kind of a radiological device—in fact, if you have any kind of modern explosives, our families would probably impacted just as well as our workers would, too. So we really appreciate the strides that everyone's made.

We also really appreciate the Coast Guard. If anyone has worked closer with the unions in the ports, there isn't anyone closer than the Coast Guard. The Coast Guard in L.A./Long Beach, in Oakland, in San Diego, in Seattle/Tacoma, on the Columbia River—the Coast Guard's done a great job. They've helped more, and I think we have a closer relationship than we ever have.

On the day of 9/11, the Coast Guard was the one that reacted first. And within 2 hours, they put together a stakeholder group of 200 people. So the Coast Guard, I think, has to give—be given kudos.

Every day, we unload thousands of containers from vessels that call from all over the globe, and they're filled with things from everywhere, loaded by everybody. Most of them do not undergo an inspection before they're loaded on a truck or a rail car bound for all points east to the interior of the United States.

Consider the recent suicide-bombing in Israel. In Ashdod, port workers and their infrastructure were clearly targeted. This is the very same type and level of an incident that could very—it could very well happen here. And, you know, we've been afraid of it since 9/11. And in the Port of L.A./Long Beach, we're really, you know, thinking this could happen. It's coming.

Some of my comments are going to center around some of the security procedures that we do within the port, and also some of them that have been discontinued, and we feel should have never been discontinued, and should be recontinued.

For many years, protocols such as the inspection of loaded container seals and the verification of empty containers were a given. These were done at nearly every facility by marine clerical workers and longshoremen employed there. Container-seal inspections are critical. And they're critical because you simply can't inspect every container. The integrity of the seal, that it hasn't been tampered with and that the seal number matches up with the container number on the cargo manifest, are two related procedures that can be done in a matter of seconds, and they can be done during the process of checking the container being offloaded from an arriving vessel. It's quick, it's easy, and it's effective. Discharge procedures accomplished as this container is being unloaded from a vessel of the dock, they're still done by a marine clerk located in the very same place as when the seal checks used to be done, yet these seal checks have been discontinued by the terminal operators that run the terminals in the West Coast.

The problem that we have is, a lot of the different terminal operators have gone so far as to officially inform us, in writing, that it's their feeling that, because of oncoming technologies, that we no longer have to seal container—check the seals on containers; because of incoming technologies, we no longer have to worry about checking empty containers coming into the port. And you have to realize that if we have 12 million empty—12 million loaded containers coming in from Asia, there's going to be at least 7, 8, 9 mil-

lion empties being cycled back to Asia. If these empties are allowed to come into the port uninspected through our terminals, it's—you're having an open invitation for something to happen.

The new MTSA regs require that seal checks are being done. But the problem is, the terminal operators are now going to interpret that these seal checks are only going to require them to check the seals at the terminal's in-gates, but not at the vessels, where the majority of all containerized cargo is offloaded. Why would we check the seals of this relatively small number of export cargo going through the in-gates, but ignore the seals on the enormous quantity of our inbound imports coming from Asia?

The empty-container inspections, like I said, ones that were—it was an inspection that was once unilaterally done throughout the port—has been discontinued since 9/11. This is perhaps one of the most threatening of all the traditional practices that we no longer do. The ability for a trucker to introduce an empty container at a marine terminal in-gate, with the knowledge that it will not be inspected as a matter of policy, is not right. And it really is no different than boarding an aircraft and being searched, yet being allowed to carry on a piece of luggage without it ever being opened. The only difference is, in this case you have the knowledge beforehand that whatever you want to smuggle inside a terminal will not be searched as long as it's inside this empty container.

Many empty containers also are cycled back to the United States, especially refrigerated ones, and they have been acting as an ideal conduit for the smuggling of people and aliens trying to come back into this country. There are presently terminals in Hawaii—specifically, the Horizon facility—that require all empty containers to be opened and searched. And then they have to have a seal affixed, clearly marking it as an empty. For us to do no less is asking for trouble.

If you knew that you could drive a 40-foot container onto a terminal in the largest port of the country without it being opened, don't you think that others may also have this same knowledge? Empty-container programs should be part and parcel of the new facility security plans. Their exemption presents a clear and present danger to not only our workers and to the community, but it also presents a danger to the marine terminals and our port transportation infrastructure.

The implementation of the new TWIC card, called the Transportation Worker Identity Card, is a process that the ILWU has participated in. We're concerned that all aspects of—all true aspects of port security are important. Along with TSA and the port authorities, ILWU and the related stakeholders have embarked on a concurrent effort helping to create and prototype a successful terminal access ID concentrating on the importance of individual recognition. We must have a better way to identify our port workers, our clerical workers, our vendors, subcontractors, even management personnel coming onto the terminals so that we all know who everybody is, and that an ID just can't be shuffled back and forth from one person to the other.

Senators, expensive and technological advancements will eventually take their place in the seaport security environment. Examples of this, like the new radiologic portals, and especially the VACIS

gamma ray inspection machines, are excellent examples of 21st century technology. The problem is, is that they have to be well thought out. These radiologic portals, they're a great idea, and they are part and parcel of a good, basic terminal strategy. But the very fact that they want to locate these things at the out-gates of the terminal presents a problem. Most containers coming off the ships are going to sit in the terminal between 5 days and 2 to 3 weeks. Why would we expose not only our port workers, but the community, to a radiologic problem or an accident? And instead of siting these radiologic detectors at the out-gates, why not pull them close to the ship, so when these containers come off the ship, they can immediately go through them, and, therefore, ensure the security of the people that work there and the people that live close to the ports?

It is still the sensible, inexpensive, and logical approaches to port security, and especially practices like container-seal inspections, empty-container verification, and other things like this, that will provide a basic and solid foundation under which to build a proper security infrastructure. Couple this with an accurate port ID system that really works, and you have the basics on which to build this no-nonsense marine terminal security system.

Cargo security cannot be allowed to denigrate into a catch-all for new and developing technologies at the expense of the traditional practices that were developed over many, many years inside the ports. These were practices that really worked, they accurately addressed real problems, and they were relatively less commerce-inhibiting than others that were not, and they were tried and true methods.

Many new technologies surrounding cargo security are still developmental, and some aren't even fully ready, yet many terminal operators have decided already to abandon some of the most traditional—more traditional techniques in favor of waiting for some of these newer technological advancements to come online. We all understand that these new technologies will eventually replace many of the inspection and verification protocols that are now done in person; but until we come to that point, we must make a commitment to continue to do what is logical, what is practical, and has worked for us for so long.

Probably the most important part of my testimony here today is to talk about the funding. Funding must be made available. It will have to come from Congress so that our Coast Guard assets can properly assume the role designated to them as the primary landside and terminal enforcement agency. The traditional waterside role that the Coast Guard has always assumed must now include sufficient funding that is going to require additional manning, training, and enforcement to make sure that they can accomplish acceptable levels of marine terminal container security. Funding is essentially, and not only for these needs, and not only for the Coast Guard, but, just as important, it is going to be very necessary for the answers that will lead us to the infrastructure and port security solutions nationwide, that we're going to allow us to move cargo and keep commerce moving in the event of a terrorist attack.

Properly applied, this type of funding should address both the port security and the infrastructure solutions necessary to ensure that the flow of cargo is not interrupted. Properly appropriated, these funds will help to not only develop and increase port security, but also to design an underdeveloped security infrastructure necessary to move cargo in volume in the years to come.

The major problem on the West Coast is this. You have three load centers. L.A./Long Beach is the largest one. You have Oakland and Seattle/Tacoma. If there's a terrorist attack or any kind of a terrorist security incident, we simply do not have the alternatives where we can move cargo. The major cargo island in L.A./Long Beach houses five of the largest mega-terminals in the world. Each one of these is capable of moving up to 5,000 gate moves a day. And to give you some idea of what that is, Rotterdam, at their largest terminal, moves about 850 gate moves a day. Each of ours on this island can move up to 5,000 a day. Right now, we're averaging between 1,800 and 2,600 a day. The numbers game, once again, shows how big L.A./Long Beach is, and then, in relation to a smaller bit, to Oakland and Seattle/Tacoma.

This cargo island is connected to the mainland by two bridges. If either of these bridges were to go down—and I just heard this same kind of a thing from my colleague from New Orleans—we're done. You could bring cargo flow to a grinding halt.

You know, not wishing to touch on something that could be a little touchy, you know, we had a problem last year, a small labor dispute on the West Coast. We had a 10-day lockout. And I'm not making light of the situation. But the problem is this. In just those 10 days, look what happened. If one of these bridges was to be taken out, we could be looking up to 3 to 6 months, possibly even a year, of an interruption of commerce. And 92 percent of all the commerce coming into this country is waterborne. Of the commerce coming into the West Coast, 65 percent comes into L.A./Long Beach alone. And one incident, one incident, could bring this to a screeching halt.

So I would hope, if nothing else today when I'm talking to you, that everyone would understand that, on the West Coast, it is the major cargo import receiver for this country. It has now obviated the need of the Panama Canal through the intermodal rail. Intermodal rail connections are able to take cargo throughout the country even faster than a ship going through the canal and going to an East Coast port, in most cases. And because of that, and with only three small load centers, any one of these centers goes down, and we have a big problem.

So I would really hope that by making this point of how important these load centers are, we can appreciate the fact that funding must be made available to look for alternatives in cargo movement, in cargo flow, and alternatives how to unload these ships in case of a terrorist security incident.

Thank you.

[The prepared statement of Mr. Mitre follows:]

PREPARED STATEMENT OF MIKE MITRE, INTERNATIONAL LONGSHORE AND WAREHOUSE UNION (ILWU)

Chairman McCain, Ranking Member Hollings and members of the Committee, my name is Mike Mitre. I am a member of the International Longshore and Warehouse Union (ILWU), which since 1934 has been chosen by thousands of West Coast port and dock workers to represent us in all matters related to our employment. For the past two years, I have served as the union representative regarding port security and have had opportunities to work with the Coast Guard, TSA, Customs, and other stakeholders in an effort to effectively secure our ports from acts of terrorism. We commend these agencies for their hard work and commitment to the national security of the United States. In particular, the ILWU commends the Coast Guard for developing comprehensive port security regulations in a very short time frame. We appreciate the hard work and dedication of the Captain's of the Ports, coast guard personnel, TSA, and Customs personnel. I also want to commend other labor organizations that have worked on a common agenda to protect our ports including the International Longshoremen's Association, the International Brotherhood of Teamsters, and the Transportation Trades Department, AFL–CIO.

As co-chair of the International Longshore and Warehouse Union Legislative Committee, I have developed a number of policy statements with respect to the security of our ports on behalf of our members and communicated our position to members of Congress and key staff. We appreciate the commitment that Congress and this Committee in particular, has made to the goal of protecting both our ports and ILWU dockworkers from the threat of international terrorism.

Mr. Chairman, thank you for holding this important hearing. We are at a critical time in the history of this country. The threat of a terrorist attack against the marine transportation system is a new reality. On March 14, 2004, suicide bombers at the Ashdod Port in Israel killed 10 people and wounded another 16. It appears that all the victims were workers. It is certainly in the interest of American port workers to secure our ports. Every day we unload thousands of containers from ships calling from virtually every point on the globe, each filled with unknown items packed by unknown people throughout the world. Few of these containers or vessels are screened or inspected before being unloaded by longshoremen. Many of the containers do not go through any type of a security screening process before being loaded on a truck or railcar bound for the interior of the United States. Many of our families, friends, and coworkers live in different seaport communities such as San Pedro and Oakland, California, Portland, Oregon, Seattle, Washington, and Honolulu, Hawaii. While I would like nothing better than to be able to tell them that all the stakeholders within the marine transportation system are doing everything possible to keep them safe and secure from terrorism, this may not exactly be the case.

My testimony today will focus on specific measures that, if implemented, will provide more meaningful security for our port marine terminals and our communities. Marine terminal operators along the west coast continue to refuse, despite repeated encouragement and demands from the ILWU, to implement adequate port security measures to protect our port workers, communities and the Nation as a whole from possible terrorist attacks. Even more shocking and inexplicable is the reality that some terminal operators have reduced or abandoned some of the most basic port security measures following the September 11th and the terrorist attack against our American people.

