

THE 9/11 COMMISSION REPORT AND MARITIME TRANSPORTATION SECURITY

(108-85)

HEARING

BEFORE THE

SUBCOMMITTEE ON

COAST GUARD AND MARITIME TRANSPORTATION

OF THE

COMMITTEE ON

TRANSPORTATION AND

INFRASTRUCTURE

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

—————
AUGUST 25, 2004
—————

Printed for the use of the
Committee on Transportation and Infrastructure



—————
U.S. GOVERNMENT PRINTING OFFICE

97-931 PDF

WASHINGTON : 2005

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

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

DON YOUNG, Alaska, *Chairman*

THOMAS E. PETRI, Wisconsin, *Vice-Chair*
SHERWOOD L. BOEHLERT, New York
HOWARD COBLE, North Carolina
JOHN J. DUNCAN, Jr., Tennessee
WAYNE T. GILCHREST, Maryland
JOHN L. MICA, Florida
PETER HOEKSTRA, Michigan
JACK QUINN, New York
VERNON J. EHLERS, Michigan
SPENCER BACHUS, Alabama
STEVEN C. LATOURETTE, Ohio
SUE W. KELLY, New York
RICHARD H. BAKER, Louisiana
ROBERT W. NEY, Ohio
FRANK A. LOBIONDO, New Jersey
JERRY MORAN, Kansas
GARY G. MILLER, California
JIM DEMINT, South Carolina
DOUG BEREUTER, Nebraska
JOHNNY ISAKSON, Georgia
ROBIN HAYES, North Carolina
ROB SIMMONS, Connecticut
SHELLEY MOORE CAPITO, West Virginia
HENRY E. BROWN, JR., South Carolina
TIMOTHY V. JOHNSON, Illinois
DENNIS R. REHBERG, Montana
TODD RUSSELL PLATTS, Pennsylvania
SAM GRAVES, Missouri
MARK R. KENNEDY, Minnesota
BILL SHUSTER, Pennsylvania
JOHN BOOZMAN, Arkansas
CHRIS CHOCOLA, Indiana
BOB BEAUPREZ, Colorado
MICHAEL C. BURGESS, Texas
MAX BURNS, Georgia
STEVAN PEARCE, New Mexico
JIM GERLACH, Pennsylvania
MARIO DIAZ-BALART, Florida
JON C. PORTER, Nevada
VACANCY

JAMES L. OBERSTAR, Minnesota
NICK J. RAHALL, II, West Virginia
WILLIAM O. LIPINSKI, Illinois
PETER A. DeFAZIO, Oregon
JERRY F. COSTELLO, Illinois
ELEANOR HOLMES NORTON, District of
Columbia
JERROLD NADLER, New York
ROBERT MENENDEZ, New Jersey
CORRINE BROWN, Florida
BOB FILNER, California
EDDIE BERNICE JOHNSON, Texas
GENE TAYLOR, Mississippi
JUANITA MILLENDER-McDONALD,
California
ELIJAH E. CUMMINGS, Maryland
EARL BLUMENAUER, Oregon
ELLEN O. TAUSCHER, California
BILL PASCRELL, Jr., New Jersey
LEONARD L. BOSWELL, Iowa
TIM HOLDEN, Pennsylvania
NICK LAMPSON, Texas
BRIAN BAIRD, Washington
SHELLEY BERKLEY, Nevada
BRAD CARSON, Oklahoma
JIM MATHESON, Utah
MICHAEL M. HONDA, California
RICK LARSEN, Washington
MICHAEL E. CAPUANO, Massachusetts
ANTHONY D. WEINER, New York
JULIA CARSON, Indiana
JOSEPH M. HOEFFEL, Pennsylvania
MIKE THOMPSON, California
TIMOTHY H. BISHOP, New York
MICHAEL H. MICHAUD, Maine
LINCOLN DAVIS, Tennessee

SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION

FRANK A. LOBIONDO, New Jersey

HOWARD COBLE, North Carolina

WAYNE T. GILCHREST, Maryland

PETER HOEKSTRA, Michigan

JIM DEMINT, South Carolina

ROB SIMMONS, Connecticut

MARIO DIAZ-BALART, Florida, *Vice-Chair*

DON YOUNG, Alaska

(Ex Officio)

BOB FILNER, California

PETER A. DeFAZIO, Oregon

CORRINE BROWN, Florida

JUANITA MILLENDER-McDONALD,
California

NICK LAMPSON, Texas

MIKE THOMPSON, California

(III)

CONTENTS

TESTIMONY

	Page
Flynn, Stephen E., Ph.D., Commander, U.S. Coast Guard (Ret.)	23
Gorelick, Jamie, Commissioner, National Commission on Terrorist Attacks Upon the United States	4
Hereth, Rear Admiral Larry, Director of Port Security, United States Coast Guard, accompanied by James Sloan, Assistant Commandant for Intel- ligence, United States Coast Guard	13
Lehman, John, Commissioner, National Commission on Terrorist Attacks Upon the United States	4

PREPARED STATEMENT FROM A MEMBER OF CONGRESS

Oberstar, Hon. James L., of Minnesota	59
---	----

PREPARED STATEMENTS SUBMITTED BY WITNESSES

Flynn, Stephen E.,	37
Gorelick, Jamie	43
Hereth, Rear Admiral Larry	49
Lehman, John	43
Sloan, James	49

THE 9/11 COMMISSION REPORT AND MARITIME TRANSPORTATION SECURITY

Wednesday, August 25, 2004

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

The subcommittee met, pursuant to call, at 2:00 p.m., in room 2167, Rayburn House Office Building, Hon. Frank A. LoBiondo [chairman of the subcommittee] Presiding.

Mr. LOBIONDO. Good afternoon. The subcommittee on Coast Guard and Maritime Transportation will come to order. I am going to start out with an opening statement. We welcome Mr. Secretary, Ms. Gorelick, thank you, and the subcommittee members who are here. We are going to be joined by Mr. Oberstar and probably by Mr. DeFazio shortly. Oh, here is Mr. DeFazio. Peter, welcome.

The subcommittee is meeting this afternoon to review the findings and recommendations of the 9/11 Commission and to examine the current state of security of our maritime transportation system. The horrible events that occurred on September 11, 2001 had a profound impact on the lives of all Americans, including the intense loss still felt by so many families in my home State of New Jersey.

In order to prevent future terrorist attacks on this Nation, we must, as elected representatives, learn from the events of that day and the circumstances that conspired to make such events possible. By meeting today to discuss the recommendations of the 9/11 Commission, we are taking a step further toward establishing measures that will protect the security of the American people.

As members of this subcommittee, we are specifically charged with overseeing the security of the maritime sector. The 9/11 Commission report alludes to the fact that ports and maritime transportation industries may be particularly vulnerable to a future terrorist attack. The introduction of a dirty bomb, or large amounts of explosives into one of our ports could have a catastrophic effect, not only on the safety of the many Americans living in coastal areas nearby, but could effectively halt the global transport of goods and materials.

In order to ensure security in our ports and along our coasts, we must focus our attention on improving the Coast Guard's capabilities to prevent future attacks. The Coast Guard has been, and continues to be, the lead agency responsible for protecting homeland security along our Nation's shores.

On September 11, the Coast Guard played a vital role in coordinating the evacuation of nearly 1 million people by boat from harm's way in lower Manhattan. After September 11, the Coast Guard quickly incorporated additional maritime homeland security responsibilities with the many missions that the Service carries out each and every day. The men and women of the Coast Guard should be commended for the speed and skill with which they have accomplished this feat.

Nevertheless, I believe there are many measures that we can take to improve our awareness of activities occurring in the maritime domain. The Coast Guard has identified maritime domain awareness as one of its major objectives. It is our job to ensure that the service has the necessary resources, technology, and authority to achieve this objective to better secure America's ports and maritime transportation sector.

The Commission's report includes a number of recommendations that call for a system-wide improvement in the national intelligence community so that we may improve the quantity and quality and the integration of information that is being collected. We must focus energy and resources to increase our intelligence capabilities on the high seas and in overseas ports. Increased intelligence efforts in the maritime sector will allow the Coast Guard to further push out our borders, allowing the Service to identify and track potential threats at a distance from our shores.

We must be able to verify the list of ports previously called on by vessels approaching the U.S. We must also enhance our capabilities to both identify the individuals or groups that control interests in both the vessels and the cargo carried aboard those vessels and track the long-range movement of those vessels. Enhancing the collection and dissemination of maritime intelligence data is critical if the Coast Guard is to be successful in securing America's ports.

Like the Coast Guard, this committee has been given increased responsibilities in overseeing the security of the maritime sector following September 11. I believe that we have met this challenge. This committee has worked hard to ensure two unprecedented pieces of legislation that have, for the first time, imposed a state of security in the maritime transportation sector. We are beginning to see the results of the Maritime Transportation Security Act today with the boarding and inspection of thousands of foreign and domestic vessels and the security improvements being implemented at our ports. However, security needs are continually being identified and further refined, and we must continue to develop legislation to adapt and to address these emerging needs. I am interested to hear the testimony today from our witnesses as to what they see as the critical areas that remain to be addressed.

Finally, I would like to echo the sentiments that have been so often directed to yourselves and to the other members of the Commission. You and your staff are to be commended for the bipartisan manner in which this report has come forth. We thank you for your service.

Mr. DeFazio, do you wish to open?

Mr. DEFazio. Yes, in Mr. Oberstar's absence I will. Thank you, Mr. Chairman. With deference to Mr. Oberstar, I will substantially purloin his opening statement.

America is vulnerable to a terrorist attack. Our maritime transportation system is vulnerable to a terrorist attack. We have over 95,000 miles of coastline. We import more than 7 million shipping containers annually. Thousands of tankers carrying oil and hazardous materials enter our ports each year, and millions of vacationers enjoy their holidays on cruise ships.

Beginning July 1, every ship and port facility was required to have implemented a security plan approved by the Coast Guard. Yet, somehow, I think we are missing the big picture.

Eighty percent of the drugs that are shipped out of Colombia by water penetrate our security and reach our shores. It would not be difficult for a narcoterrorist to smuggle a weapon of mass destruction into the United States using the same means and paths. Less than 4 percent of the containers that enter the United States each year are fully inspected. It would be easy to secret a weapon of mass destruction in one of those with a GPS triggering device and when it reached a certain point in the United States, it would detonate.