On March 15, 2004, the ILWU wrote to Coast Guard Admiral Hereth to urge the Coast Guard to take effective action to compel these employers, the marine terminal operators, to immediately implement and maintain adequate security measures in accordance with the Maritime Transportation Security Act (MTSA) and the applicable and related Coast Guard regulations issued on July 1, 2003 and October 22, 2003.

Since September 11, 2001, the ILWU has made repeated overtures to these same employers to develop and institute, without delay, practices and procedures designed to increase the level of security to at least that which existed on September 11th, 2001. The Union's requests for Employer action to increase port security is documented in various proposals and letters to the employers, samples of which are attached to this testimony marked Attachment 1.

Many of these companies have actually reduced security by, among other things, discontinuing the practice of inspecting the integrity of container seals upon entering marine terminal facilities. The second attachment to the testimony are copies of some of the letters documenting our Employers' discontinuation of the regular inspection of container seals and inspection of "empty" containers shortly before and after September 11, 2001. The Employers' insistence, over Union objection, to stop

inspecting container seals at certain West Coast marine terminal facilities is especially disconcerting given that the Coast Guard regulations in 105.265(b)(4) specifically mandate that terminal operators and owners "check seals and other methods used to prevent tampering upon entering the facility and upon storage within the facility".

While we have urged our Employers to initiate adequate port security measures regardless of specific governmental mandates, the Union has especially pressed for the PMA Employers' immediate full compliance with Coast Guard Regulations 105.265, "Security Measures for Handling Cargo", which plainly constitute the core security provisions for marine terminal facilities; where the majority of ILWU port workers are employed.

With respect to the specific security measures mandated in Coast Guard regulation 105.265, "Security Measures for Handling Cargo", our information, daily work experience, and observations disclose that the PMA Employers have failed to implement the following security measures listed in that provision:

- *105.265(a)(5)—"Identify Cargo That is Accepted for Temporary Storage in a Restricted Area While Awaiting Loading for Pickup"*—Most if not all port facility operators/owners have, after September 11, 2001, and also after the December 31, 2003 filing of security plans, continued the standard practice of mixing cargo and containers designated for loading on different ships and trucks scheduled for different time periods and also mixing them with other cargo and containers not yet designated for a particular loading or pickup. Moreover, few, if any, facilities have "restricted areas" for temporary storage of cargo.
- *105.265(a)(6)—"Restrict the Entry of Cargo to The Facility That Does Not Have a Confirmed Date for Loading as Appropriate"*—No facility operator/owner, as far as we know, has instituted any restrictions on the entry of cargo that lacks a confirmed date for loading, let alone conduct any determination of "appropriateness" for receipt of such cargo since September 11, 2001, and since the December 31, 2003 filing of security plans. In fact, many facility operators/owners continue to use what they call "dummy bookings" to document the regular receipt of cargo that lacks a designation or confirmed date for loading onto ships. In addition, most, if not all, marine terminal facilities continue the standard practice of allowing cargo to first enter the facility and only after entry determine the existence of appropriate documentation and designation for loading. Many facility operators/owners also continue the practice of storing on site, without restriction for several days, cargo with inadequate documentation and unknown designation for loading.
- *105.265(a)(9)—"Create, Update, and Maintain a Continuous Inventory of All Dangerous Goods and Hazardous Substances From Receipt to Delivery Within the Facility Giving the Location of Those Dangerous Goods and Hazardous Substances."*—This critical security measure has simply not been implemented at any facilities where ILWU members work since September 11, 2001 and continuing after the December 31, 2003 filing of security plans. In nearly all marine terminal facilities, hazardous material cargo is randomly integrated with other types of cargo, including even food products throughout the terminals. Also, as noted, it is standard practice for marine terminals to receive and store for a certain period of time containers of unknown contents pending receipt and verification of complete documentation.
- *105.265(b)(1)—"Unless Unsafe To Do So, Routinely Check Cargo, Cargo Transport Units and Cargo Storage Areas Within the Facility Prior to and During Cargo Handling Operations for Evidence of Tampering."*—Few if any West Coast Marine Terminals have instituted any practices or procedures to "routinely check" cargo, containers and the storage areas for possible tampering within these facilities following September 11, 2001 and even since the December 31, 2003 filing of security plans. In those port facilities where some checking is performed, such as for example, at Terminal-6 in Portland, Oregon, the security guards merely drive through the facility in a perfunctory manner no differently than they did before September 11, 2001.
- *105.265(b)(2)—"Check That Cargo, Containers, or Other Cargo Transport Units Entering the Facility Match the Delivery Note or Equivalent Cargo Documentation."*—While this practice was commonly followed in the West Coast ports ten or more years ago, the industry trend starting before September 11, 2001 and continuing to the present is the elimination of requiring that cargo and containers match the delivery documentation before entry into marine terminal facilities. Neither the terrorist attacks of September 11, 2001, the issuance of the

Coast Guard interim regulations of July 1, 2003, nor the filing of facility security plans as of December 31, 2003, have changed this regressive trend.

- *105.265(b)(3)—"Screen Vehicles".*—The screening of vehicles before entering marine terminal facilities is done in some West Coast ports, but not all.
- *105.265(b)(4)—"Check Seals and Other Methods Used to Prevent Tampering Upon Entering the Facility and Upon Storage Within the Facility."*—As noted, most marine terminals on the West Coast have not instituted any procedures for the checking of seals and other methods to prevent tampering either upon a container entering a facility or upon its storage within the facility. Indeed, some marine terminal operators have actually discontinued this practice in years before and in months after September 11, 2001. That most marine terminal operators do not routinely check and verify the integrity of seals on most containers is reflected by the one limited exception where such checks are more commonly done with respect to cargo and containers subject to USDA regulations. Moreover, most marine terminal operators fail to have adequate procedures for monitoring pilferage and other tampering of containers and cargo as reflected in the common practice of the terminal operators and the carriers splitting the cost of any such losses based on their failure to know the time and location where such tampering occurred.

Mr. Chairman, I cannot emphasize enough the importance of checking the outside seal of containers upon entry into the facility by rail or truck and especially, upon entry by sea. A broken seal would immediately alert the port facility that the container may have been with tampered and needs to be carefully inspected. A systematic check of container seals also provides authorities with a record as to the parties responsible for placing the seal on any container that may be the means of a terrorist act.

The Coast Guard regulations do not contain references regarding the need to develop a program to inspect and seal "empty" containers. There should be little disagreement over the need for an inspection or verification protocol concerning these containers. The fact that marine terminal operators routinely conducted "empty" inspections in the past as a regular part of their security program to verify the absence of harmful contents and to detect and deter possible terrorist attacks only adds to the viability of this procedure. The ILWU urges the Coast Guard to strongly consider creating a mandate regarding the inspection of empty containers. If there was ever to be an attack from anyone using an "empty" container to transport and stage explosives or chemical or biological agents, this would be the ideal manner in which to accomplish it. The level and manner of intelligence gathering and the sophistication of technique used by various terrorist organizations should leave nothing to chance.

It is the Union's view that the Coast Guard regulations in general, and the MTSA in particular, as well as basic common sense and good faith concern for the security of the ports and the country necessarily require that all maritime companies initiate comprehensive and adequate port security measures *without delay,* notwithstanding the technical final compliance date of July 1, 2004 as set out in 105.115(b) of the Coast Guard regulations. Terminal operators that fail to implement necessary security measures in the interim preceding the July 1, 2004 deadline is contrary to the stated intent and objective of the MTSA and the Coast Guard regulations.

Indeed, Section 70103(c)(7) of the MTSA mandates that the Secretary of Homeland Security, who has delegated such responsibility to the Coast Guard, "shall require each owner or operator of a vessel or facility located within or adjacent to waters subject to the jurisdiction of the United States to implement any necessary interim security measures, including cargo security programs, to deter to the maximum extent practicable a transportation security incident *until the security plan for that vessel or facility operator is approved."* Under these clear statutory and regulatory mandates, there is no legitimate reason or excuse for any vessel or facility operator/owner not to implement the provisions of the Regulations and of their security plans after submission to the Coast Guard on December 31, 2003, and pending review and approval by the Coast Guard by July 1, 2004. Any good faith approach to port security would demand no less. To be sure, would-be terrorists will not wait for the passing of a technical future deadline to attack our ports; nor should port Employers wait to adequately protect our port facilities from such potential attacks.

Common sense would indicate that waiting until July 1, 2004, in which to institute necessary port security measures actually could heighten the risk of potential terrorism during this waiting period. I understand that our employers are concerned about the cost of port security measures. The ILWU is mindful of their concerns and we understand that it may be cost prohibitive and impractical to subject every container to a thorough and complete inspection. However, every container that enters

our ports can and should be subjected to a security check. When there is a conflict between efficiency in the maritime transportation system versus additional security measures that will enhance the security of the system and our port communities, we believe that security should prevail.

The ILWU has worked closely with TSA in developing the TWIC ID, envisioned as a nation wide transportation worker ID security program. The prototype phase now underway in the ports has already actively involved many ILWU members, an indication of the realization by the most average worker just how serious security has become. It is also an indication of the degree of commitment the ILWU has exhibited. Only through a dedicated and unified effort by all stakeholders will true port security be achieved.

Finally, we ask the Congress and the Administration to fully fund port security. It is critical that when the facility security plans are finalized that money is available for optimum security rather minimal security. We applaud the members of this committee, and particularly Senator Hollings, for efforts to secure the necessary funding. If a terrorist attack occurred in a major port, the lives of our workers, families, and community would be lost. The national economy would be badly shaken. It is incumbent on the Congress to provide the necessary funding to meet longshore labor and other port workers security objectives.

On behalf of the members of the International Longshore and Warehouse Union, I thank you for the opportunity to testify today. I would be pleased to answer your questions.

ATTACHMENT 1

ILWU PROPOSAL FOR SPECIAL CLRC MINUTES RE WATERFRONT SECURITY—SEPTEMBER 20, 2001

The CLRC met to begin assessing waterfront security issues in light of the terrorist attacks inflicted on the United States on September 11, 2001. The Coast Parties condemn these terrorist acts and will not be deterred from performing the work that is so vital to the nation's interest. Accordingly, the CLRC agreed to the following:

(1) The Union and the Employers pledge to work together to assess the safety of waterfront personnel and the security of operations covered by the PCL&CA with respect to the threat of terrorist attacks.

(2) The Union and the Employers. through the CLRC, will jointly develop any programs and initiatives that they deem appropriate in response to the threat of terrorist attacks affecting waterfront personnel and operations covered by the PCL&CA.

(3) The Employers will promptly notify the Union of any developments and initiatives, including any actual or proposed government mandates that could affect waterfront security or operations covered by the PCL&CA.

(4) The CLRC will have Waterfront Security as a standing item of its regular meetings= agenda until such time as it deems appropriate.

(5) The CLRC instructs all Joint Port Labor Relations Committee to review Waterfront Security as a standing item of their regular meetings—agenda and to report promptly to the CLRC any problems or proposals for its review and action.

The CLRC agreed to send copies of these minutes to all JPLRC's by facsimile today.

August 28, 2002

JOSEPH MINIACE,
President and CEO,
Pacific Maritime Association,
San Francisco, CA.

Re: Letter of Understanding on Port Security

Dear Mr. Miniace:

The Parties agree that the Pacific Coast longshore industry must expand port security measures to address the new threats of terrorism arising from the tragic events of September 11, 2001. The Parties recognize that though many port security

provisions may eventually be mandated by law, the Coast Parties must act responsibly and proactively, utilizing their expertise in port operations, to have in place immediate security measures for the protection of port workers and 'communities. Accordingly, this will confirm that the Parties have agreed to implement under the Pacific Coast Longshore and Clerks Agreement (PCL&CA) the following port security measures and to work together to lobby the Federal Government to adopt laws and regulations that are consistent with these provisions:

(1) Any work and functions covered by section 1 of the PCL&CA that are to be performed as part of any port security measures that may be mandated by law or regulation shall be performed by ILWU bargaining unit members.

(2) The Union and the Employers pledge to work together in good faith to assess and address the safety of waterfront personnel and the security of operations covered by the PCL&CA with respect to the threat of terrorist attacks. The Union and Employers also agree to work together in good faith in implementing any security procedures that may be required by law.

(3) The. Union and the Employers, through the CLRC and the JPLRC's, will Jointly develop a security plan for each port area as well as security plans for each marine facility covered by the PCL&CA These plans shall, among other things, contain procedures for:

(a) the identification, assessment, prevention and response to security breaches, emergencies, hazards to health and safety, and threatened and actual terrorist acts;

(b) notifying waterfront personnel of emergencies and hazards, for evacuating and otherwise protecting personnel from such dangers, and for determining that personnel may be returned to the area without danger to their health and safety;

(8) Any conflicting law or regulation shall supersede any contractual provision regarding port security and related health and safety issues; however, these contractual provisions may expand any legal obligations in this area unless specifically prohibited by law or regulation.

Please confirm your agreement by signing below.

Yours truly,

JAMES SPINOSA,
International President.

Understanding Confirmed:
Joseph Miniace,
President and CEO
Pacific Maritime Association

ATTACHMENT 2

EAGLE MARINE SERVICES, LTD.
3/4/02

ILWU Local 52
Seattle, WA

Attn: John Daquisto

John,

As was discussed last week we have discontinued the checking of seals containers loading to our on dock rail and the inspection of empty containers discharging from on dock rail. We do not interpret this as a change in method of operation and therefore section 15.12 does not apply. We refer to section 1.21 which addresses the employers right to determine what work will be performed.

If either of these duties are to be performed in the future will done in accordance with the PCCCD.

Regards,

KELLY GARBER,
Operations Manager, GGN.

SEATTLE
January 15, 2002

SCOTT GODFREY, President
Labor Relations Committee
ILWU Local 52
Seattle, WA

Dear Committee Members,

This letter is intended to inform you of some procedural changes that will be taking place at the in-gate Terminal 18, related to the processing and receiving of export full and empty containers. Within the next few weeks, pedestals and cameras will be installed in the lanes. As a result, the in-gate clerks will be moved into a "kitchen/tower" situation where they will no longer be in the lanes, but will be stationed in the gate house building. The cameras will allow the clerk to see all four sides of the container from inside the building and the pedestal monitors will be used to display the yard location to the trucker. Tickets will no longer be given to the trucker.

As previously stated above, the hardware will be installed within the next few weeks but we don't expect to implement the new procedures for a couple of months. Please be advised that we have consulted with the appropriate regulatory agencies and a camera inspection of export containers is allowed by a marine terminal as long as all four sides of the container are visible. If you have any questions regarding this letter please let us know, as we would be happy to meet with your committee upon request to discuss these changes.

Sincerely,

GRAHAM C. HUNTER,
Ops/Labor Mgr.,
SSAT, T–18.

Scott Munger—PMA
Sandra Starkey—PMA
Lee MacGregor—SSAT
Steve Hanses—SSAT

SSA—TERMINAL 18—SEATTLE

To: Dennis/Bob
From: Lee
CC: Graham/Steve
Date: 02/15/01
Re: Gate one change

Please be advised that is has been decided by SSAT Terminal 18 that inspections of export containers arriving on trucker's own equipment are no longer required. Therefore, as of Tuesday, 2/20/01, the number of mechanics working the full in lanes will be reduced, with the remaining mechanic's focus being to inspect line owned chassis and the associated containers being received.

Please instruct your clerks that they are not to leave their booth to inspect export loads that are on trucker's own equipment. They are to receive all information from the drivers (same as today) for processing and they will only need to leave their booths for CY moves if a mechanic is available. Even though mechanics will be present to inspect CY moves, if the clerk has finished the transaction and a mechanic has not arrived, the clerks are to process the truck without the inspection. This also means that seal number/license number verification is not required for these types of moves.

Please note, all renter boats will need inspections and seal verification, regardless of what type of chassis being received.

Thank you for your cooperation.

LEE

MARINE TERMINALS CORPORATION
San Pedro, CA, May 2, 2003

Mike Zuliani
President, ILWU Marine Clerks, Local 63
San Pedro, CA

Re: New Method of Operation at WBCT, SP 126

Mike:

Please be advised that effective Monday, May 12, the West Basin Container Terminal (SP 126) will be eliminating seal number verification and empty inspections on all equipment entering the terminal. The seal number will be obtained from the truck driver and received by the Marine Tower Clerk via the existing gate audio systems.

This new method of operation will reduce the daily number of marine clerks employed by approximately four.

Please feel free to contact me if you have any questions or concerns.

Sincerely

SEAN LINDSAY,
General Manager, Labor Relations,
Marine Terminals Corporation.

Adrian Diaz—VP Local 63
Mark Wheeler—WBCT
Robert Owens—MTC
Dave Adano—MTC
Walter Romanowski—MTC
Tim Kennedy—PMA

Senator BREAUX. [presiding]. Thank you very much. I apologize for having to go back and forth, we had a vote on the Senate floor. And I'm sorry for the interruption. Thank you very much for being with us.

Let me start. Mr. Koch, one of the concepts was, to make sure that the cargo that's coming into the United States is safe and secure. After it's in the port, it's very difficult to do that. It's certainly more difficult to do it on a ship in port than it would be to do it when that ship is located in a foreign port, on its way to the United States. And you heard, the Admiral and Mr. Bonner talk about how 38 foreign ports now have adequate inspection-type facilities that we would approve in order for them to be able to ship their products to the United States. And I guess the question is, Suppose we just said, "Look, you're not going to ship to the United States unless and until you have an approved port"—what would that do to your folks?

Mr. KOCH. I think it's the question of the criteria, Senator, which is—are we talking about being compliant with the ISPS code?

Senator BREAUX. Yes, it would have to be something that the United States would say, "Look, if you want your ship to call on the Port of New Orleans or the Port of Long Beach or on Baltimore or whatever, you have to have that ship originate in a port that has an approved inspection system on products that are coming to the United States."

Mr. KOCH. Well——

Senator BREAUX. "Until you have it, we're not going to let you do it."

Mr. KOCH. What I think is important is to draw a distinction between ISPS code and CSI, which is the set of agreements that Commissioner Bonner was talking about, where they put the U.S. Customs people in the foreign ports, have to have the VACIS in-

spection equipment, and have the information sharing arrangement with the foreign customs authority and where after, let's say, a container is identified by ATS as having a question, U.S. Customs asks Dutch Customs, "We want you to look at that." Because that's separate and——

Senator BREAUX. Yes, what would happen?

Mr. KOCH.—beyond the required——

Senator BREAUX. What would happen if we said you couldn't come to the U.S. until you have that system in place?

Mr. KOCH. I think you have to give people a lot of lead time to put it in place. While there are 38 ports on that list, only 18 are currently operational. And it's the kind of strategy that we'd have to sit down with our trading partners and really work through to make sure that we give people enough time that trade is not brought to a halt, and people can plan and know what is expected of them and get it in place in time.

Senator BREAUX. I take it that we're moving to put these systems in place in the larger ports. I'm not so much worried about a ship with a loaded container of explosives coming in from Rotterdam or from Singapore as I am coming in from some small, third-world country, or a Caribbean island, where someone has transported some device to that island to stick on a rusty bucket to come into the Port of Miami or the Port of New Orleans or any of those ports. Many of those ports will never have any kind of a system in place. I mean, they're barely operational. And yet they're loading vessels that are much larger than the one that blew up the USS Cole. Seems to me that—obviously, if I was a terrorist trying to load a ship coming to the United States to do grave damage, I wouldn't load it in Singapore or Rotterdam; I'd do it in some little third-world country, where I'd buy off everybody in the port and load the ship, and ship it on to the United States. I mean, how do we address that? I mean, can we address that?

Mr. KOCH. The potential vectors are so numerous, it makes your head hurt. I mean, I think we have to realize that there are al Qaeda cells in Hamburg, in Spain, in a lot of places, so you can't just assume something coming through Rotterdam is automatically safe because it's coming through Rotterdam. I think you have to use the kind of more sophisticated screening that ATS is supposed to be, which is—you want to know as much as you can about that box, so you can make as intelligent a risk assessment decision as you can.

Senator BREAUX. I take it the answer is yes, but can you elaborate perhaps on how the industry is working with the ports to try to facilitate this—I mean, this is not anybody's sole responsibility. It's not Congress' sole responsibility, it's not the shipping companies' sole responsibility, it's not the longshoremen's sole responsibility by themselves, it's not the port by themselves. It has got to be a coordinated effort, or it will never work. So how are the folks that you deal with working with the ports and with the government to help make this work?

Mr. KOCH. Well, we're trying to support the government on every initiative that we can, whether it's Coast Guard, whether it's Customs, whoever it is. We try to sit down with them and work through these issues. We've supported the 24-hour rule, we've sup-

ported the ISPS code. We're supporting the Coast Guard and its implementation, working through it with them; working with Customs, for example, on these ATS questions, "What information do you want, from whom, when? Let's get agreement on what it is you're trying to build." Then we can define what the gaps are between what we want to have, what we presently have, and then we can sit down and figure out, OK, there's this option or there's this option, and try to work through with them.

I would observe that I think what this security challenge has done is, it has brought labor, carriers, shippers, and third parties actually closer together, because we all recognize there's a common challenge here. We all want to work with the government in every way we can. A lot of this is beyond our ability simply to come up with solutions. If it doesn't work for the government, it doesn't work, because they're the ultimate assessor of what ships get inspected and what cargo gets inspected, as is appropriate. So I think we view ourselves as partners, working with government in any way we can on this, and there's no—as you point out, there's no silver bullet; it's taking every piece, whether it's ship, port, cargo, people, and working on all of them simultaneously, and it's a huge challenge.

Senator BREAUX. Yes.

Mr. LaGrange, you talked about coming to the Port of New Orleans on 9/10, and then the tragic events of 9/11 the next day. Not only in the Port of New Orleans, but in the other major ports around the country, what would you say is different today from what it was on that awful day of 9/11, in terms of security?

I mean, when we had our hearings, quite frankly, I was amazed and appalled at the lack of security in the ports with regard to protective zones around ships in the port and what have you. Going back to the Cole, a little 35-foot boat pulled alongside of a military naval vessel and almost blew it to pieces and sunk it. And yet I saw, in some ports, the only security was a 25-foot fiberglass bass boat that would pull around and point out where the "Do Not Dock" signs are, and it really wasn't much of anything. I mean, that wasn't going to stop anybody intent on blowing up a vessel.

You and I know that in the Port of Houston, New Orleans, Baltimore, and in so many other ports, the port sometimes has, a chemical plant, an LNG facility, an oil and gas refinery, located right in the middle of a city.

What is different today, in reality, in the Port of New Orleans or any of the other ports, that was not there on 9/11, in terms of security?

Mr. LAGRANGE. Just yesterday, here in Washington, the American Association of Port Authorities Legislative Planning Council met in—over 150 corporate members, the major ports, all of the players in the country—and unanimously, again, adopted a resolution supporting $400 million in annual requests needed, and we feel as though for quite some time.

What's difference is, as an example, to use an analogy, the week after 9/11 we were rushed to a scene where a guy in a kayak with a red box on the front of his kayak, in the Mississippi River, had violated the safety zone of the Grandeur of the Seas, Royal Caribbean's cruise line that calls on the port. As it turned out, it was

a guy in a kayak heading to the Gulf of Mexico from Minnesota, and that was his lunch box up on the hull of the kayak.

Senator BREAUX. You all should have picked him just on basic principles of not being——

[Laughter.]

Mr. LAGRANGE. That never would—he never would have been accosted, he never would have been stopped, there wouldn't have been a safety zone on that cruise ship the week before. And that's just a small analogy.

I think where a lot of the problems are happening now—much is happening, but, as I said, not enough has happened, earlier. We just have so many resources and so much wherewithal, and unfunded mandates or partially funded mandates seem to be the order of the day, and we just simply can't stop the order of facilitating commerce for security. The Admiral alluded to, many times, a balance, and that's basically what we're trying to do, balance everything to still make it work and happen.