Terrorist organizations have used suicide operatives to attack civilian and military maritime platforms with small boats, loaded with explosives. Al Qaeda used these methods in the October 2000 USS Cole and in the October 2002, M/V Limburgh incidents. Other terrorists used these methods in the April 25, 2004 attack at the Basra Oil Terminal in Iraq.

These tactics could be used against cruise ships; LNG, liquified natural gas; chemical tankers, or offshore oil facilities, or other ships. For example, the LOOP oil terminal off the coast of Louisiana handles 25 percent of the U.S. imported oil. A small boat with explosives attacking that facility could severely cripple our economy that depends upon those imports.

Yet, the administration has not developed a coherent strategy that can realistically thwart these types of attacks other than designating areas as security zones, which is like simply posting a "no trespassing" sign over a high security area. The Congress authorized the Coast Guard to lease additional aircraft for a West Coast Helicopter Interdiction Tactical Squadron. Yet, the administration has failed to lease these aircraft.

We could be lucky next time and discover a bumbling terrorist, like the alert Customs agent did at the ferry in Port Angeles, Washington. But maybe we will not be so lucky and there will be a successor to the 9/11 Commission trying to get the government to address our security problems.

It is not too late. The turf wars within the Department of Homeland Security need to end. We need to clarify which agency is in charge of which area of security. We do not need to have the Coast Guard and the Border and Transportation Security Directorate both operating ships on the water.

When the Committee wrote the Maritime Transportation Security Act of 2002, we viewed it as the beginning of our major involvement in improving security along our Nation's waterfront. While some would say that you must centralize congressional oversight so that one committee has a single mission to oversee the homeland security activities of the executive branch, you also must have an expertise in transportation to protect our Nation from the

threats that can be launched through the transportation system. This committee brings that expertise to the table.

I look forward to hearing from today's witnesses about what more we can do to help prevent another attack against America using our transportation system as a weapon.

Thank you, Mr. Chairman.

Mr. LOBIONDO. Thank you. Mr. Gilchrest.

Mr. GILCHREST. Just briefly, Mr. Chairman. I would like to thank the witnesses for coming this afternoon, and I look forward to the testimony from the Commission, from certainly the Coast Guard, and from our other witnesses, to understand how the Congress can be an active, positive participant in securing the ports and the waterways of the United States by coordinating our activities, not only with the various and sundry Federal agencies, but also with the private sector, with the ports, and with our international friends.

So we look forward to your testimony and we will take your recommendations to heart.

Thank you, Mr. Chairman.

Mr. LOBIONDO. Thank you, Mr. Gilchrest. Mr. DeMint.

Mr. DEMINT. Mr. Chairman, I will pass on an opening statement. I am ready to hear the testimony. Thank you.

Mr. LOBIONDO. Thank you.

TESTIMONIES OF JOHN LEHMAN, COMMISSIONER, NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES; AND JAMIE GORELICK, COMMISSIONER, NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES

Mr. LOBIONDO. Again, we welcome you and thank you for being here and for the work you have done, and please proceed.

Mr. LEHMAN. Thank you, Mr. Chairman, and thank you for inviting us. We are here as we have conducted ourselves in the prior 20 months with a total unity of effort and purpose, and we have submitted a unified statement for the record, and I will only briefly touch on some of the points that have already been mentioned that are key to our report.

We certainly appreciate and applaud everything this subcommittee has done with the Maritime Security Act in particular. It is a tremendous step forward. We agree with Mr. DeFazio's view that congressional oversight is crucial to this and that if there is one committee in each House for homeland security, there needs to be the maritime expertise in the specialized expertise in subcommittees, and I think this subcommittee in particular has demonstrated an exemplary role in producing bipartisan legislation.

But there is a lot more to go. We have concentrated in particular on the need for congressional reform. While much of the attention in our recommendations has gone to the reorganizations that we are recommending in the intelligence community and in the executive branch, a true partnership is the only way successful policy can, over time, succeed, and the example of a subcommittee where tenure and expertise and seriousness of purpose in the substance

of what is a complex matter, maritime security, is an excellent example for the rest of Congress to follow.

Maritime security, in many ways, is a much more difficult issue to deal with than aircraft security, because there is a much greater geographic area to deal with in terms of port aircraft having to come to large airports, and ships and small boats have the whole coast to penetrate in terms of smuggling in weapons and terrorists. We have grown a global economy that is utterly dependent today on the rapid movement of people and products just in time, manufacturing, personnel moving quickly, commodities, particularly petroleum, moving unimpeded in a world market. This is an almost irresistible target for terrorists, and we know that they are planning on targeting these vulnerabilities, vulnerabilities in the infrastructure which you have mentioned.

We are not today adequately prepared to deal with the range of threats that we know are being planned by our enemies, and we do not have time to wait. We have to start with an overall strategic plan. You on this subcommittee have to be a major initiator or provocateur in seeing that this happens so that there is a strategic overview and an allocation of resources based on threat and based on risk and not on pork barrel and not on bureaucratic imperatives.

So we think you are off to a very good start in this matter. This is not something new to you at all, and we think that the opportunity to build on what you have already done with the Maritime Security Act is very attractive, without an enormous increase in resources, certainly as resources have to be increased.

But this is an achievable objective, and as we talked about earlier, some of us, on the aviation security, the approach of this committee has to be that this is not a goal line that we have to get across and once we are there, we can turn to other problems. We have to, you have to see that the executive branch adopts a culture of constant change, of constant improvement, because the threat is constantly changing, and this is a very innovative, agile, intelligent enemy that we are going to be facing for the next decade or more.

So our approach to dealing with it and being ahead of them in having better defenses around where they are going to come depends on a constantly improving and ever-flexible, changing and adapting culture in the executive branch. And it will not happen by itself, because bureaucracies seek steady state, and without the responsible provocation and energizing from Congress, you will inevitably see it settle into a stasis in which the enemy then moves well beyond and we will see another 9/11.

So I am looking forward to your questions, and now I would like to have my fellow Commissioner say a few words.

Ms. GORELICK. Thank you, John. We were very lucky to have a former Navy Secretary among our Commissioners, and you can be assured that the interests of maritime security were well represented on the Commission, both in terms of perspective and expertise.

I would make and emphasize four points. First, neither the agencies themselves nor this Committee can do the jobs that need to be done unless they are good consumers of intelligence. One of the overarching themes I think that you see in our report is that intel-

ligence is only as good as the pressure from the consumer to have good intelligence. So the questions that you ask of the agencies that you oversee have to be informed by the intelligence community's best assessment of the risks to our maritime security. It is as simple as that. That has to be your baseline. You have to insist, in my view, that the agencies that you oversee do that, and you have to have a very good window into that yourselves.

Second of all, the strategic plan has to match up against those risks. So, if you get a strategic plan that does not reflect in your view the risks as presented by the intelligence community, then you have a very good basis for rejecting it or asking hard questions about it. I think your insistence on having a plan is critical. When we looked at congressional oversight generally, we found an inability to look strategically across a group of agencies, an inability to understand what the problem was that they were trying to address, what their strategy was in trying to address it, and what the obstacles were to achieving the strategy.

And you have deep expertise in this Committee to do just that. I think your insistence on having a plan that you can scrutinize is absolutely right.

But the third question, then, is what are the obstacles to achieving the plan? Although we did not spend a tremendous amount of time on the particular issue of maritime security, we did see throughout the Department of Homeland Security—in part because of its newness and, on the issue of maritime security because of the fact that we have Customs, border protection, Coast Guard all addressing the same threat—you see the need for deconfliction of roles and missions. That is a perfect role for congressional oversight.

And then I think, as John said, it is important not to assume that once you have set a strategy and identified the obstacles and tried to address those obstacles, that your work is done. Because one thing we learned in reviewing reams of intelligence about al Qaeda and its antecedents over 15 years, is that it is agile and pretty sophisticated.

We saw a group of people in remote areas of Afghanistan—where they frequently do not have functional electricity, where their communications systems are not anywhere near as sophisticated as ours—who had a pretty good view of our society and its vulnerabilities. They were far away to us, but we were not far away to them. And they will probe, and they have probed, the vulnerabilities of our ports and our shores.

So I join with John in commending you for the interest that you have taken on this Committee in these important issues. I urge you, really urgently, to hold the agencies' feet to the fire in terms of developing a strategic plan and hone in on the obstacles—both bureaucratic, and in terms of expertise, financial and otherwise—to achieving the plan. In our view, if you do that, you will more than have met your responsibilities and will have added immeasurably to the security of our country.

Again, I join with John in thanking you for the interest that you have taken in this subject and for your tenacity in pursuing the difficult goals in front of you.

Mr. LOBIONDO. I thank you.

Mr. DeMint, do I understand you have a time conflict with a flight?

Mr. DEMINT. Yes.

Mr. LOBIONDO. I will let you start off then.

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

I want to thank both of you for being here. I have found nothing gets done until someone is willing to propose some solutions and put some ideas on the table for the rest of us to shoot at, and I appreciate you doing that. I assure you we will not be shooting at you today.

But this is very important to me. I am a Congressman from South Carolina; the South Carolina ports are the fourth busiest in the country. Port security is something that comes up all the time. So we are very interested in what you have done in this report. While there could be some things we disagree with, you have certainly given us a focus and a sense of urgency which we need to pursue, and I appreciate the chairman getting us started here today.

I just wanted to hear, and Mr. Secretary, I will start with you, just to talk a little bit more about potential solutions related to the port security, what the Coast Guard's involvement is perhaps in the surveillance, sensing devices, and I know while the report did not get into a lot of specifics, it did suggest that you thought that we should allocate our resources for security based on an evaluation of transportation assets, and certainly that involves shipping, air cargo, a lot of other things that are in the port.

So my question to you really is, if you would talk a little bit about what your vision is, and just from discussions with other commissioners of what is the most cost-effective means of providing port security without sacrificing the flow of commerce? I appreciated you referencing just-in-time inventories and things that are—I mean these ports have worked on productivity and efficiency. We have to figure out some way to keep our country safe and, at the same time, not allow them to disrupt commerce, which is their intent, to get at our economic foundations.