Senator BREAUX. How is the Port of New Orleans security plan progressing?

Mr. LAGRANGE. Oh, it's—well. It's been accepted. It's not implemented, but it's been accepted by the Coast Guard. It's one of the few that he mentioned earlier. We feel really proud about that. And lion's share of that was part and parcel following the Florida's Ports Council, and starting early on.

Senator BREAUX. So, you have devised a plan, for the Port of New Orleans that meets the Federal requirements of what they would like to see a plan consist of. But you haven't implemented it, and part of that's financial.

Mr. LAGRANGE. Exactly. Eight million of $60 million in needs would be 100 percent implementation at this point in time. The $60 million would.

Senator BREAUX. Do you know if the ports have attempted to raise additional funds in some fashion in order to help implement the plan? Or are the ports saying, "Look, we just need more Federal money, and we're not going to do anything until we get money from Washington?" Have the ports, in general, tried to add more money to their own budgets in this area, do they get the states to help, or the port authorities to help, or do they try generating funds locally to help meet this requirement?

Mr. LAGRANGE. Right. That movement has started. We're doing it in New Orleans on a public/private basis, working with our tenants. We're a land mart port, and the stevedores actually operate our terminals, for the most part, with one or two exceptions. But there is some very casual talk going on—in the fact of—in the case of South Carolina, it has been a little more than casual—the opportunity of looking at some fee, maybe not called a security fee, but some fee that could be imposed at each port individually, dependent on what that port's needs may be. Just recently, in the airport in New Jersey, I noticed on my ticket a $15, I think it was, surcharge for security, a point in case. And our question, at the LPC with the APA is, if airport can do it, maybe we should be thinking about doing it, particularly at the cruise line terminals. The other—how it would be implemented at the other level, I'm just really not sure yet, but we are beginning very casual conversations

and talks about it, looking at the reality of how slow this is going to take to get it at the Federal level.

Senator BREAUX. Just out of curiosity, when a cruise ship comes in, and the passengers disembark and get back on the vessel, the inspections that are done of those movements and the loading of those ships, is under the jurisdiction of the port or is it the Coast Guard?

Mr. LAGRANGE. Customs, for the most part.

Senator BREAUX. Customs, for the most part.

Mr. LAGRANGE. Yes, Customs, for the most part. And there is 100 percent screening of every luggage. But, again—that message was made very poignant and very clear earlier—it's a metal detection only.

Senator BREAUX. Yes, Senator Nelson correctly pointed that out. I visited the Port of Miami, and saw that every single suitcase onboard that huge ship of 3,000 passengers went through a metal detector, but nothing else. So, if I was a terrorist, I wouldn't ship anything metal. They'd get my little pocketknife again, but they're not going to get the plastic bomb.

Dr. Carafano, I did not get to hear your testimony. I've looked through your statement though. We tried to talk yesterday about the type of transportation security risk we have in this country. It seems like we spent four and a half billion dollars, approximately, on airline security, and I don't know what else we can do on airline security that we haven't already done. We haven't come anywhere close to that, in terms of both rail security or port security. If I were a terrorist planning where to attack the United States, I certainly would not go to an airline. I would go to something else that has fewer implemented security measures. That would be either railroads or ports and all their vulnerabilities.

Are ports more vulnerable than airlines, in your opinion?

Mr. CARAFANO. Yes, Senator, of course they are. The real question is, How do you deal with that vulnerability? You know, I'd just like to make two points real quick on that. Virtually all of this infrastructure is in the private sector, and security is part of the cost of doing business. And do believe, at the end of the day, it's going to be—most of the security costs are going to fall, properly, on the private sector to pay for this.

And, now, is there a proper role for the Federal Government? Sure there is. Does the Federal Government have a role in improving critical infrastructure protection? Absolutely. And there are things it should be doing. But I think we have to look at what's an investment in that area, as opposed to how can it really contribute to improving security in the maritime domain. You know, we look at the numbers for critical infrastructure protection, and they're enormous because of the vulnerabilities are absolutely enormous.

Senator BREAUX. Mr. LaGrange mentioned a user fee at the New Jersey Airport. I guess, at the terminal for the airlines. The money's got to come from somewhere. And it's either going to be in terms of a user fee for the people who use the ports, or it's going to come from the taxpayers, who may not directly use the port at all. What would your recommendation be if the ports needed additional funding? I mean, do you have any recommendation——

Mr. CARAFANO. I think——

Senator BREAUX.—about it?

Mr. CARAFANO. Primarily for critical infrastructure protection, I would look for solutions that are based on good, solid business models that—if a port can compete economically, it has to do safety things, it has to do environmental things, and it has to do security things. So I think, in the long term, those kinds of solutions will be most sustainable.

I think in the critical infrastructure protection area, the thing that the Federal Government could do best is to provide consistency to the business model. I mean, we should—I think we should go to multi-year funding for these grants, so people have a clear understanding of how much money is really coming down the pipeline, "What can I really count on?" And then we ought to be very clear, in terms of what our national performance standards are, what we expect state and local governments to do, and we ought to be very clear about what our priorities are and who's going to get this money. And that way, people can approach this with a sense of, "Now I know what assistance I'm going to get."

I really think where we can make our bigger bang for the buck is in domain awareness and increasing counterterrorism operations—you know, finding this stuff before it gets to the port, because the things are so vast. So, for example, I think the biggest bang we could get for our buck would be rapidly increasing funding for Deepwater. I mean, Deepwater cuts across every single mission area in the maritime domain. We know that if we spend a lot more, we're going to get a lot—we're going to get much more capability, and we know exactly what we're going to get for our money, as opposed to when we just buy another fence or a light or a rent-a-cop. And we know we're actually——

Senator BREAUX. All right.

Mr. CARAFANO.—we know we're actually going to create $4 billion, which can then be plowed back into the maritime security role.

Senator BREAUX. The Deepwater Program is a real success, and is going to be a success. I know that we are using vessels from the Coast Guard for patrol boats that are going to be very important to this effort. We are extending their length from 110 feet to 123 feet for some of the patrol boats, and some of the larger vessels, three and four-hundred-foot cutters are all going to be very important in the whole scheme of things. This is something we need to continue. And I think this Committee is going to insist that the Deepwater Program be adequately funded, because of its importance.

With regard to the private money that is being spent by the ports to provide some of their security measures, ports have to be competitive, and I would imagine that there would be some that would say, "All right, if I'm up in New Jersey, I'm not going to do all of this, because the Port of Houston may not do it." So then nobody does it. Is there a way to ensure that there's consistency here? Is the Federal Government saying, "All right, ports, you've got to all do the following things," so that one port in one part of the country will not do it because it'll make him noncompetitive with other

ports. Therefore, nothing gets done. Any thoughts about how we could address that?

Mr. CARAFANO. You know, I think—well, the answer is—I mean, I think we need to say, "You need to do this." But in terms of standards, "You need to provide this kind of security," and then I think we need to leave it up to the ports to determine the best way to do that.

I actually think that ISPS and MTSA provide a good foundation for that. I think what's important is the funding, for example, for the Coast Guard, to make sure that—and, I think, grant funding to complete an assessment, is extremely important. I think it's in funding for the Coast Guard, so they're going back and they're doing assessments and audits and inspections to make sure that people are compliant with the standards.

And I think the Admiral had it right. I mean, I think—well, first of all, when we say, "Who's providing good security, and who isn't," they're going to be more economic competitive, and they're going to get more business. So, in the end of the day, I think a business model will solve that.

And I also think that, you know, if people recognize that they're—I mean, I think in a large sense, the private sector story is, that there is value in security. And Target, for example, recently has created their own brand-new computer system to audit their supply chain. And they did this because they realize that there's money to be made in security. It provides better visibility, it reduces pilferage. And, at the end of the day, if something really happens, the economic loss to all of us is going to be terrible. I mean, there is, I think—I don't think we acknowledge it quite often, but there is money to be made in security, and I think the private sector will respond if the standard——

Senator BREAUX. Oh, there's money to be made in providing the security. I'm worried about the people who have to pay for it. I told them yesterday, I want to go into the dog business, because they're going to be buying a lot of them.

[Laughter.]

Senator BREAUX. The dogs to sniff out everything in the world, and that's going to be a heck of a business to be in.

But, if the Port of New Orleans as an example, provides first-class security facilities and is the most secure port in the world, and the Port of Houston decides, "We're not going to do that." Then a ship has to decide whether they're going to call at the Port of New Orleans, which is the safest, but, by far, the most expensive port——

Mr. CARAFANO. Right.

Senator BREAUX.—they're going to lose business to the Port of Houston. There ought to be some kind of a national standard so that all the ports have to play by the same rules. If one wants to be the most secure port in the world, and the one in the next state over says, "Well, we'll cut it in half, and we'll cut our rates in half," the shippers are going to go use the other port that is the cheapest, but maybe not quite as secure.

Mr. CARAFANO. Well, I do think that MTSA and ISPS provide a good foundation for that. And I also think that, you know, for example, if you were Target of the—and I go back to the point I made

earlier about allowing the private sector to identify and have validated and certified their means of providing a secure supply chain—if you go to the Target of the world and say, "Look, we don't care what happens"—but if, for example, you've determined—or we agree that the Port of Houston is a secure port, and that we can depend on this. So if something goes off in New York, there's no way that we're going to stop stuff in the Port of Houston unless we know for a fact there's a bomb in Houston. Then Target may very well say, "Well, you know something? It makes good economic sense for me to make a deal to move my stuff through Houston, because I know I'll always be able to get through." And I think that, at the end of the day, those factors will become the real driver to—because we need security that's sustained for—you know, we know now it took five to 7 years to plan and execute the 9/11 attack. That fact that there hasn't been an attack is irrelevant. The next attack may come five, ten, fifteen years from now.

Senator BREAUX. Yes.

Mr. CARAFANO. We need a physically responsible system that's going to get us ten or fifteen, twenty years in the future.

Senator BREAUX. Well——

Mr. CARAFANO. I think Federal funding's not going to do that.

Senator BREAUX. Mike, how do you pronounce your last name? I'm sorry.

Mr. MITRE. Mitre.

Senator BREAUX. Mitre, OK. I noticed, in some of our hearings right after 9/11, that there was a lack of restriction and easy access to ports. I mean, people just drove in and drove out with very little checking. There were tourists, in the old days, walking around the port, looking at the port, looking at the big ships. That cannot be allowed today. Things have changed, and people are going to be restricted. I think you spoke about the question that if you're in a port today, you ought to be there for a reason, and it ought to be verifiable. How is that being handled? If some people don't want to be restricted in their activities, is it working all right now? There are many more requirements regarding access to ports and who's there and what your business is. How is that being handled by the workers themselves? Is that an acceptable system, by requiring more identification, and reasons for being in a port?

Mr. MITRE. Well, I think—especially since 9/11, I think there has been a new—almost like a renaissance, a new rebirth, of awareness, the fact that we do need security.

One of the problems with the ports is, they were designed not to be secure. We didn't used to have fences. We could drive——

Senator BREAUX. Sure.

Mr. MITRE.—right up to the ship. So we had always less. And fences and other things are kind of—I don't want to say Band-aids, but are things that have been added on. They weren't built in as part of the infrastructure. The problem is, with what you're talking about now, is this, we used to have a mentality, "No, we don't want an ID, we don't want"—but, you know, really, going back to the Vietnam War, we used to have to have—for probably 6, 7 years, we had a port security card. Everyone had to have one. And, you know, there was no problem, because people understood. But, at that time, we hadn't had an incident domestically. Now that we've

had an incident domestically, our workforce is very much—very, very much more aware. And it's not a problem.

To get on a terminal, you have to have either the company picture ID or your driver's license to get on, and everyone's checked. If you don't have it, you don't come on, and you don't work. And I think we have, now, more self-reporting things about—because we have a number of them—we can call the Coast Guard—that if a terminal isn't asking, we have our own guys calling the Coast Guard saying, "Hey, we have a problem. They're not even asking us for our ID anymore." And for us to switch around the mentality from not wanting it——

Senator BREAUX. Right.

Mr. MITRE.—to that, that kind of answers the question, in and of itself, I think.

Senator BREAUX. Well, I'm glad to hear that. I was particularly interested in your comments about the empty containers. Does anyone have a comment on that? Mr. Mitre talked about, the empty containers not being checked and certified. I mean, if I wanted to load something, I'd go find an empty container I know is not going to be checked, and put whatever I want in the empty container and backload it to somewhere else.

Mr. LAGRANGE. At the Port of New Orleans, in particular—I think a lot of the ports are addressing that—we're performing a study right now, called the "steel wheel shuttle," which will relocate the empties to an outer, more rural, sparsely populated location. It's kind of like putting a Band Aid on something, if you will. But with the resources and funds available, we'll utilize a smaller shallow draft port with good rail access to do that, where the empties could either be railed or barged to that site. But, in the interim, you still have the issue that Mr. Mitre alluded to, you still have the box at that point, and the dangerous point is when it gets off the ship or when it's ready to put on the ship. So that's not the final solution, either.

Senator if I may, I just wanted to add one comment that, for a long time, the Ports Association has been on record, unlike the airports and others, as feeling as though a significant contribution is already being made by the ports to the Federal budget. Customs being one perfect example. So, in terms of your user-fee question a little earlier, I want you to know it's a sensitive issue with all ports. It's not as though we're not trying to solve the solution, but we feel as though we don't have, even at the other infrastructure level, any of those programs in place at other entities like ours.

Senator BREAUX. Thank you.

Can anybody answer this question: When a container box is sealed in a foreign port destined for New Orleans, who seals it over there? Is it the government, or is it the company that does that? Does the shipper seal it himself, or is there a Coast Guard equivalent that says, "Well, we're looking at this box, and this is what's in there, and I'm sealing it?"

Mr. KOCH. The government generally not involved with sealing the box. The time the seal should be applied to the box is by the person stuffing that container, the shipper at origin. That's the time that the seal should be put on. That's the time most seals are put on.

Senator BREAUX. OK, well, how do we find boxes that have illegal commodities in it? I mean——

Mr. KOCH. Well——

Senator BREAUX.—if you've just got a crooked sealer over there that is in cooperation with whoever's trying to ship drugs, or whatever——

Mr. KOCH. That certainly can happen. Or seals can be tampered with, or containers could be tampered with. Sometimes a seal isn't put on at stuffing, but the truck driver will carry it, because they know, "I'm going to go down, I'm going to hit local Customs. Local Customs is going to open the box and look inside of it, so I won't put the seal on until I'm finished with local Customs." In some countries, local Customs pops the seals on every single container, and then re-puts a new seal on. This is an area that requires attention. The World Shipping Council, together with the NIT League and together with the Mass Retail Association, put together a comprehensive seal-verification proposal that we submitted to the government in September.

Senator BREAUX. I think that's a key point in the shipping process. If each box has to have a seal, you could have someone certify that this is what's in the box. You've got to put a foolproof system if, in fact, that person is doing their job.

Mr. KOCH. Well, it's one indicator. It's not foolproof, because, as you point out, Senator, you could have somebody stuffing the box, who has bad intent, and then put a good seal on it.

Senator BREAUX. Oh, I understand. But, I mean, if you had the right person sealing every box, you would be certifying that that box doesn't have a bomb or anything else in it. But it's always a problem making sure it's an honest person doing it.

Mr. KOCH. Which is what the C–TPAT Program is trying to get at, which is, they're trying to identify those importers who will take the steps to go to their foreign manufacturing places, require that a high-security seal be put on at stuffing, and then track it through with their vendors all the way through.

Senator BREAUX. I mean, if we had absolute faith at that point in the process, we wouldn't need all 145 container screeners that screen every box that comes through every port. This is a huge expense.

Mr. Mitre, do you have any comments on these seals?

Mr. MITRE. Yes, you know—yes, I do—you know, one of the things that I think is absolutely necessary to remember is, one of our points about checking the integrity of the seal here is exactly for the reasons that have been made. It's a very quick way to do it. You can see if the seal's been tampered with. And one of the things we always used to do is, the clerk that was down there used to have a list of what the numbers were on the seal. That number will match up with the manifest list. He didn't have to write it down. He could just see it. Someone else putting another seal on it, a dummy seal, that immediately gets it right there. And that was always a very, very important thing. Very important.

The other point, besides that one, is the fact that—let's say, for example, someone was to cut a seal off somewhere to get into the interior of the container, whether they put explosives in it or to steal something, whatever it is, for contraband, or whatever. We

used the recognition of having a seal or not as an indication of something's wrong. And, for example, we have empty lanes at the terminals. Empties don't have seals on them. They should, but they don't. The other day, a container was going through with a seal on it, through an empty lane. And someone just said, "Hey, wait a minute. Why's that thing's got the seal there?" Because, at that one place, he—that's not part of the job, but the guy just happened to spot it. They go, "Hey, take that thing over there and open up the doors. Let's see what's going on here." And they got—I guess one of the Customs guys—and they got it over to the side, and it was full of flat screen TVs. The point is, is that seals, in and of themselves, are a quick, but it's an efficient way to see if something's wrong. And that's why we've made such a point of saying coming off the vessel—we're not asking them to take this huge half-hour thing, but it takes about 30 seconds to check this seal and to check the integrity of it. And I think that's why it's—that's very important.

Senator BREAUX. The seals are not matched up with the manifest when they come off a ship?

Mr. KOCH. Carrier systems should have it manifested, and the seal number should be there. I think the objective we all agree on, I think, if a seal-verification process is in place, and that seal's been checked before it's loaded on the ship, then that should be all that's needed, because it's not going to be tampered with on the ship. Terrorists are not likely to go messing with a container once it's on a ship. Or at least the risk of that is extremely low. So we think if a seal verification's been done properly at the foreign port, you shouldn't need to do it when it's taken off the ship here.

Senator BREAUX. Well, these are all interesting points, and I think all of this has been very helpful. We heard from the Chairman and the Ranking Member. We are making a new effort on legislation to get something going here. In order to guarantee the ports have the means needed to implement the desired security systems. We could have the same degree of security at the ports as we do at the airports, which are much better than before 9/11.

So I think you all have been very, very helpful, and your suggestions have been very, very important. And with that, the Committee will stand adjourned until further call of the Chair.

[Whereupon, at 12:29 p.m., the hearing was adjourned.]

APPENDIX

PREPARED STATEMENT OF HON. TRENT LOTT, U.S. SENATOR FROM MISSISSIPPI

I want to thank the Chairman for holding today's hearing, and thank all the witnesses for appearing before the Committee to discuss this important subject. I worked closely with the Committee on the Maritime Transportation Security Act of 2002, and I have followed the Department of Homeland Security's implementation of the Act's provisions. In general, I am pleased with the efforts to date, but I see that there is still much work to be done.

The Department of Homeland Security is working on a number of initiatives to take advantage of the co-location of the various agencies under one roof. For instance, Customs and Immigration personnel are being cross-trained to handle each others' duties. This will help airports, such as Jackson International Airport in Jackson, Mississippi, to acquire an immigration screening capability with its current Customs workforce without additional personnel. I encourage the Department to expedite programs such as this.

This co-location also provides an opportunity for the Department to eliminate some of the redundant efforts of these agencies to perform the same missions when they were housed in separate departments. For instance, during the 1980s, the Coast Guard and Customs Service both developed capabilities to intercept drug smugglers on sea and in the air. I recommend the Department consider whether to eliminate this duplication and assign each of these two missions to one or the other agency. From my perspective, it seems to me that the Coast Guard's ingrained ship and boat operating, maintaining, and personnel training system is naturally superior to Customs', and that the Customs Service aircraft fleet is more specialized for the air intercept mission than the Coast Guard's aircraft fleet.

I also want to support Senator Snowe's statements advocating an increase in the Coast Guard's Deepwater program funding. It was clear to me at the beginning of this program that the Coast Guard's cutter and aircraft fleets were all reaching the end of their service lives simultaneously and would need replacement during the same 10–15 year period. I understood that the Coast Guard's proposed funding profile was based more on what OMB felt comfortable with than on what was needed to ensure that the Coast Guard's operational capability was maintained, so the time line was stretched out past 20 years. However, as we have recently seen, the equipment is not waiting for the funding to show up before it fails. The Coast Guard is losing operational capability under the current funding profile, and indications are that it will get worse. The Congress should fund the Deepwater program at least at the $1.1M level in FY05 so that replacement cutter and aircraft can be expedited.

On the subject of port security, a great deal of attention has been paid to improving security at our Nation's largest seaports, and rightly so. However, while maritime-based attacks on ports such as Los Angeles or New York would clearly have major consequences for this nation, the hardening of those ports is proceeding at a much faster pace than for smaller ports. As others have noted, terrorists look for vulnerabilities as well as for effect. We also need to ensure that smaller ports with particularly sensitive vulnerabilities are hardened. For instance, Pascagoula, Mississippi has a Navy homeport, a major shipyard that builds Navy combatants, an oil refinery, and a natural gas pipeline.

Thank you all for your attention to our nations' security.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ERNEST F. HOLLINGS TO (RET.) REAR ADMIRAL DAVID STONE

Question 1. Admiral Stone, your agency gave out the first three rounds port security grounds, and in my opinion consistent with the authorizing law. TSA set up a process to require each Coast Guard Captain of the Port to rank all grant applications in the district, after that the Maritime Administration's regional director worked with the Coast Guard to come up with a regional recommendation for rank-

ing all of the grant applications. Grants were then forwarded to TSA where two panels comprised of officials from Coast Guard, TSA, and MARAD gave a final ranking and award. Grants were intended to help ensure compliance with Federal security plans, and prior to the adoption of plans to address Coast Guard identified security concerns. Recently, Secretary Ridge announced that he was shifting all grants the Office of Domestic Preparedness. Are we dumbing down the process, what was wrong with the approach that had been taken?

Answer. The responsibility of securing our Nation's ports is a shared one. The Department of Homeland Security (DHS), the Department of Transportation (DOT), and other Federal agencies are working together to enhance security in partnership with the public and private entities that own and operate the Nation's ports. With the exception of the Office of Domestic Preparedness (ODP) administering the grants, the selection process will not be materially different. TSA, Coast Guard, and the Maritime Administration will continue to provide the necessary operational expertise for the grant programs as required by ODP. These functions include assisting with determination of eligibility and evaluation criteria, solicitation and application review procedures, selection recommendations, and post award technical monitoring. TSA will also continue to leverage existing transportation expertise by working with industry stakeholders, Coast Guard, and DOT modal administrations to assist ODP in ensuring that competitive Federal security grants are awarded to most eligible applications for the reduction or elimination of identified security vulnerabilities at ports.

Additional information. The Office of Domestic Preparedness has become the Office of State and Local Government Coordination and Preparedness.

Question 2. It is my understanding that your agency is working on a risk based analysis of intermodal cargo shipments, to facilitate targeting of cargo for purposes of inspection. It is my understanding that GAO also testified critically, that the Customs targeting system was not being adequately tested. Have TSA and Customs sat down together and critically reviewed each others methodologies? Would not that be the right thing to do?

Answer. We agree that interagency coordination will yield a more robust information analysis and risk assessment approach for the Department. The Border and Transportation Security Directorate is addressing risk assessment issues mentioned above through a multi-agency working group that includes TSA, CBP, USCG, and DOT. This working group is looking at vulnerabilities and security measures across the supply chain. Risk assessment is but one aspect of this review. BTS also has established an Office of Screening Coordination (OSC) that will be reviewing the various existing and proposed methodologies and overall domain awareness and risk assessment tools within DHS agencies that could be interlinked to provide more comprehensive assets to target cargo, vessels, and passengers more effectively. The Office of Screening Coordination will be conducting its review in the cargo analytical arena with the cooperation and participation of CBP, USCG, ICE, DOD, and DOT. OSC will review CBP's Automated Targeting System—Cargo and other targeting and domain awareness initiatives envisioned or under way TSA, USCG, and the National Maritime Information Center. The goal is to leverage all existing risk assessment tools within the Department.

Question 3. How much Federal funding provided by Congress for port security grants remains to be allocated?