I mean, you have mentioned tracking and sensing devices, but—and we want to try to take some of those ideas and move them forward with specific, strategic plans, as you mentioned, really tactical options. But I would like to hear you and perhaps both of you talk just a little bit more about ideas that you have, particularly in port security.

Mr. LEHMAN. Well, thank you. I firmly believe that the opportunity here is a dual one. It is not a trade-off between efficiency and security.

As a country, we are well behind the levels of excellence in other places like Singapore, as you well know, and the technology that is employed in our ports. By applying state-of-the-art technology in port management, particularly with regard to containers, you bring in technology that in and of itself, even though you may invest in it for economic reasons, brings you much better security, and I am sure you are familiar with the technologies that I am talking about.

So a little bit of investment goes a very long way in bringing up the ability of the Coast Guard to tremendously improve the level of security, while not adding friction, which would be the worst

thing, but actually easing up and opening up and taking away friction from the way our ports operate today.

Resource allocation has been touched on earlier. We believe as a Commission that there has not been any top-down, strategic look at allocating the resources, with 90 percent going to aviation and 10 percent going to everything else. That is not the fault necessarily of the agencies, of the administration, so much as, in my judgment, and here this is not a Commission finding, but my own particular view, the problem is the problem of the 90 committees and subcommittees that want a piece of the action in homeland security. And that is why we have put the objective of congressional reform right at the top of our list.

Second, we need to recognize that there are resources available without having to spend money. The United States Navy does most of its training and has most of its ships in home waters all the time. And they can be made available, put under OP CON in certain circumstances while they are training at home for homeland and port security. Naval reserves. The Coast Guard has a tremendous relationship with the pleasure boat world. The Coast Guard auxiliary, and so forth. There are many resources that can be harnessed that can fill in many of the geographic gaps that we have. And I think the Coast Guard is well on top of these issues. We can take confidence that we really have an energized and professional force that is finally beginning to get some of the resources that it has long been starved of.

So I remain optimistic about our ability to deal with this, but we have a long way to go.

Mr. DEMINT. Mr. Chairman, could I just ask for a quick follow up from Ms. Gorelick.

Ms. GORELICK. Thank you very much. My follow-up would be extremely quick. I would only add this: do not forget the private sector. We have a very innovative private sector with tremendous abilities to contribute technologies that can help us leap-frog some of the countries that currently do this better than we do. One of the things that I would suggest is that you review with the Department of Homeland Security its practices with regard to the private sector. How is it procuring the finest technologies? What assurances can it give to an innovative developer of technology that it will not be penalized if its innovations do not perform perfectly? Take a hard look at the way in which we are intersecting as a government with private companies that want to help.

I am a lawyer in private practice. I represent companies who ask me, "How can I help? How can I, how can I tell the Department of Homeland Security about the products that I have that might help?" The government has never been particularly good at this. Both John and I have worked at the Defense Department which, goodness knows, has tremendous interest in working well with the private sector but has nevertheless had its problems. So it is not a surprise that this would not come naturally.

But here, we do not have any time to waste and we do not have any brain power to waste. So I think it would be well worth inquiring of DHS, "How are you looking at the technologies that are available out there and trying them out to see what can be most effective in facing the challenges that you have identified."

Mr. DEMINT. Excellent perspective. Thank you both.

Thank you, Mr. Chairman, and I appreciate my colleagues accommodating my time problem today.

Mr. LOBIONDO. Happy to accommodate you, Mr. DeMint. Good, safe, traveling.

Mr. DeFazio.

Mr. DEFAZIO. Thank you, Mr. Chairman.

Commissioners, I would ask you to—I mean you noticed the disproportionate investment in aviation versus port and/or other areas of transportation and vulnerability. From your deliberations and/or investigations, where would you—I mean we have a number of places; we have aviation, and we talked about those problems earlier and extensively with Commissioner Lehman, but in terms of maritime transportation, ports, rail, other infrastructure, where do you think we should be putting funds? Do you think that we are over investing in aviation, or do we just need to make the whole pie bigger and make more investments in ports and other sectors of transportation?

Ms. GORELICK. We did not ourselves make the comparative risk assessment that we think needs to be made, but we did hear from the GAO and from other experts who suggested that the current allocation is not proportionate to the risk, and that we are in danger of fighting the last war.

One of the reasons I started my comments with urging both the agencies themselves and this committee to be good consumers of intelligence is that it is important to force the intelligence community to outline the risks and to identify, to the extent that they can, the capabilities that they see on the part of terrorists. Had that been done prior to 9/11—had there been a sweep, for example, of all of the intelligence that we had about the intentions and capabilities of terrorists to utilize airplanes as missiles—we could well have configured the way in which we defend ourselves more effectively.

The same is true with respect to maritime security. We only have to look at the COLE. We know that terrorists, and al Qaeda in particular, have identified maritime avenues for threatening U.S. interests. The question is, where do you rank these threats? Our intelligence community is assigned the task of identifying and ranking risk. You ought to be the beneficiaries of that, as should be the agencies that you oversee. Otherwise, what are you to make of the current allocation?

Mr. LEHMAN. One of the frustrations in our investigation was as we looked and looked through the various agencies, we found no real overview, no strategic analysis that has been done as to relating the levels of risk from which you could plan and allocate a reasonable proportion of resources. I certainly do not think too much is being spent on aviation security today, which would mean, and we all agree on the Commission, that there is not enough going to the other, then clearly, there is an underfunding problem in rail, marine, and other modes and nodes.

Because we know from interrogations and other sources of intelligence that there is a very keen interest in economic disruption as a tool, not in addition to killing masses of innocent civilians; there is a belief in many quarters of the Islamist terrorist world that our economy is very fragile, that the economy of the West is very frag-

ile, and that by hitting the nodes, the most vulnerable nodes, forcing, for instance, because of a disaster perhaps involving weapons of mass destruction, forcing the inspection of every container that come into the United States would bring the economy practically to a halt.

So we know they know that. We know they are planning that. Yet, the overview strategic planning has not been done to allocate the 50 most vulnerable or most important ports in the United States. There should be a threat analysis for each of those ports. There is none. Why is there none? I mean, that is the kind of thing that you need to really bore in on.

Mr. DEFAZIO. Thank you.

Thank you, Mr. Chairman.

Mr. LOBIONDO. Mr. Gilchrest.

Mr. GILCHREST. Thank you, Mr. Chairman. I think maybe the first thing we ought to do today is find out the 50 most vulnerable ports in the United States and why they are vulnerable.

Mr. LEHMAN. We would have to go into classified session for that.

Mr. GILCHREST. Maybe we could find that out by the end of the month.

The maritime industry is extraordinarily efficient in and of itself. The private sector, the shippers, and it is my understanding they try to make sure that a Greek ship is able to transport a 6 pack of Heineken for 2 cents cheaper than the a Chinese ship. So these guys are really pretty efficient. I guess I have 4, and I know, to some extent, I do not represent the Port of Baltimore, but it is in the State of Maryland, and for years and years and years, the maritime industry has, in my judgment, pitted the Port of Baltimore against New York, against Norfolk, Virginia, against ports in South Carolina to get those ports to come up with the best type of off-loading mechanisms, technology; otherwise, they will not come there and you have to dredge deeper and deeper and deeper; otherwise, we are not going to go there.

So these guys are sophisticated, they know the ports that they go to like a fine tooth comb. And I guess my question is, how much cooperation has there been post-9/11 with the maritime community insofar as transparency is concerned, who owns these ships, who is the flag, the State flag of where these ships originate? Do the insurers of the maritime community, have they cooperated in trying to ensure that the point of origin of a particular cargo is inspected, I mean cooperating with the United States? Is there much cooperation with the maritime community, with the IMO, and interested international parties, specifically the United States, in finding the whole mechanism from the time that you put a piece of furniture into a container and then that gets put on a ship, and then it leaves a port and goes to another port, another port, and finally ends up in Philadelphia or Baltimore. Has the Commission seen an overall sense of urgency and cooperation by the international community in finding ways that they can reduce the threat, not only from chemical weapons or nuclear weapons, but a container of Anthrax tucked away in a drawer of a dresser that was picked up in Greece and went to Amsterdam and then went to, I don't know, New York, and ends up in Norfolk, Virginia? That is sort of a broad

overview, but your assessment of that, how far behind are we on that?

Mr. LEHMAN. Certainly American owners and insurers have been extremely cooperative, and of course, I would preface this by saying that the Coast Guard is very much seized of these issues, and they are the authoritative responders to this, because we did not spend a great deal of time on that particular dimension of it. But certainly the impression we have is that there is no coordinating leadership in addressing these problems internationally, and it has to be done. Because the maritime world, even more than the aviation world, which is so much, so much of the problem is the domestic internal aviation issue, that the maritime world is utterly dependent on cooperation between the port of embarkation, the port of demarcation, and it is a totally constantly shifting and efficient market.

So there is going to have to be leadership shown through the IMO and other organizations. It is not going to happen by itself, and while—

Mr. GILCHREST. Do you get a sense that the people are waiting for the United States to be that international leader?

Mr. LEHMAN. Yes and no. I mean there are some who fear it because it is going to bring changes that are not going to be welcome to some quarters economically, and of course there is the overall resentment that is abroad in some quarters against United States leading anything yet, for the most part, there is a feeling that yes, only the United States could do this, and even if we do not like them, somebody better start pulling this together, because it is not being pulled together now.

Ms. GORELICK. Mr. Gilchrest, I think that you ask very good questions about both the engagement of the private sector generally, and the relationship between the U.S. and international maritime corporate interests. As John said, we did not really look at this question, but we did look at the Department of Homeland Security's plans and procedures for engaging the private sector generally. I would just make one comment, having been the co-chair with Senator Sam Nunn of the Advisory Committee of the Presidential Commission on Infrastructure Protection, which looked precisely at how is it that the government can help protect the security of the United States when 90 percent of our critical infrastructure is in the hands of the private sector.