Answer. For Fiscal Year 2004, $50 million in Congressionally appropriated port security grant funds remain to be allocated. Applications for this remaining money have been both solicited and received and are currently going through the multi-level, multi-agency review process. It is estimated that grants for the remaining funds will be awarded in the fall of 2004.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO REAR ADMIRAL DAVID M. STONE (RET.)

Question 1. If your Federal budget for port security functions were doubled, in what ways would you use it to improve security?

Answer. DHS has designated the United States Coast Guard (USCG) as the leading operational agency for maritime security issues. Other DHS agencies, including the Border and Transportation Security Directorate, Customs and Border Protection, and TSA, have been delegated lead and supporting roles by the Secretary for various sections of the Maritime Transportation Security Act. As the leading operational agency, USCG utilizes the resources and expertise of TSA, Customs and Border Protection (CBP), and other Federal agencies (Department of Transportation's MARAD, as an example) as part of a team to complement USCG actions within the

overall maritime security regime. Whatever the budget level for port security functions, TSA would continue to carry out its mission in maritime security and continue to support the USCG in its lead role.

Question 2. What is your intention for the use of the $17 million appropriation for OSC? Do you intend to share the results of Operation Safe Commerce with organizations like World Customs Organization, the International Standards Organization or the International Maritime Organization in order to help create an international container security standard?

Answer. DHS anticipates that the Request for Applications for the $17 million appropriated in Fiscal Year 2004 for Operation Safe Commerce (OSC) is on track to be released later this summer, with final award anticipated in the fall. These grants are now administered by the Office of State and Local Government Coordination and Preparedness (formerly known as the Office of Domestic Preparedness) within DHS. This funding will be used to build on current OSC pilot projects, and may include other supply chains. The expenditure of the remaining funds will be fully coordinated within the Department and Congress to ensure that the cargo security efforts through OSC are integrated into broader departmental initiatives to secure the cargo supply chain.

Results from the projects will be used to recommend container supply chain best practices and standards for use by commercial maritime shippers. Results will be shared with all relevant stakeholders, including World Customs Organization, the International Standards Organization and the International Maritime Organization.

Question 3. Are there any plans to expand Operation Safe Commerce to the auto, bulk or break bulk shipping trades?

Answer. As previously stated in Question 2 above, the remaining $17 million in Operation Safe Commerce (OSC) funds will be used to build on current OSC pilot projects and may include other supply chains.

Question 4. What are the goals of TSA and CBP for the Operation Safe Commerce program and how do you believe it can contribute to securing international commerce entering the U.S.?

Answer. It is important to note that the goals for this program support the Department's goals for cargo and supply chain security. One departmental goal is to ensure effective cargo security from point of origin to final destination. In order to ensure that international and domestic approaches to cargo security are coordinated and policies are consistent, under BTS leadership, a working group consisting of personnel from TSA, CBP, USCG and Science & Technology has been meeting regularly. The working group is conducting a gap analysis on existing cargo security and intelligence programs, coordinating existing containerized cargo security programs and R&D efforts to identify synergies, and coordinating existing DHS component activities in the containerized cargo security environment.

The working group's efforts at coordination include applying lessons learned from Operation Safe Commerce as well as leveraging existing CBP programs like the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C–TPAT).

Question 5. How far along is the Department in setting specifications for a "smart container"? Do any effective technologies exist that can be applied at reasonable cost today?

Answer. Through the BTS-lead working group described above, the Department is determining appropriate minimum standards for container security. This assessment will be complete this fall. This assessment includes a review of available technologies to determine what may be required within the short term (12 months) to enhance container security. As mentioned above this group is looking at the results of OSC and other programs designed to evaluate technologies and best business practices to improve container security while avoiding disruption of the flow of cargo. In addition to OSC, CBP is currently engaged with Customs Trade Partnership Against Terrorism (C–TPAT) members in established trade lanes to test Container Security Device (CSD) technology in order to develop standards for a "smart container". Data relative to such technology is assessed upon arrival in the United States and is ongoing. In FY03, DHS initiated the Homeland Security Advance Research Project Assessment (HSARPA) Advance Container Security Device Program with the objective of developing the next-generation shipping container security devices with multiple sensing modalities, "smart" condition monitoring, automated alerting, and advanced communications. HSARPA is conducting this development effort in cooperation with CBP, including the Smart Box Initiative and the efforts of the Applied Technology Division. HSARPA is also conducting this development effort in cooperation with the Transportation Security Administration's Operation Safe Commerce (OSC).

The cost of technology is a major factor when assessing the viability of a certain product. The effectiveness of such technology, however, cannot be gauged without applying it to "real world" testing *i.e.,* applying it to containers in established trade lanes. In order to determine if effective technology exists today that is technologically and operationally viable and can be applied at a reasonable cost, comprehensive testing must be conducted

Question 6. If Operation Safe Commerce was supposed to guide TSA and CBP in creating international standards why is it that CBP announced standards prior to getting results from Operation Safe Commerce?

Answer. The Department is still in the process of setting standards for cargo containers and to meet the MTSA requirements for performance standards in this area. DHS will consider the results of the OSC test bed in the development of these standards. In addition, within the context of the Container Security Initiative, CBP has identified several characteristics of a so-called "smart container". The Department supports CBP efforts to implement voluntary measures, but is still working to determine whether these criteria would be acceptable for an enforceable Departmental standard in support of MTSA requirements. Through a DHS advisory committee, we have engaged industry in a comprehensive discussion of minimum standards. We expect to issue formal standards later this year, with the results of OSC and other relevant programs considered as appropriate.

Question 7. Is CBP involved in guiding Operation Safe Commerce? How?

Answer. Yes. CBP plays an integral role in this grant program by providing input and lessons learned from existing CBP programs like the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C–TPAT). CBP is an active participant in the OSC Executive Steering Committee, and CBP field staff are also involved as requested to assist with testing and operational issues associated with the program.

WRITTEN QUESTIONS SUBMITTED TO HON. THOMAS H. COLLINS AND RESPONSES BY THE UNITED STATES COAST GUARD

Intelligence Programs Within DHS

Question 1. Why are four separate agencies, three of which are in the Department of Homeland Security (Coast Guard, Customs, and TSA), developing distinct intelligence programs?

Answer. DHS component agencies, by virtue of fielding front line officers (CBP inspectors, ICE agents, USCG personnel, TSA screeners, etc.), each have an organic capacity to collect and generate information and intelligence, and each, by virtue of having mission specific operations, need to be able to analyze and disseminate that intelligence to its field personnel. At the same time, it is absolutely critical that that information and intelligence be provided to and analyzed at a higher level within DHS, and shared with other components of the department that did not generate it. For that reason, each of these agencies fields a collection and analysis capability that supports its specific mission, but also engages in robust information sharing with both IA and other members of the intelligence community.

Information Sharing

Question 2. What are you doing to make sure intelligence is being shared among DHS, the Navy, and the rest of the intelligence community?

Answer. The Coast Guard took an early role within DHS to ensure that intelligence products were accurate and available to the DHS Information Analysis and Infrastructure Protection (IAIP) Directorate and throughout the entire Federal Government. The Coast Guard Command Center is co-located with the National Response Center (NRC) sharing threat information and reports of suspicious activities from the maritime industry and other maritime stakeholders. The Coast Guard has been functioning as the Information Sharing and Analysis Center for the maritime industry in accordance with PDD 63 since February 2003.

Additionally, the Coast Guard and Navy continue to build an effective joint intelligence partnership to enhance maritime domain awareness. The Coast Guard's Intelligence Coordination Center is co-located with the Office of Naval Intelligence, which comprise the National Maritime Intelligence Center (NMIC).

The Coast Guard has also provided access to its intelligence databases, advice to other agencies and DHS components developing intelligence-shared architectures, and exchanged intelligence analysts and liaison officers with other agencies and components active in the maritime arena. These liaison officers work with the following organizations: Terrorist Threat Integration Center, Defense Intelligence Agency, Federal Bureau of Investigation, Border and Transportation Security, U.S.

Navy, IAIP, National Security Agency, Central Intelligence Agency, National Drug Intelligence Center, El Paso Intelligence Center, and Joint Intelligence Task Force for Combating Terrorism.

The Coast Guard and Border and Transportation Security (BTS) have also exchanged personnel to enhance data sharing between the CG Intelligence Coordination Center's COASTWATCH (which analyzes information from notice of arrival reports on vessels, people, and certain dangerous cargoes approaching U.S. ports) and BTS' National Targeting Center (cargo tracking process). While both systems are closely related, the Coast Guard's COASTWATCH and the Border and Transportation Service's National Targeting Center (NTC) have developed complementary roles in the area of targeting and tracking cargo, vessels, and people. This effort is enhanced by the exchange of BTS and CG personnel to eliminate duplication of efforts and ensure free flow of information such that the centers act nearly as one entity. The focus and expertise of the two efforts are however, separate functions—one based on a cargo targeting and tracking processes and one based on vessels and people from a law enforcement and intelligence perspective. The Coast Guard and BTS will continue developing practices and policies to improve the capability and capacity of these two systems.

Impediments

Question 3. Are there specific impediments that restrict the ability of the Department of Navy to cooperate with respect to commercial and domestic information and data?

Answer. While the Coast Guard cannot respond directly to the question for the Department of Navy, there is a well-established relationship between the Coast Guard and the Navy for sharing intelligence information specifically for maritime homeland security and maritime homeland defense. This cooperation is most visible at the National Maritime Intelligence Center where the Coast Guard Intelligence Coordination Center is co-located with the Office of Naval Intelligence.

The Intelligence Community components of the Coast Guard and Navy are governed by intelligence oversight laws and policies, which allow for the lawful collection, retention and dissemination of intelligence information while protecting the privacy rights of United States persons.

Support from Intelligence Agencies

Question 4. Are you receiving adequate support and information from the Intelligence Agencies? When you receive a specific warning from the Intelligence Community, how do you disseminate that data down to state and local maritime/port officials?

Answer. Yes, the Coast Guard has received excellent support from the Director of Central Intelligence, Intelligence Community Management Staff, and other Community members on a broad spectrum of issues.

Coast Guard participation in sharing intelligence at the state and local levels is facilitated through the DHS Information Analysis and Infrastructure Protection (IAIP) Directorate. IAIP makes the decision as to what information is shared at various levels of government. DHS promulgates Sensitive Homeland Security Information to facilitate sharing information with our local partners.

The Coast Guard, in coordination with IAIP, uses a variety of methods to share intelligence information with state and local officials:

- Under the Maritime Transportation Security Act, the Coast Guard disseminates intelligence information to state and local officials through Area Maritime Security Committees.
- Coast Guard Field Intelligence Support Teams (FISTs) and Coast Guard Investigative Service (CGIS) Special Agents work closely with state and local law enforcement officials to share intelligence information.
- In close coordination with IAIP, the Coast Guard rapidly disseminates terrorist threat warning information to the maritime industry.
- Some of the coordination between the Coast Guard and state and local governments is formally recognized through various memorandums of understanding, but most are accomplished via numerous working relationships.

Coordinated Security Efforts in Huntington

Question 5. [West Virginia officials believe that the Coast Guard, TSA, and others involved in port security have a bias for coastal ports. These questions related to the Administration's efforts to protect inland ports. The Port of Huntington is the seventh largest port in terms of tonnage handled in the country. Over 50 percent

of the cargo processed at the port is hazardous material. I have a series of questions relating to this port.]

The Marine Safety Office (MSO) in Huntington, West Virginia is responsible for over 300 miles of navigable waterways. Within the MSO Huntington there are 3 state jurisdiction boundaries and upwards of 18 county jurisdictional boundaries. What steps can be taken to make sure the security efforts are coordinated, and that responders are aware and positioned to respond to a maritime terrorist incident?

Answer. The Coast Guard's Port, Waterway and Coastal Security (PWCS) mission is to deter, detect, prevent and respond to attacks against U.S. territory, population, and critical maritime infrastructure throughout the entire Marine Transportation System (MTS). This mission is accomplished through interagency, intergovernmental, and public/private sector cooperative efforts.