So I hearken back to the comment I made a minute ago about how do you fully engage the private sector. Certainly you want to make sure that your rules are not so rigid that the private sector will be deterred from offering its best technology. But the other thing that needs to be done is that the rules for having those conversations need to take account of what it is like to be in private business. It is an act against nature for companies to sit with their competitors and share their vulnerabilities. It just does not happen, and it will not happen on its own.

Unless there are ways of protecting and securing competitive information unless there are ways of protecting companies from charges that they are behaving in an anticompetitive way; unless there are ways of protecting from public disclosure private information that is critical for the government to know, then those con-

versations are not going to happen the way they need to. It is my guess that what is true for the energy industry, for the financial institutions industry, for the defense industry is also true for the maritime industry—that they need both help in creating an infrastructure where they can talk, and rules that will allow them to speak freely and constructively with each other and with the government. I think your question is excellent and it is a very fruitful area of inquiry for you.

Mr. GILCHREST. Thank you very much. It is always nice when some people think your question is good.

Thank you, Mr. Chairman.

Mr. LOBIONDO. Thank you, Mr. Gilchrest.

I think what I am hearing is that you believe that we need to press the Department of Homeland Security, for an overall plan, specifically as it relates to maritime, but the Commission did not look at making any specific recommendations for the maritime side of this specifically. And even more specifically, I think your report makes brief reference to the need to intensify the efforts to identify, track, and screen maritime cargo. Did the Commission investigate the possibility of maritime cargo containers as a means of importing either material to carry out a terrorist attack or terrorists themselves? Will the Commission issue specific recommendations to us to improve the screening of cargo? Did you get that far?

Mr. LEHMAN. We certainly got far enough into it to know that the threat is very real, that there has been planning, it is an area that our enemies have indeed focused on. And we saw a great disparity in the level of interest from the Islamist terrorist world compared to the level of effort to deal with those security measures. Certainly x-raying and bar-coding and those kinds of technologies are part of the solution, but we did not go beyond the fact that it was beyond our purview, if it was look as we might through the bureaucracy, we found no place where we could find a framework to evaluate the efforts that were being done. It just—it is at such a beginning stage, as was mentioned earlier. Four percent at most are looked at in some way.

So what we have done, again, our approach in our report has not been to provide an exhaustive list of nice-to-haves and must-haves, but to highlight. We only made 41 recommendations, because we wanted to concentrate on those things that we felt were the most important and not try to get into the level of detail that the expertise in your committee and your staff would be essential to carry out. We found insufficient basis of evidence that work was being done within the bureaucracy to make a clear set of specific recommendations, other than the ones that we have made, which are we have got to get on with it, recognize the nature of the problem, the insufficiency of the resources, the availability of resources that are not being harnessed in technology and the private sector, and urge that the administration and Congress, and specifically this subcommittee, get on with it at a very high priority.

Mr. LOBIONDO. Can I ask you just to elaborate a little bit on something you commented on earlier, about the Navy possibly being a partner for resources with port security, how that would work, in your view?

Mr. LEHMAN. Yes. Well, this is beyond what we actually evaluated in the Commission; it is more drawn from my own experience as Secretary of the Navy. In the East Coast at any given time there are dozens of naval ships in home waters exercising, operating and so forth. There are a significant number of Reserve ships operating out of gulf ports and East and West Coast ports, although now far fewer than there used to be. But the Navy is just moving to a very innovative new way of deploying. Rather than the 6 months workup, 6 months deployment, 6 months repair, the Navy has now shifted and is in the process of shifting to deploying on an exceptional basis for shorter periods, for surge and for crisis management and spending much more time operating and training in home waters. As you know, the instrumented test ranges for the Navy and Air Force are all up and down all of our coasts. So we have that presence there. It was like, you know, we had a total of four aircraft on alert on 9/11 on the whole east coast, yet we had probably 500 or 600 aircraft, military aircraft flying that day on the East Coast, not harnessed into NORAD, because they were, the belief was that there was no more threat.

So the resources are there. You do not have to buy new ships if you couple up the homeland security and Coast Guard to the available training that naval ships are doing in port. I might say the Army actually has a larger fleet of relevant boats in American ports than the Navy does, so I would not leave the Army out.

So these resources are there, and if they can be coupled in while they are—and it has been done in the past. It just takes somebody to decide that this is a priority to do, and that can plug a lot of holes, in my judgment.

Mr. LOBIONDO. OK.

Well, I thank you, Secretary Lehman, Ms. Gorelick, thank you very much for being here today and for your work on the Commission. We will take a brief adjournment until we move to panel 2.

I would like to thank our second panel. Admiral Hereth, we thank you for being here today. You are the Director of Port Security for the United States Coast Guard. The Admiral is accompanied by James Sloan, Assistant Commandant For Intelligence for the United States Coast Guard.

Admiral, thank you. Please proceed.

TESTIMONY OF REAR ADMIRAL LARRY HERETH, DIRECTOR OF PORT SECURITY, UNITED STATES COAST GUARD ACCOMPANIED BY JAMES SLOAN, ASSISTANT COMMANDANT FOR INTELLIGENCE, UNITED STATES COAST GUARD

Admiral HERETH. Always a pleasure, Mr. Chairman. Thank you very much.

I am the Director of Port Security and the Coast Guard's Marine Safety, Security, and Environmental Protection Directorate. I am pleased to be here with Mr. James Sloan who is our Assistant Commandant for Coast Guard Intelligence. It is a pleasure to appear before you today to discuss the Coast Guard's continuing efforts to improve maritime transportation security. It is also appropriate that we appear together, because intelligence and port security must go hand-in-hand if we are to secure our Nation's vast maritime arena.

First, on behalf of the Commandant, we would like to thank the Commission for the service they provided to the Nation and for their thoughtful deliberations and recommendations on how we can further secure the homeland. We would also like to thank this subcommittee, Mr. Chairman, for your tireless efforts to secure final passage and enactment of the Coast Guard and Maritime Transportation Security Act of 2004. It is important legislation that will help us continue enhancing security and reducing maritime risk.

As recognized in the Commission's report, the Nation's maritime transportation system is vast and diverse. The system spans 26,000 miles of commercially navigable waterways. It accounts for \$800 billion of freight trade each year and is used by 180 million ferry passengers and 78 million recreational boaters. Protecting this system is indeed a significant challenge.

A maritime terrorist attack with its associated ripple effect through our country will have a dramatic impact on trade and commerce and will severely impact on the Nation's economy. So we must focus our efforts on preventing such an act.

While we take great pride in the progress we have made since 9/11 to improve maritime security, we are intent on pressing hard for greater improvements. For the Coast Guard, that means continuing the aggressive efforts to build capability and apply resources related to risk to support our maritime security strategy. The four key pillars of that strategy are: awareness, through enhancing the maritime domain awareness program that we are trying to emphasize; building prevention through enforcement of our effective domestic and international security regime; increasing protection by improving our operational presence and by leveraging State, local, and private sector capabilities; and improving our capability to respond and recover should an incident happen.

The core of our maritime domain awareness efforts revolve about the development and employment of accurate information and intelligence, and knowledge of vessels, cargo, crew, and passengers, and extending this well beyond our traditional maritime boundaries. All of the DHS's components are working hard to provide this layered defense through collaborative efforts with our international partners to counter and manage security risk long before they reach a U.S. port.

While we have taken some steps to improve maritime domain awareness, we have implemented the 96-hour advanced notice for arrival requirement for vessels; we have accelerated the implementation requirements for AIS equipment; and we have stood up joint operation centers. We still have much to do, however, to ensure an adequate level of maritime domain awareness.

To help that, we have set up a specifically dedicated staff, an MDA staff, to coordinate those activities and to encourage collaboration with all agencies in the government that share our goal.

Regarding building a security regime, much attention has been paid to the implementation of MTTSA and IPSP. This is certainly a major part of our prevention strategy. Our domestic efforts and international efforts have focused on implementation in a very short period of time centered around that one July date. We are also intent on improving supply chain security. And our basic premise is that since trade is global and terrorism is global, we

thought it was necessary to build a global security regime, and, therefore, we collaborated with representatives from 147 other countries at the International Maritime Organization to build this new and substantial security regime that applies to vessels and port facilities around the world.

These international requirements mirror our domestic standards set forth in NTSA. So there is very much an equal push domestically and internationally on the same security front. This provides a powerful way to leverage our efforts, not only across the country but across the world.

We do have implementation challenges, and we have met those; and the 1 July implementation date has come and gone very smoothly, despite these many challenges.

Since 1 July, we have continued our enforcement efforts and have conducted over 2,500 foreign vessel security exams under our port State control program and about 1,000 other facility and domestic vessel security inspections to ensure compliance with that new regime.

Also, Coast Guardmen and women are working every single day on the waterfront to deter and prevent terrorist acts, and are preparing to respond should something happen in a port.

As required by the NTSA, the Coast Guard has also established an international port security program that works in concert with Customs and Border Protection, with Immigration and Customs Enforcement, with the Transportation Security Agency, and the Maritime Administration and some other Federal agencies to identify foreign ports that pose a potential security risk to international maritime transportation because of their lapse in security as the vessels or cargo comes to the United States.

BTS, Border and Transportation Security, is also leading our effort, along with TSA, CBP and the Coast Guard, to develop a cargo security strategic plan known as the secure systems of transportation, which is an NTSA requirement by the way. It takes a systems approach related to risk to cargo transportation by enhancing existing security regimes through minimal regulatory standards and using performance-based options to improve shipments. The secure systems of transportation effort will ensure security requirements that international and domestic cargo shipments are aligned for all modes of transportation.

Further, enhancing our maritime security implementation efforts has been our gaining membership in the national intelligence community. Intelligence community membership is absolutely necessary, in our opinion, because it gives the Coast Guard expanded authority to collect, retain and disseminate foreign intelligence to meet the various homeland security objectives, one of which is port security. This also gives us enhanced access to information and enhanced intelligence and maritime domain awareness through our partnerships and access to information from the many intelligence community members.

To continue facilitating our intelligence capabilities and information-sharing capabilities, the Coast Guard will hold a public meeting on September 1 here in D.C. To discuss information-sharing mechanisms that will allow the Federal Government, particularly in the maritime security arena, to more effectively share threat in-

formation with maritime industry stakeholders, specifically the private sector.

Regarding our operational presence, our collective efforts to increase our operational presence in ports and coastal zones continue to build upon a layer of security posture established by the Maritime Security Strategy, which is a document we published in December of 2002.

Since 9/11, the Coast Guard has grown by over 4,000 people. We have increased our cutter operating hours by almost 100,000 and our small boat operating hours by an estimated 200,000 hours just in support of port security missions. We will also, by the end of this calendar year, have deployed and commissioned 13 maritime safety and security teams. Those are surge teams, as you well know, that provide us a great deal of asset capability should something happen, and also for daily operations, to surge to make the needs related to the risks in the various ports around the country.

We also are working with DOD as closely as we ever have, and we will receive and commission five new coastal patrol boats from the Navy before the end of the year. We will also add 17 new 87-foot coastal patrol boats and nearly 300 new small boats by the end of this year. So operational presence certainly depends on the acquisition and development of those resources, and we are making great progress on that front.

Regarding response and recovery, the Coast Guard has been working with Customs and Border Protection, TSA, the Maritime Administration and other DOT mobile administrators on establishing national standards, plans and policies for maritime transportation security, including response and recovery.

Just three short examples that are key, but significant: Since 9/11 we have adopted now the National Incident Management System, the NIMS system, which essentially is a 9/11 Commission recommendation, to adopt ICS; NIMS is essentially the incident command system. That will be the Nation's first standardized model now for incident management that will create a unified structure to involve Federal, State and local responders to respond to any kind of incident, including a terrorist incident.

The national response plan, which is the capstone document that talks about response and recovery, is in its final stages of review, and we look forward to getting that finalized.

I would also offer that area maritime security committees, 43 of them, have been stood up around the country; and one of their charters, in addition to a strong focus on prevention, is also to talk about jurisdictional responses in their particular area of responsibility, identify agencies that have response capabilities and, in general, make sure that there is good coordination between local, State and Federal agencies to any incident that may occur.

We have recently, in the last couple of months, had the opportunity as a department to exercise our planning and coordination at three national security special events: the G8 summit; the state funeral for President Reagan; and the Democratic National Convention up in Boston. During all these events, the Department not only coordinated its own agency efforts, but it also worked with other Federal, State and local agencies as well as our private sector maritime community partners. This allowed us to address the secu-

rity risks presented while ensuring a free flow of commerce and minimizing the effects on recreational boaters and the commercial fishing community, which is important. Our efforts again will be surged for the Republican National Convention in New York.

In conclusion, we have come a long way since the morning of 9/11, but we still have a great deal to do. It will require continued capability growth and development of strong partnerships among the Coast Guard, Transportation Security Administration, Customs, ICE, MARAD and State and local agencies and our maritime community private stakeholders.

No single stakeholder, whether it be government, industry, labor, private sector, anyone, can do this alone. We must continue to work together to improve security.

The recent 9/11 Commission report and the focus it places on the national intelligence infrastructure in maritime security provides further opportunities for improvement. While we must remain vigilant and dedicated to the effort, the Coast Guard's Maritime Homeland Security Strategy has, we believe, produced significant results since 9/11.

We have a rich tradition of answering the Nation's calls. We are proud of our accomplishments over the past 3 years, and we appreciate the dialogue, with this committee in particular, to continue those improvements.

Thank you very much for the opportunity to come today and talk to you, and we will be happy to answer any questions you may have.

Mr. LOBIONDO. OK. Thank you, Admiral.

Mr. Gilchrest, why don't you start off?

Mr. GILCHREST. Thank you, Mr. Chairman.

Admiral, welcome to the subcommittee hearing.

The first panel made a recommendation that Congress reform itself so we do not have 45, 32, however many, subcommittees dealing with this issue and fragment the kind of information that needs to be consolidated so that we can keep the Coast Guard and the bureaucracy dynamic.

I also want to welcome James Sloan, a graduate of Cranford High School, 1964, a neighboring high school. We challenged each other in a whole range of sports. I am glad to see after 40 years we have finally gotten together again.

Mr. LOBIONDO. You have got to hold on. You have got to give him a chance to respond, Wayne. You threw something out there.

Mr. SLOAN. I am not foolish enough to say that Congressman Gilchrest won everything.

Mr. GILCHREST. It was a great rival, though, Cranford and Rahway, part of the Garden State, Mr. Chairman.

Admiral, I have three questions, two parts to the first one. Was the Coast Guard able to communicate during the tragedy of 9/11 with the first responders, with State and local officers at the scene, on 9/11?

The second part to that question is, last Friday an off-duty policeman in Maryland found a member of Hamas videotaping the Chesapeake Bay Bridge. God forbid anything ever happened where a suicide bomber actually detonated a pick-up on the Chesapeake Bay Bridge.

With that kind of catastrophe, would the Coast Guard be able, in the Chesapeake Bay, to communicate with the Department of Natural Resources, police, with the other various first responders in the region of, let us say, Queen Anne's County and Anne Arundel County.

Admiral HERETH. Sir, we believe that the Coast Guard could have and did communicate with first responders in New York on 9/11. That communication capability was probably one of the better systems in the country.

We also believe, since 9/11 there's been a tremendous focus on communications development and capability, and much has been done in that regard to ensure that all first responders can, in fact, communicate.

In particular, that is one of the reasons and one of the strong things that had been the focus of discussion in the area of maritime security committees as they have stood up around the country. Communication obviously underlies a good, effective and efficient response, and so we are very concerned that is on the table on each of the committees' agendas and that they talk and engage on that front in a robust fashion.

There also have been a lot of equipment purchases since 9/11 to continue to foster that development.

So you are right on target. That is a very crucial need. It has to be handled properly, but it is being aggressively addressed, sir.

Mr. GILCHREST. Thank you very much.

The second question, the container security initiative, you spoke about your efforts with the international community, working with the International Maritime Organization and so on. Have you seen any problems with the container security initiative in foreign ports?

It is my understanding that an agent inspects the containers as they are being loaded. Is that a correct assumption? And are any of those agents that inspect the containers U.S. Agents, and are there still ports out there where there is not an agent that inspects the containers as they are being loaded?

Admiral HERETH. Yes, sir, that happens all over the world. There are a limited number of agents deployed around the world. They generally do not inspect the containers as they are being loaded or stuffed. Generally, the practice is to screen containers and look for anomalies and then de-van the boxes, look at the boxes as necessary. Those agents are, in effect, CBP agents that are deployed around the world.

Mr. GILCHREST. What is that?

Admiral HERETH. Customs and Border Protection agents, inspectors.

Mr. GILCHREST. So they are American. Do we have counterparts? Are there agents from England or France or Japan or so on?

Admiral HERETH. No, sir, not that I am aware of.

Mr. GILCHREST. This is a unique U.S. Initiative?

Admiral HERETH. I believe it is, sir.

Mr. GILCHREST. They go to ports where they know the ship that is being loaded is coming to the United States?

Admiral HERETH. Yes, sir, and try to focus on ports where the largest amount of cargo is flowing to the United States.

CBP, of course, manages that program principally and the intention is to pretty much double the program from 20 ports around about now to 40 ports by the end of the year.

Mr. GILCHREST. Just a quick follow-up, Mr. Chairman.

The idea of a container security initiative, with the U.S. Agent in various ports around the world inspecting to the degree that it is humanly possible the kind of goods loaded into that container, it is my understanding that there are in the IMO new security code and security provisions.

Is there anything in that proposal that deals with people actually, to some extent the way we are doing it now—where our security agents are monitoring the containers that are being loaded? Is there anything in the new IMO initiative that does that?

Admiral HERETH. Not that specifically requires inspections once a container is stuffed. But there are all sorts of recommendations and guidelines to push up the supply chain and know before a container arrives in your terminal where it is coming from, who it is coming from and establish a relationship with that shipper. So the term "trusted shipper" is prevalent. That seems to be a focus.

Mr. GILCHREST. So the private sector would have a great deal of motivation to inspect each container as well, I would hope.

Admiral HERETH. In effect, there is quite a bit of motivation to sign up for a standard set of protocols known as CT-PAT, and I am sure you may have been briefed on that program, essentially a set of protocols for shipping containers around the world. Most of the shippers in the world in the liner trade have signed on to those contracts or agreements with Customs, again, establishing requirements or standards that are followed by companies as they move cargo to the United States.

Mr. GILCHREST. I see. Thank you, Admiral.

Thank you, Mr. Chairman.

Mr. LOBIONDO. Thank you, Mr. Gilchrest.

Mr. Sloan or Admiral, it's only been since, I guess, December of 2001 that the Coast Guard has had a full seat at the intelligence table, so to speak. A lot of the focus of the Commission was on intelligence and how it was handled, and there is a lot of emphasis that suggests, and I believe, that our ability to deflect future terrorist incidents rests on our ability to collect intelligence.

Are you satisfied with the Coast Guard's participation at this point, Mr. Sloan.

Mr. SLOAN. Yes, sir, I am. You are absolutely correct. We became the 14th member of the intelligence community in late 2001, and as you know, there are now 15 members with the information analysis arm of the DHS as also a member of the intelligence community.

Being a member of the intelligence community, I think, has enhanced the Coast Guard's ability to do many of the things that Admiral Hereth referred to in his opening statement. Not only do we get the expanded authority to collect and retain and disseminate information, but it also helps us in our MDA relationship, most particularly with the Navy.

As you may know, over in Suitland, Maryland, we are collocated with the Office of Naval Intelligence and doing many of the things that have been discussed here today relative to reaching out as far

as we can beyond our shores to pay attention to what is approaching the shore; and the information that we receive, the funding that we can receive, the training that we receive, leveraging all that within the Coast Guard, I think, has made Coast Guard's membership in the intelligence community a very valuable resource, for the Coast Guard and for the Nation.

Mr. LOBIONDO. We may need to schedule a classified session for some of this, but we understand that the Coast Guard, with a 96-hour notification, will review crew manifests, cargo manifests and determine through intelligence sources where there is a vessel of interest; and we are interested in making sure that you have all the tools necessary to push our borders out as far as possible. I don't know if there are any comments you could make about how that is working or how it could work any better than it is working now.