As the lead Federal entity for maritime security, the Coast Guard accomplishes its mission in part through Area Maritime Security Committees (AMSC). These committees, which are required by the Maritime Transportation Security Act of 2002 (MTSA), include representatives of law enforcement agencies, intelligence agencies, first responders, vessel and facility owners/operators, as well as Federal, state and local agency representatives. The AMSCs, under the leadership of the Coast Guard Captains of the Port/Federal Maritime Security Coordinators (COTPs/FMSCs) provide a framework to communicate threats, identify risks, and coordinate resources to mitigate threats and vulnerabilities at the regional level. Such a committee has been established for the Huntington region.

The COTP/FMSC in Huntington, like other field commanders throughout the nation, is partnering with the state Joint Task Forces, sharing DHS information bulletins, and working with local law enforcement and emergency response agencies to establish procedures for responding to security threats. These procedures are being proven through exercises and drills. Additionally, the AMS Committees on the inland and western rivers have created "River Watch," a volunteer network to increase awareness and detection capabilities.

Coordination on Different Jurisdiction

Question 6. How do your agencies coordinate security efforts in large multi-jurisdictional areas such as this? And, are we investing in technology that will allow us to maximize resources to protect, prevent, and respond to incidents that could result in a catastrophic loss?

Answer. The Department of Homeland Security's mission to deter, detect, prevent and respond to attacks against U.S. territory, population, and critical maritime infrastructure is accomplished through interagency, intergovernmental, and public/private sector cooperative efforts.

As the lead Federal entity for maritime security, the Coast Guard accomplishes its mission in part through Area Maritime Security Committees (AMSC). These committees, which are required by the Maritime Transportation Security Act of 2002 (MTSA), include representatives of law enforcement agencies, intelligence agencies, first responders, vessel and facility owners/operators, as well as Federal, state and local agency representatives. The AMSCs, under the leadership of the Coast Guard Captains of the Port/Federal Maritime Security Coordinators (COTP's/FMSC's) provide a framework to communicate threats, identify risks, and coordinate resources to mitigate threats and vulnerabilities at the regional level.

To coordinate security efforts in large areas, many COTP/FMSC have established multiple AMSCs to address more specific issues. In those COTP/FMSC areas of responsibility that encompass several geographically separate areas, or when one AMSC has a significantly large membership, COTPs/FMSCs have formed an executive steering committee to oversee the multiple AMSCs. Those geographically separate AMSCs, in turn, may be viewed as subcommittees of the parent AMS Committee.

The U.S. Coast Guard is pursuing a number of initiatives for new technologies that will allow us to detect, prevent and respond to incidents including:

- Nationwide implementation of the Automatic Identification System (AIS) and requiring the installation of AIS equipment on towing vessels in compliance with MTSA requirements;
- Technologies to allow the automatic tracking of barges;
- Enhancing our information systems to integrate results of the Port Security Assessments (PSA) with other security information from the Coast Guard, other Federal, state and local agencies and the regulated maritime community.

Efforts to Secure Huntington, WV

Question 7. What have your agencies done in particular to safeguard inland ports like Huntington? What additional resources—equipment, personnel—have you deployed to Huntington and other inland ports? Have you started developing security plans to address some of the unique characteristics of inland navigation, which possess different security challenges from coastal operations?

Answer. Due to the Coast Guard's multi-mission nature, resources provided to the Coast Guard assist in the performance of all missions. Since 9/11/01, the Coast Guard has added 19 FTP and assigned dozens of Title 10 recalled reservists (current number is 77) toward safeguarding inland river ports, including Huntington. Six new boats have also been located on the inland river, including one in the Huntington, WV. Additionally, in March of 2003, using Title 10 personnel, the Coast Guard established the Inland Rivers Vessel Movement Center to attain awareness of barges carrying Certain Dangerous Cargoes on the inland rivers.

The Area Maritime Security Committee (AMSC), led by the Federal Maritime Security Coordinator (FMSC)/Captain of the Port (COTP), has developed an Area Maritime Security (AMS) Plan for the Port of Huntington. The AMS Plan will greatly enhance the capabilities of the Coast Guard, and other Federal, state and local authorities with securing the Marine Transportation System.

Grant Funding for Inland Ports

Question 8. What percentage of port security grants has gone to inland ports?

Answer. The Transportation Security Administration (TSA) reported that applicants on the inland waterway system received 55 grants totaling $14.7 million through the first three rounds of Port Security Grants. This represents 3.3 percent of the $445.9 million awarded to date.

Resources for the Ohio River Valley

Question 9. Admiral Collins, you are aware, I'm sure, that there is a small Coast Guard detachment in Huntington, West Virginia. The personnel at this duty station oversee inland waterway safety on the Ohio and Kanawha Rivers, but also have some responsibility for ensuring the riverside security of chemical plants and power plants that dot both of those rivers in West Virginia. Are you satisfied that the Coast Guard has sufficient manpower and technological capabilities at this location to adequately protect the lives and health of the residents of the Ohio River Valley?

Answer. Due to our Service's multi-mission nature, resources provided to the Coast Guard assist in the performance of all missions. The President's FY2005 Budget Request includes sufficient resources to perform Coast Guard operations and activities within the Ohio River Valley in FY2005. The Coast Guard continuously evaluates resource requirements and will address any gaps in the Ohio River Valley, as well as throughout the entire Coast Guard.

Staffing Levels

Question 10. Let's pretend that there are no financial constraints on the Coast Guard or Congress. Given risk assessments you have seen, or in the exercise of normal prudence, how would you change staffing levels or the availability of vessels or other materiel at places like Huntington, where the Coast Guard presence is relatively small?

Answer. The FY 2005 Budget supports the Coast Guard resource needs in FY2005 to conduct the full spectrum of Coast Guard missions in Huntington and throughout the Nation and world.

However, the Western River region is one of the highest priorities for consideration of establishing a future Maritime Safety and Security Team (MSST). Within the Western Rivers region, there are six cities that we believe require a greater security posture due to their population and/or throughputs of certain dangerous cargoes. Theses cities are Huntington, Cincinnati, Louisville, Paducah, St. Louis, and Memphis. The Coast Guard's preference would be to centrally locate a MSST to leverage command, training, administrative, and facility efficiencies and deploy detachments as needed to cover as many as six areas concurrently. However this concept of operations would require this MSST to be larger than the standard teams that have been established to date.

PSRAT to Evaluate Huntington

Question 11. When is the Coast Guard going to use the Port Security Risk Assessment Tool to re-evaluate the Port of Huntington Tri-State?

Answer. The Huntington Captain of the Port Zone received a Coast Guard sponsored Port Security Assessment (PSA) in September 2003. As part of the PSA, subject matter experts from the Port Security Assessment Team reviewed the local Port Security Risk Assessment Tool (PS–RAT) scores for facilities covered by the assess-

ment. Based on their expertise and field observations, the assessment team validated the local PS–RAT content and suggested changes, additions, and deletions to reflect PSA findings.

Local Coast Guard port officials routinely update their PS–RAT information and scores to adjust to changes in the threat, consequences, or vulnerabilities related to an asset or activity in their area of responsibility. Coast Guard Marine Safety Office Huntington most recently updated their PS–RAT and re-scored assets in mid April 2004.

Huntington, WV Area Maritime Security Plan

Question 12. The Port of Huntington Tri-State would seem to be a perfect opportunity for the Coast Guard to develop a prototype for area maritime security plans—the area is filled with hazardous materials and chemical facilities, the river system spans a great distance connecting to many states, and coordination and monitoring for both security and contingency response is complicated. I would appreciate it if you would evaluate the possibility of prototyping a system for inland waterway security management.

Answer. The Coast Guard's internal timeline for implementation of the Maritime Transportation Security Act of 2002 (MTSA) called for all Captains of the Port/Federal Maritime Security Coordinators (COTP/FMSC) to prepare an Area Maritime Security Plan and submit it to the respective District Office for approval by 1 April 2004. The COTP/FMSC for the Port of Huntington met this deadline.

While each port is unique, the Port of Huntington was the first of several inland waterways ports to receive a Port Security Assessment (PSA) under the Coast Guard's domestic PSA program outlined in the MTSA. As such, the Port of Huntington served as a baseline for assessing inland port security and identifying ways to minimize security risks and improve the overall security posture at U.S. inland ports. Using the PSA as a foundation, the Coast Guard is taking a systems approach that ties in multiple COTP zones with similar key assets and vulnerabilities to improve security on the inland river system.

Status of AIS

Question 13. The MTSA requires all vessels arriving in U.S. waters to be equipped with transponders to allow the Coast Guard to track their movements by the end of this year (currently oil tankers and cruise ships are carrying them). Last year your budget only requested $1 million dollars for the installation of towers and equipment to monitor shipping. I was able to get you an additional $23 million, but again here we are with another request of only $5 million. Why is it that we can track small aircraft, big aircraft, anywhere in this country. Yet when an oil tanker comes into downtown Charleston, we have no means of tracking this ship?

Answer. The Coast Guard has commenced developing a nationwide Automatic Identification System (AIS) to provide tracking of vessels required to carry the AIS transponders in our ports and waterways. Through the Ports and Waterways Safety System (PAWSS) project we currently have, or will have by the end of 2004, full AIS capability at 9 designated Vessel Tracking System ports:

- New York
- Houston/Galveston
- San Francisco
- Puget Sound (Seattle-Tacoma)
- Prince William Sound (Valdez)
- St. Mary's River (Sault Ste. Marie, MI)
- Berwick Bay (Louisiana)
- Lower Mississippi River (New Orleans)
- Los Angeles-Long Beach

In addition, the Coast Guard is already operating basic (primarily receive-only) AIS installations in the following locations:

- Miami and Florida Keys
- Long Island Sound (Groton, CT)
- Hampton Roads (Norfolk, VA)

By the end of 2004, the Coast Guard intends to have established initial AIS capability (primarily receive-only) at additional locations nationwide. These sites will be determined based on a variety of criteria, including the expected density of AIS-equipped vessels in the area, existing command and control capability to put the data to use, compatibility and support for the more extensive and capable system

currently in the planning stages, and coordination with other needs and assessments.

Requirements for the nationwide AIS project are being developed as we continue to adhere to the Coast Guard's major acquisition process. By adhering to the major acquisition process, the Coast Guard will ensure the proper project planning, analysis and cost estimating is performed as required by the Federal Acquisition Regulations. The intent for the nationwide AIS project will be to use and build upon the initial AIS capability currently being developed and deployed to create a fully integrated nationwide system providing real-time vessel tracking information to compliment other inputs in the development of Maritime Domain Awareness (MDA). The FY05 Budget request of $4 million is adequate because it's the minimum funding level necessary to proceed with the acquisition process in the concept development phase and would include limited AIS deployment capability. The FY05 budget request was based on the strategy to implement as many ports with AIS as possible with funding provided in FY04. Because of the critical nature of a nationwide system, we deemed the best way to proceed long term was through the major acquisition process.

Cost of National AIS System

Question 14. How much, ballpark, would a national system cost?

Answer. The Coast Guard is currently developing an implementation plan for the nationwide Automatic Identification System (AIS) consistent with Coast Guard and Department of Homeland Security requirements associated with major systems acquisitions. Once the Acquisition Project Baseline is developed, a total project cost estimate will be known and we will be able to provide a more accurate estimate of the cost for the number of additional ports that will be outfitted with AIS technology.

Based on its experience to date with Ports and Waterways Safety System (PAWSS) installations, the Coast Guard has found that port geography and vessel congestion are the primary drivers behind AIS infrastructure costs. Additionally, as the Coast Guard expands its AIS infrastructure outside of VTS/PAWSS ports, other factors such as availability of electrical power, communication links, tower availability, and real property will impact the design and ultimately the cost of a nationwide AIS network. Site surveys are needed in order to determine the precise AIS infrastructure required to meet Coast Guard requirements in any particular area.