Mr. SLOAN. You are right. There would be some details of that program, at least what we do with the manifests, that would be suited for perhaps a closed hearing. But I think it is safe to say publicly that it does help us push the borders out significantly 96 hours. A crew manifest would come in, and we are able to vet that through a lot of fused information which could be information that we have received and used appropriately in accordance with the national intelligence requirements, but also fuse it with domestic law enforcement intelligence, whether it is coming from the Customs Service or the FBI and others, and do a pretty thorough vetting of that manifest, the cargo, before it arrives in the United States. And that, too, has been a success.

Mr. LOBIONDO. So there isn't anything additional you would ask for in the way of tools or authority at this point to further enhance your capabilities?

Mr. SLOAN. Well, I think it is safe to say without getting—and having been a former regulator, I will be careful that I do not go down the line of notice of public rulemaking. But I do think that because that applies to vessels that are 300 gross tons and above, I think there would be some effort to try to lower that threshold. I think that would be something that we would be discussing in the future, and I think Admiral Hereth from the maritime safety could talk about that to a greater extent.

Admiral HERETH. Sure. We certainly do, and as was mentioned by Mr. DeFazio, concern about small vessels is certainly there and relevant.

The reporting requirements now apply to vessels greater than 300 gross tons. We intend to discuss pushing that down to a much lower threshold, and we are evaluating that right now, talking to our partner agencies about how quickly and how much we can lower that threshold.

But our intention is to gain—again, reflecting back on awareness—gain total awareness of what is going on in the maritime domain; and that is going to require some substantive changes, and we are looking at those right now.

Let me just add one thing to what Jim said. The intelligence in the Coast Guard is linked very much to our operations on a day-to-day basis. There is a daily targeting message that comes directly out of our intelligence coordination center in Suitland. It goes

through our intel fusion centers, which now exist on each coast, and then it is directly fed to the operational units, and they use that in targeting their boardings and all the operational activity that occurs in ports. So it is a very tightly wired operation connecting intel and field operations in the Coast Guard, and we think that is exactly where it should be.

So we are constantly searching for ways in which to gain better intelligence and have that flow through operational units and make it actionable so we can influence and make our operations tailored to the concerns and the threat that is posed.

Mr. LOBIONDO. When might we expect to hear a timeline from you about pushing down the threshold?

Admiral HERETH. I would think in the next month or two, sir, we would have that completed, and then we will begin an aggressive push to put that into place.

Mr. LOBIONDO. On cargo container security, in your view, is there any technology that we can expect that would be deployed on a pilot program at any time soon that would help in this particular area? I know that a lot of ideas have been floated through, but we are not involved with any pilot projects with anything new yet, are we?

Admiral HERETH. Yes, sir. I think there is about \$58 million focused on the Operation Safe Commerce pilot programs at three low ports, and we would expect that the outcome of that testing would, in fact, drive the new standards for containers relevant to the construction of the container, any container improvements, any tracking technologies that might be appropriate, but also some continuing supply chain improvements.

Mr. LOBIONDO. What about technologies that we have heard are in R&D stages that would be able to quickly and efficiently, in essence, take an MRI of a container?

Admiral HERETH. We are trying to work with the private sector to implement technology improvements that not only foster improvements in efficiency but also in security as quickly as possible.

We just signed a request for implementation of the use of RFID equipment on containers on the West Coast with 13 companies about a week ago. Rate of frequency identifying equipment will be used on containers now as they approach the gates that will then identify drivers before the container gets there, but also the purpose, the business purpose for the container arriving at that facility, allowing the gate checker to be much more efficient in the process.

And so we are going to continue to look for ways in which we can foster the use of technology, at the same time bolstering security. And so that is, I think, one good example of how technology and security can go hand in hand. We will continue to look for options to do things like that in the future.

Mr. LOBIONDO. Lastly, the Maritime Transportation Security Act directs the Secretary to develop a national maritime transportation security plan for deterring and responding to transportation security incidents. We heard Secretary Lehman talk about that needing to be a real top priority.

What is the status of the development of this plan, can you tell us?

Admiral HERETH. Yes, sir. We have a dozen or so folks focused on pushing that through the system in a broad, interagency way. In fact, there is 12 different agencies that we are working with, both inside and outside of DHS, to draft that National Maritime Security Plan. The timeline for that is completion by the end of this calendar year. We are on that timeline.

It is a big challenge because of the interagency involvement and because some of the national policies are difficult to come to grips with, but while that is underway, there has been quite a bit of other planning put in place.

We have done some strategic planning. A couple of years ago, we had the area maritime security committee doing regional plans. As you know, we just completed the review and approval of some 13,000 vessel and facility security plans for terminals and vessels all around the country.

So lots of planning has been done, including strategic planning; and this National Maritime Security Plan will be the capstone document in a family of plans that begins with the local plans for regulated infrastructure, which is then covered by the area plan which is a regional look at security, and then this national plan will give us a capstone national policy view of national security issues and—

Mr. LOBIONDO. On the maritime side?

Admiral HERETH. On the maritime side only, yes, sir.

And the way we are thinking about that is, TSA owns the transportation security plan, all the modes. We are plugging in the maritime mode as one of the modal feeds to that transportation security plan. It is a connected effort, and of course, the transportation security plan is one of the 13 sectors that feeds into the national infrastructure protection plan.

Mr. LOBIONDO. So that will be folded into that overall plan?

Admiral HERETH. Yes, sir. We tried to make sure that that was a very connected and logical extension of our planning efforts.

Mr. LOBIONDO. OK. Admiral Hereth, Mr. Sloan, thank you very much. We will go into a very brief recess while we go to—excuse me.

Mr. GILCHREST. I am sorry, Mr. Chairman, just if I could, two very brief questions.

One is, homeland security issues, orange alerts, yellow alerts, red alerts, things like that. What is your counterpart for the maritime community in and near a port for a certain—do you have levels of alerts that you issue?

Admiral HERETH. Yes, sir.

Mr. GILCHREST. The other question is, we have talked a lot about containers. Are there any provisions dealing with bulk cargo, whether it is coal or sugar or things like that?

Admiral HERETH. Yes, sir. Bulk cargo, break bulk cargo container vessels, terminals, everybody in the maritime mode now comes under the NTSA requirements that specify that they must define three levels of security. And we relate those three levels of security; those are pro forma standards of protective measures.

So when the country is at yellow, we are at protected level one, MARSEC level one, maritime security level one. When the country goes to orange, which signifies an increased threat, we then ratchet

up the protective measures in a defined way. And it is defined really according to the owner-operator meeting the regulatory standards which are performance-based in a fairly flexible way. So it allows people to develop standards that are customized to their particular operation or the nature of their business.

So we have tried to make it as cost-effective as possible, but yet have a defined standard that people go to as the threat bumps up.

Mr. GILCHREST. Your security levels are basically the same as what are issued by homeland security?

Admiral HERETH. Yes, sir. They match yellow, orange and red for one, two and three.

Mr. GILCHREST. Thank you very much.

Mr. Sloan, Admiral, thank you.

Mr. LOBIONDO. OK. We thank you very much.

And now we will take a brief recess as we prepare for Dr. Flynn.
[Recess.]

Mr. LOBIONDO. Dr. Flynn—thank you—Council on Foreign Relations. We appreciate very much your being here today, and please proceed.

STATEMENT OF STEPHEN E. FLYNN, Ph.D., COMMANDER, U.S. COAST GUARD (RET.)

Mr. FLYNN. Thank you very much, Mr. Chairman and Mr. Gilchrest. It is an honor to be with you today. I think our last trip together the Congressman was in Philadelphia. I believe we were on a panel together.

Mr. LOBIONDO. Yes, it was.

Mr. FLYNN. I am thrilled to be back here today in front of you to talk about this very, very important issue.

What I would like to try to do is address what I believe are the ongoing shortcomings of our maritime transportation security and speak directly to what the Commission's findings are, but to expand on them. And I hope to be able to elaborate in your questions afterwards here, maybe on some of the specific measures, some of which are already discussed before, on things like container security initiative, how well is that going—I will speak to that a bit in general terms in my testimony here—but also some of these other technologies that might be used and what the applications are. These are issues that I have immersed myself in for quite some time, so I look forward to the chance to chat with you about some of these.

I think the Nation owes an enormous debt of gratitude to the Commissioners and the dedicated staff of the 9/11 Commission. The report should certainly serve as an anecdote for anyone in Washington who thinks that we can afford to take a business-as-usual approach to confronting the threat of catastrophic terrorism. From my perspective, the report makes three central points that are critical for understanding our post-9/11 world:

First, that the attacks on New York and Washington were a meticulously planned and executed campaign by a tenacious enemy intent on exploiting America's most glaring vulnerability, which is our largely unprotected home front.

Second, prior to 9/11 the U.S. Government was neither focused nor effectively organized to confront this threat and that neither

Democrats nor Republican are blameless for that unhappy state of affairs,

Third, that despite the horror of that day and the passing of nearly 3 years, there is so much work to be done towards making the critical infrastructure that underpins U.S. Power less of a soft target.

I would be less than candid if I did not acknowledge that the hearing today sparks within me a bit of a sense of *deja vu*. Prior to 9/11, I had the privilege to work with the former Senators Gary Hart and Warren Rudman on the U.S. Commission on National Security for the 21st Century. As members of this committee undoubtedly know, that commission would spend 3 years of study, concluding in their final report which was published in January 2001 that the greatest national security challenge that would confront the United States in the 21st century would be a catastrophic terrorist attack on U.S. Soil and that the U.S. Government was simply not organized to deal with that new reality.

In our case, we had a blue ribbon commission, bipartisan, chartered by Congress, much like the 9/11 Commission. I hope that is where the similarities end, because in our case, of course, there was a collective yawn in Washington when the report came out.

In this case, this hearing certainly would suggest, as other hearings that have been held normally in the time of recess, that Congress is quite interested in stepping up to this problem and responding to many of the, I think, excellent recommendations the Commission has made. I think it is vital for the Nation that we act on these with dispatch.

I am confident the 9/11 Commission would readily acknowledge, from some of my interaction certainly with that staff, that had they had more time, one of the areas they would have spent more of it on would have been fleshing out some of the recommendations for improving transportation security specifically and critical infrastructure protection more generally. This was not the strongest part of the report, but still they performed a very valuable service, I think, by documenting the extent to which, during the decade prior to 9/11, counterterrorism measures as a part of border security were just simply not a national priority. They were largely going through motions.

Secondly, that there remains a serious lack of balance: We have talked about the 90 percent resources going into aviation, really passenger aviation, and not much left over for anything else.

That the risk of harm is great, or greater in the maritime surface transportation modes than the aviation modes, something I would certainly subscribe to.

And finally, that TSA still has not developed the big picture, a strategic plan by which anybody can assess where we should be going and at what pace and where we should allocate priorities.

Based on my assessment of the state of transportation security both before and since 9/11, I agree with all these findings. I would add to that list my concern that many of the helpful measures that are being pursued by the administration in the area of maritime transportation security quite simply have not been adequately resourced or staffed to meet the threat to the sector. They are baby steps.

Specifically, in my testimony today, I will point to some critical shortcomings, I think, in these major initiatives that deserve the immediate attention, now, of this committee, the Congress as a whole and the White House.

I begin by talking about the International Ship and Port Facility Code, the ISPS code, that went into effect on July 1. This should not be a new age. We were supposed to have 22,539 vessels that ply the seas and 7,974 port facilities that serve as the on-ramps and off-ramps for the transportation system abiding by new security measures that were adopted back in December 2001. Congress, through the NTSA, gave this the force of law here in the United States, but the new mandate just simply hasn't come with any resources, adequate resources, to meet the threat.

Since 9/11, Washington has provided only \$516 million toward the \$5.6 billion that the Coast Guard estimates U.S. Ports need to meet to make ports minimally secure. And I would suggest that is "minimally secure"; that is not any high bar. That is basic gates, cameras and basic access control and so forth. So we have got a big shortfall.

This year, in fact, is the very first budget that the administration has asked for any new money for seaports, and we have got just \$50 million in the budget towards this. Given that ports are run by State and local authorities, most of which are in serious budget constraints, I don't see any way, particularly given the other competitive needs on those ports for upgrading infrastructure, that they can make up this difference anytime soon. So we remain in a situation where the mandate on seaports is grossly underfunded.

Equally importantly, I suggest Congress has failed to authorize new funding to pay for staffing and training for Coast Guard inspectors to verify that everybody is actually following these new rules. That is something I understand that fell out of the authorization process here quite recently for next year's budget. The result is, we have a Maritime Transportation Security Act with a mandate that says the Department of Homeland Security will certify annually that ports and port facilities and ships are complying with the new standards, but we forgot to give any money for this actually to be accomplished.

The Coast Guard has largely responded to this by a quick fix. What they essentially have tried to do is put together a quick team or a team of reserve, primarily junior officers, who have very limited experience in marine inspections, little to no background in security, and sent them off on basically fly-by inspections in many of our ports around the world. I am very deeply concerned that this, in fact, will send just the wrong message, that the international maritime community will size up this very quick effort to try to check in on how they are doing as essentially an indication that the United States Government is not really serious about maritime security.

I have already heard, from talking to some overseas port players, that the result may, in fact, be highly counterproductive. It will be very difficult for a security officer to go to a port authority and say, we need to make investments in security, that he is able to point to; or, we had the Coast Guard here, and they said we are good to go. So we could actually have a slowdown in investments instead

of the opposite. This is a direct result of not making sufficient investment in the oversight of a new requirement and regime.

The Coast Guard is obviously struggling not only with this new mandate, but it also, of course, is operating with a fleet of cutters and aircraft that has been pushed to the breaking part and beyond. We have heard from Admiral Hereth about the number of new hours assigned to the boats and cutters. This is a fleet that is not aging gracefully. It is decades old.

This subcommittee needs no reminder that the Coast Guard is only slightly larger than the New York Police Department, and yet it bears the burden of being America's first line of defense along 95,000 miles of shoreline and covering over 3 million square miles of water. It is patrolling our Nation's coastal waters in vessels and airplanes that are operating long beyond their expected service life. The result of this is that the already dangerous job of performing these missions at sea is being compounded by frequent engineering casualties that puts the lives of Coast Guardsmen and women at jeopardy.

Just a couple of weeks ago, when we had Hurricane Charley rolling through the southeast, the Coast Guard cutter Gallatin, the large, high-endurance cutter, a 378-foot cutter was ordered to sea to make it safe. They barely got out of port, and then its main engine promptly crashed in an effort to get out. This is not uncommon. High-endurance cutters, which were primarily built in the 1960's, are having main engine casualties virtually every patrol, some of them leading to fires, which is obviously not something you want when you are at sea.

It is inexplicable to me that despite the age of the fleet, despite the new demands of homeland security, the enormous task before us, we still haven't gone back and assessed the pre-9/11 schedule for how we are going to recapitalize this fleet. We are still on a 20-plus-year schedule, and I don't see any possibility that this fleet will survive the transition for new frames to be out there; and this is going to create a particularly delicate time in the 3-to-7-year frame-out where we are going to have fewer and fewer ships and aircraft able to deploy, new ones on the drawing boards not being deployed and America still under threat.

Now, another Coast Guard initiative that I would suggest really needs another look at and investment in resources is the automated identification system. Most Americans that I meet are simply flummoxed by the fact that while FAA can track airplanes, it turns out we can't track ships—kind of big things. No, we don't know until they get here who they are, where they have been and so forth. We get advance warning if they give it to us, but we don't find out until they get closer.

AIS is a first step, but I would argue in the wrong direction. Its focus is using, of course, radio frequency technology that only goes out to the horizon about 20, 30 miles. In a world when we are putting GPS devices in cell phones, I am not quite sure why we are not raising the bar for tracking ocean-carrying ships from the regional ports to here. The technology is available.

Every trans-Pacific ship and Atlantic carrier uses INMARSAT. It is a communications system that communicates with satellite. You can't do that without the satellite knowing precisely where you are.

The tools are out there, and we can make these investments and we must.

The problem with AIS is there is simply not enough response time, if a ship comes barreling in you suddenly identify as a threat, that you will have momentum to review them. Twenty miles, you can do most ships in just over an hour. You can't mobilize a response to that with limited time.

So I worry that the emphasis on AIS is steering us away from basically simply insisting that if you are going to travel the U.S. Waters, across the Atlantic, Pacific Oceans, you are going to 'fess up where you are along the way.

Next, I would like to talk about the Customs and Border Protection directorate which shares with the Coast Guard the burden of securing the maritime transportation system. CBP is the lead agency for addressing the risk that cargo containers might be used as a poor man's missile. It has undertaken a number of initiatives since 9/11, some of which have already been talked about today, but I would again—because of the paucity of resources that have been dedicated to this effort, I would suggest that it leaves America dangerously vulnerable to another attack of catastrophic terrorism.

The container security initiative is the centerpiece of the administration's effort in this area. It is a well-conceived program, involving placing U.S. Customs inspectors overseas at the port of loading to target containers for inspection before they are loaded on a ship destined for the U.S.

There is, in fact, reciprocity for the program. The only foreign inspectors that I am aware of who are here in the United States are Canadians. They are in Seattle and they are also in Port Elizabeth. So as they sign on, it is possible for a foreign customs officer to examine outbound cargo in cooperation with the U.S. Government, which I think has been an important part of making it attractive to other nations, given the sovereignty issues involved.

To date, over 24 ports, including all the largest seaports in the world, have signed agreements to participate in the CSI. It is miraculous really how quickly these other agents have got on board. That is the good news.

The not-so-good news is that CBP is staffing the CSI program by sending teams of just four to eight inspectors on temporary-duty assignments of 3 to 4 months duration because the administration hasn't sorted its way through giving them overseas billets that allow these folks to stay more than 12 months.

In Hong Kong, the world's biggest port, there are just eight inspectors on temporary duty. It takes them a while to get acclimated. They have no formal training. They have no language training. We wouldn't think of sending attaches overseas basically by just putting you on a plane and landing, given this kind of job, but that is, in fact, how we are approaching this problem.

Next, the limits of CSI would suggest simply not enough people, not enough time to get acclimated to the area—so small numbers. They are targeting a tiny percentage. When I am talking "tiny," I am talking several a week, when we are talking ports like Singapore and Hong Kong that are doing a million a month. So it is a step in the right direction, but again a baby step.

Next, I want to talk about the Customs-Trade Partnership Against Terrorism, which is a companion piece to CSI. Under C-TPAT, CBP has reached out to companies and carriers involved in importing goods into the United States. It has asked them to assess the vulnerability of their supply chain and to put in place measures to address any weaknesses they discover. Companies that join C-TPAT enhance the odds that the Customs and Border Protection will view them as low-risk shippers, which translates into their conveyance or shipments not being subjected to routine examinations.

Like CSI, the underlying logic of this program is laudable. Unfortunately, again we run into staffing and resources issues. CBP has received over 5,000 applications to join in this program. It doesn't have the staffing to get through them. The last count that I was aware of, a little over a month ago, they went up through the first thousand. That is just the beginning step.

The problem is, they have no means to go back and certify whether anybody is living up to the application. It is essentially a trust-but-don't-verify program, but please be trustworthy. That is essentially what we have got going. What this means is that the maritime transportation system remains an extremely soft target for America's enemies to exploit.

We have heard from the 9/11 Commission about the extent to which groups like al Qaeda are willing to stake places out, spend the time to plan, and then this sector is one which is recognized within the intelligence community as one which they have in their sights.

We have learned also from the orange alert here on August 11 the extent to which they will spend the time and energy staking out critical infrastructure, and yet we have a system, because it is trust-but-don't-verify, that I believe creates a real opportunity for terrorists to exploit and to target, that would have enormous consequences for our economy if we don't get our act together quickly.

My sense of worst-case scenario today is, in fact, this one: That we have a terrorist incident that will involve a C-TPAT participant, loaded in a container that arrives in a loading port that is a member of the Container Security Initiative protocol, is on a ship that is certified as ISPS-compliant, steams the waters, lands in the United States, put on the rail or a truck, sent into the interior of the United States and the container goes off with a weapon of mass destruction.

When that happens, what we will have is a discrediting of the entire regime. Every container becomes viewed as high risk. In that context, particularly if it is a multiple attack, which al Qaeda is often prone to do, as we have seen, we would have shutdowns to sort it out and then trying to develop, on the fly, a credible mechanism for validating low-risk is low-risk.