Because of the differences in installations, the Coast Guard cannot accurately determine the cost of a nationwide AIS system, but a ballpark estimate of acquisition costs range from $62 million to $165 million with a life cycle cost range of $155 million to $675 million. The Capital Investment Plan includes $81 million over five years for AIS, including $4 million in 2005. It also includes $37 million for the final stages of the Ports and Waterways Safety Systems (PAWSS) deployment. The large ranges are reflective of the uncertainties in system requirements and uncertainty over whether the nationwide AIS system will be able to reuse existing or planned Coast Guard infrastructure. The low end of the cost ranges assumes available infrastructure will be used with incremental increases in support costs and no use of satellite systems. The high end assumes some new towers and sites will be required with associated new support costs and the use of some satellite systems (moving AIS from a national to a more international operating picture). In addition, the highest life cycle cost is based on a commercially built and owned system that provides AIS information to the Coast Guard as a service.

Status of Long-Range Tracking System for Vessels

Question 15. Additionally, we authorized the development of a long range tracking system using satellites to allow the Coast Guard to poll movements to track vessels as they enter into our EEZ, or areas of particular sensitivity. Where are we in this program?

Answer. Long-range tracking of vessels is a critical component of Maritime Domain Awareness. The Coast Guard is pursuing a wide variety of means to track cooperative and potentially non-cooperative vessels calling on, or operating near, the United States. We have submitted a proposal to the International Maritime Organization (IMO) that will require ships to report their positions and other information, which will enable the Coast Guard to conduct an assessment of the risk posed by a vessel. While not "ruling out" any system, use of an Automatic Identification System (AIS)-based system would leverage existing/future carriage requirements and mesh with existing systems.

In addition to our efforts through the IMO, we are also pursuing a wide variety of methods to track vessels, such as long-range radar systems, acquisition of information on vessel positions and intentions through other sources, and cooperative ar-

rangements with the maritime industry. Existing capabilities within the government domain will be integrated into a final solution.

Fraudulent MMDs

Question 16. It is my understanding that in the last couple of years the Coast Guard has rooted out widespread fraud in the issuance of documents to foreign seamen, specifically on Panamanian seamen. I also understand that a recent investigation indicated a lesser degree of fraud in the issuance of U.S. mariner's licenses. Please elaborate on this investigation, and what steps you have taken to rectify the issue?

Answer. During the last several years, the International Maritime Organization (IMO) has noted that many credentials carried by seafarers of certain countries, notably Panama and Philippines, are fraudulent, counterfeit, or altered. The IMO has taken steps to encourage these and other governments to provide better security to the credentialing process to ensure that credentials issued are legitimate and more resistant to counterfeiting or altering. In addition, the IMO requested the International Labor Organization (ILO) to revise its 1958 Convention on Seafarers' Identity Cards, with a view to using up-to-date technology for making these documents more useful in confirming mariners' identities. The ILO adopted a new convention in June 2003 and is in the final stages of developing its standard for the biometric information it intends to use in support of the Convention's goals.

On the domestic front, in December 2002, the U.S. Coast Guard and Federal Bureau of Investigation (FBI) initiated OPERATION DRYDOCK, a joint criminal and counterterrorism investigation into national security threats and document fraud associated with U.S. merchant mariner credentials. The Coast Guard and FBI were assisted in this investigation by other components of the Department of Homeland Security, the Department of Justice, Department of Defense, and U.S. Intelligence Community. Approximately 220,000 active mariner records (of which, approximately 95,000 are licenses and 125,000 are merchant mariner documents (MMDs)) were reviewed to uncover possible criminal activity, application fraud and terrorist links. This investigation focused on discrepancies between the information in the merchant mariner credential application and information contained in law enforcement and public records.

The investigation revealed nine individuals that held Merchant Mariner Credentials who have suspected associations with terrorist groups. In addition to these nine individuals, the Coast Guard identified thousands of cases of possible fraud or other problems, including mariners with active arrest warrants. In response to this information:

- The Coast Guard is suspending and revoking unauthorized credentials;
- U.S. Attorneys are pursuing criminal charges where warranted;
- Approximately a dozen people have been arrested because of active arrest warrants that were uncovered as a result of Operation Drydock; and
- The Coast Guard, FBI and the U.S. Navy worked together to screen mariners serving on Military Sealift Command ships carrying troops and material during the war in Iraq. As a result, more than a dozen mariners were removed from service aboard those vessels.

In addition to the OPERATION DRYDOCK investigation of those holding current credentials, in February 2003, the Coast Guard enhanced the security of the credential program by requiring more direct contact with all mariners to verify identification, strengthened the process for conducting criminal background checks for applicants seeking new MMDs, and began issuing MMDs on more tamper-resistant cards. The new MMDs incorporate improvements for increased security including features to deter counterfeiting, such as micro-printing and serial numbers directly connected to a single mariner.

The Coast Guard is fully utilizing its current authority to access public and government databases for the purpose of gathering background information to determine whether an applicant for, or holder of, a merchant mariner's document is a safe and suitable person to be issued such a document or to be employed on a vessel under the authority of such a document. The Coast Guard National Maritime Center currently uses a number of databases to screen mariners seeking credentials, including: public databases, the Coast Guard Marine Information for Safety and Law Enforcement (MISLE) system, the National Crime Information Center (NCIC), which includes FBI terrorism watch list information, the National Driver Register (NDR), and others.

As these initiatives progress, the Coast Guard is continuing its efforts to enhance the security of issuing all credentials to mariners operating in the U.S. marine

transportation system. Thanks to strong Congressional support in the Fiscal Year 2003 supplemental appropriations, the Coast Guard has been able to implement a very robust screening process and more tamper-resistant card as part of the MMD program. Support of the Coast Guard's Fiscal Year 2005 budget request, which includes $8M and 12 FTP specifically for this effort, will enable the Coast Guard to continue its efforts to enhance the security of mariner credentials in Fiscal Year 2005 and beyond to ensure that credentials are never issued to those who pose a threat to national security or marine safety.

Press Reports

Question 17. Admiral Collins, in the summer of 2002, there were a number of press reports about possible infiltration of potential terrorist operatives through containers. I believe the press allegations indicated a number of ports. I specifically recall Savannah and Long Beach. Are you at liberty to reveal the merits of these allegations?

Answer. The National Maritime Intelligence Center (NMIC), a Coast Guard Intelligence Coordination Center (ICC) and Office of Naval Intelligence (ONI) joint command, examined those press reports and concluded that the feasibility of the smuggling information discussed was unlikely and there were no tangential indicators (*e.g.,* stowaway records from the two U.S. ports) to support the reports. However, the Coast Guard, working with its DHS, DOD and industry partners, will continue to monitor this avenue for potential terrorist entry.

Interagency Coordination on Maritime Domain Awareness

Question 18. Admiral Collins, I have heard statements recently about the evaluation of a program to increase our awareness of maritime transportation. I believe the Secretary of Navy was also quoted similarly as endorsing the concept of a maritime NORAD. I think that this is extremely promising. However, I am concerned about the cooperation of the various agencies that collect data on commercial shipping, and last time you testified I asked all of you to try to work together on this issue. Are you all working together to make sure that you have the right information, the right analysts, and the right monitoring equipment to get the best information?

Answer. Yes, the Coast Guard recently organized a National Maritime Domain Awareness (MDA) Summit, cosponsored by the Department of Homeland Security and Department of Defense, and chaired by Admiral Loy and Assistant Secretary McHale. The Summit was intended to bring together the senior leaders of all agencies that have a stake in Maritime Domain Awareness to ensure they are working together. Participants agreed on the need to establish a Senior Steering Group to unify efforts and develop a comprehensive national MDA plan and architecture based on the following guiding principles:

- Build coalitions and partnerships
- Develop and share technology
- Develop standards and requirements
- Integrate and share information
- Drive cost effectiveness

Key Issues in Port Security Report

Question 19. Admiral Collins, in conference on the MTSA, the Senate conferees took the position that port security costs had to be paid for, and in the absence of a commitment of funding by the Administration, and proposed a fee on users of the system. Ultimately, the Senate relented in the face of opposition by the House, however, we required the Administration to file a report within 6 months to explain what they proposed to pay in the way of port security costs, both for ports and for a variety of Federal port security programs. That report is 9 months overdue—when can we expect that report?

Answer. The Resources to Address Key Issues in Port Security report was written jointly by the Coast Guard, Transportation Security Administration and Immigration and Customs Enforcement. The report has been written and is currently in the clearance process within the Administration.

NMTSP

Question 20. Admiral Collins, the MTSA mandates a national plan to allow us to reopen ports to commerce in the aftermath of a terrorist attack, where is that plan?

Answer. The Coast Guard's timeline for development of the National Maritime Transportation Security Plan (NMTSP) spans two years with development of the interim plan by the end of calendar year 2004 and the final plan by the end of cal-

endar year 2005. In addition to working in close concert with the Transportation Security Administration, the Coast Guard intends vigorous engagement with the National Maritime Security Advisory Committee in the planning effort involving recovery of U.S. ports.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. ERNEST F. HOLLINGS TO GARY P. LAGRANGE

Question 1. What would it mean to the U.S. economy if the Mississippi River was shut down for any length of time?

Answer. The vessel collision at the mouth of the Mississippi River on February 21, 2004 is a poignant example of the economic havoc that could be visited upon this Nation by a terrorist act. In this unfortunate incident, a relatively small sunken vessel in this busy waterway channel caused 158 ocean going vessels to be delayed during the four-day closure of the main international shipping channel into the Mississippi River. The closure was absolutely necessary to conduct search and rescue and recovery operations followed by removal of the vessel.

After removal of the vessel, the backlog of ship traffic was cleared and shipping returned to normal within three-and-a-half days.

Estimates are that this incident caused approximately $17 million in direct losses and $68 million in overall economic impacts. Not only were ships delayed but three container cargo ships and three passenger vessels were diverted to other ports. Thousands of passengers were bussed to other Gulf Coast ports which were ill-equipped to handle them on short notice. The cruise lines incurred thousands of dollars in ground transportation costs and reimbursements to passengers for the loss of their vacations.

With more than 5,000 ocean-going vessel calls annually, it should be readily apparent how important this waterway system is to the Nation's economy.

The Nation's economy would experience severe consequences from a prolonged closure of the Mississippi River to deep draft navigation. The Lower Mississippi River port system from the Gulf of Mexico to Baton Rouge handled $227 million tons of foreign waterborne commerce in 2002, valued at nearly $40 billion and representing 18.1 percent on the Nation's international waterborne commerce. American producers exported 27 percent of the total U.S. exports out of lower Mississippi River Ports.

Agricultural products from 17 mid-western states are exported out of the 10 lower Mississippi River Grain Elevators, representing more than 62 percent of total U.S. grain exports.

More than 92 million tons of petroleum and energy related commodities are shipped on the Mississippi River system from Louisiana representing nearly 16 percent of all waterborne import petroleum products.

Question 2. What have you received in Federal funds to help you comply with your Federal mandate and what did you use the funds for?

Answer. The Port of New Orleans has received approximately $8,000,000 in Federal grant funding. The funding has been used primarily for infrastructure enhancements; fencing, lighting, monitoring and gate access technology. Specifically, the cruise terminal fencing has been improved, and the lighting and camera project is underway. The upriver terminal facility projects will provide enhanced fencing, lighting, gate access technology, and new monitoring equipment. Funds were also received for a video teleconferencing system to enhance emergency coordination activities.

Question 3. What are some of the unique challenges in securing the Port of New Orleans?

Answer. The Port is difficult to secure because it runs directly parallel to the city's residential neighborhoods, the central business district, and major tourist attractions. Virtually all of the mandated access control requirements, especially those during elevated alert levels, have a significant potential to adversely affect port and/or city business, especially as it relates to traffic delays. Methods to curtail the affects are possible, but staff intensive. We have no vessel dedicated to river or canal patrol. The emergency response vessel has been providing some security inspections and patrols; however, the added use has taken it's toll on the vessel in the form of increased repairs. Our landlord/tenant status has required more guidance from the regulatory officials, which slows the plan preparation process.

Question 4. What are some of the unique challenges that you face as a river port with respect to security obligations?

Answer. The number of ships that pass through our port each year (6,000) adds to the "vulnerability." The diversity of the types of vessels calling on our port requires that security personnel be more adept at understanding and applying the Federal regulations.

○