If we have a 2-week shutdown of U.S. Ports, we will collapse the global trade system. That is what we are talking about here, and the notion that we have not been able to find the resources or the energy to focus attention 3 years after 9/11 to deal with this problem is something that I am still flabbergasted about.

This is my ninth time testifying on the Hill since 9/11. I am getting to be like a broken record on this score. I am grateful for the

opportunity to repeat the record, but I very much fear if the investments are not made, and the energy and the resources to get a handle on this problem, I am just giving fodder to the next commission, the next blue ribbon, bipartisan commission to sit down and say, why is it that we left Americans grossly unprepared to deal with the threat that we all were aware was coming?

Thank you very much, Mr. Chairman, Mr. Gilchrest. I look forward to your questions.

Mr. LOBIONDO. How many of those nine times were before the Appropriations Committee?

Mr. FLYNN. Only once.

Mr. LOBIONDO. We have got to get you back there, especially on deep water.

Mr. Gilchrest, we will let you start off again.

Mr. GILCHREST. Thank you, Mr. Chairman. Well, we have a lot to talk about with everything that you have mentioned to us. And this is the first time that I have sat in a hearing where you have testified. I am sure this subcommittee, along with Mr. LoBiondo, will begin to rattle some cages to let some of this dust get shaken away and the dollars poured down and the priorities set in order to meet our responsibility for security of the U.S. Ports in the United States.

You mentioned the Container Security Initiative, the automated identification system and a number of other things here. We heard the Admiral on the previous panel discuss some of those initiatives and his work, especially the Container Security Initiative and the agents that travel to foreign ports, and the inadequacy of their numbers; and apparently you are telling us the inadequacy in their training and some apparent laxity in seeing that as one of many priorities that needs to be put into place.

And I guess we can go through your testimony, but to put it in the simplest form, is there a list of recommendations that you have attached, with the dollar amounts, that you could give to us to sort of speed up this process?

Mr. FLYNN. I do have a list of recommendations and just actually finished a book that came out and spent a lot of time on this. Dollar signs is a little tricky, but I can give you a feel for what those dollar signs are.

The central thrust is that the approach that has been taken to really view this as a global network issue is precisely the right one to be taken. One of my core concerns is that we have, unfortunately—rather than obliterating a tiny distinction between our borders and domestic security and international security, which I think 9/11 should have warranted, we have actually reinforced the line by saying national security is dealing with threats over there and homeland security is dealing with these issues here; and the maritime is the perfect illustration of where that doesn't work very well.

The ports are simply on-ramps and off-ramps to a global transportation system upon which our economy depends, and if it is strictly a homeland security issue, how do you get the rest of the system to behave? But if the foreign policy and defense/national security community don't see this as a priority because they are focused on traditional national security issues, then you don't get the

resources, you don't get the energy being applied through diplomacy and other means to move this out with some speed.

The central approach that I am arguing on container security specifically is, we need layers, and the layers begin with a birth certificate, somebody you can point to, to say who loaded that container, to say it is legitimate and authorized. That should be a process that we can point to.

Mr. GILCHREST. On that point, how would we specifically do that? With all the issues that the IMO deals with, whether it is trying to make a shipper credible because he has to meet certain criteria in order to be a part of the international insurance system so that he can go on the high seas, transparency, who owns that ship and so on, how do you actually get an individual—or is it necessary to get some human being, some U.S. Agent, some agent that we trust on the ground to watch that container being loaded? Is that part of the necessity that we need to undertake?

Mr. FLYNN. I believe that we do need some trusted party. I don't think it is U.S. Agents, the numbers, we have got about 18 million containers out there. So it really is working with the private sector saying, come up with a system, either in-house that we can vet, or you rely on third-party folks who come in and make sure you are behaving by these rules.

Mr. GILCHREST. How does the U.S. undertake something like that? Do we work through the IMO to deal with that? Do we establish some other entity so that we can work with the private sector, our foreign neighbors at their ports? How do we set up a structure to do that?

Mr. FLYNN. The NTSA 2002 actually provides the mechanism, which is one that I have been working through. The good news on this problem is it turns out eight out of every ten containers that come into the United States, of the 7 million that came in last year, pass through four terminal operators, all of which are private-sector players.

There is Hutchison Port Holdings, which moved 41 million TUs last year. Next, PSA, Port of Singapore, International, which moved 19.5 million. Then you have PNO Ports, a British-based—they moved about 16; and then you have AP Moller Ports, a Dane company, that moved 13.5 million. HPH is run by a Brit. So two Brits, a Singaporean and a Dane.

All these ports, you cannot get to the United States, largely, unless you go across the big oceans relying on a megaport and a good-sized ship, except for some of the Caribbean operations. These folks basically are in a position to say, any box that comes through our terminal will have a birth certificate; it will be a small box that is trackable, whose integrity can be measured, we know where it has been and then we will scan it and get the image of what is in there.

Mr. GILCHREST. Have they said that?

Mr. FLYNN. I am working with one of them, which is HPH, in Hong Kong. I am going there next week, in fact. They have agreed to engage in a pilot where they are going to, in the world's busiest terminal, HIT terminal in Hong Kong, where they are going to scan every truck that comes through both an image and a radiation signature, combining with OCR, optical character recognition, technology so you have a truck and container through it and show that

you can do this without disrupting the throughput. The cost of this would run about \$15 per shipment to run through this equipment.

When you talk about the scale, the cost of using a smart box technology, GPS tracking, a radiological sniffing device, as well as something that could tell somebody broke in—a light or so forth—the total cost of that black box is going to be about \$300 to \$500 apiece, but amortized over 5 years, five times per year, that comes in about \$20 a shipment.

A birth certificate process is probably on the order of \$10 to \$20. Some very scary places, obviously more expensive—depends how frequently you're using it.

We are talking about \$50 per shipment basically to go from what I call a dumb box, we know nothing about that, that presents a very high risk, to one that we could have some real confidence—that is, in fact, a legitimate good, that hasn't been diverted and hasn't been exploited. It wouldn't be a failsafe system, but it would be a long ways toward where we need to be.

Putting that into context, the average shipment today for a trans-Pacific voyage is just over \$3,000 for up to 32 tons of material, which I think makes a postage stamp look a little bit overpriced, but that put in context, when the economy was at a slow point in spring 2002, those freight rates went down to just about \$2,100. I haven't heard Wal-Mart in Chapter 11 as a result of paying \$1,100 more than actual freight rates. Marine freight rates are very volatile.

But now here is the benefit, and that is what NTSA allows for. The terminal operators think it would create the incentive for people to do what this will do; we will call it a "green lane," which is basically the EZ-pass version of, essentially, throughput.

Really, the agreement that I have talked with three of the operators about doing is three things:

One is, if we pull you out of the queue to get inspected as a random inspection, we will do you right away, put—we will put you at the head of the line.

Secondly, if we go to orange alert, the heightened alert, we are not going to mess with you because you have already done this prophylactic stuff up front. You are using a thing we can measure. We are not going to slow you down.

Thirdly, if we have to shut down because we had an event, we are trying to sort it out, we will start with you guys first.

And their conviction is going to them because the certainty of the supply chain is really where the money is to be made, that paying what may be a \$50-per-box surcharge works here. And then the willingness to invest in the technology to actually do the scanning is not U.S. dollars; it is basically the system in place to incentivize this.

I just saw a mock-up of the technology in San Diego last week when I was out there. They are going to be deploying this in Hong Kong in September. We will see how it works; I will be more of a preacher when I see it really works. But the reality is, the technology and things are out there. For a lot of tools, it is an issue more of choreography than technology. It is an issue of getting the incentives and the government plays to be in alignment.

Now, you may ask, why doesn't the U.S. Government embrace this? Or why doesn't the administration embrace this since the law authorizes it? Frankly, it is because Customs does not have the resources to do a red lane; it can't put any friction in the system.

Everybody gets a green lane right now, everybody comes through, and it would take having more inspectors for those who are not complying with the protocols already laid down to create, essentially, some friction for not doing the good things for this to work and in the absence of resources for them to actually do that.

Commissioner Bonner is legitimately concerned about creating a paper target of saying go ahead and make this expense, we promise to treat you better, but it turns out everybody's getting the same treatment anyway. And so it comes down to—but when we talk about investment, and I think this is a number that should help to frame this issue, we are a nation at war. We have spent since 9/11, as I said in my testimony, just over \$500 million on port security. In 3 years, we have spent what we are spending every 3 days in the war in Iraq.

Both of these are elements for any strategy to deal with the war on terrorism. We have the political will. We have the resources to take the battle to the enemy, but we haven't demonstrated the will to protect the things that are most valuable to us and the most likely targets by our enemies as we look forward.

Mr. LOBIONDO. Thank you, Mr. Gilcrest.

Dr. Flynn, your testimony laid out a worst-case scenario in which terrorists exploit the holes in the procedures to protect our facilities, vessels and cargo. In your view—I am going to ask you for three categories—what is the most important thing? We can almost be overwhelmed by what you are telling us, and I think, especially on this committee, we understand and have sort of been preaching off the same sheet you have been. But to get something that is actionable, I don't think we can throw out so broad a net, but maybe we can be more successful if we can get down to some very single-shot specifics.

So what is the single most important additional action that you would take in each of these three categories for screening vessels, for screening cargo and to protect port facilities, if it is possible?

Mr. FLYNN. On the vessels, I think the most important thing is just monitoring your position. So simply forcing a tracking regime which is from point of origin to the arrival in the United States, I think, is the most straightforward thing.

Again, virtually every vessel carries INMARSAT technology, which is how they communicate to the front office. It is your satellite version of a cell phone call. When you make a call, it knows where you are. Mandating that basically that information be available to verify you are on the course that you have told us you would be on is something that could happen with virtually no huge expense on the industry.

There are some interesting dynamics here about endorsing a particular satellite communications technology vis-a-vis the Europeans, which has sort of slowed this whole thing down, but regardless of what the provider is, you just say, use it; you have got 60 days, figure it out.

That is important because it allows us to verify ships, they are doing what they are expected to do, they have not been hijacked or slowed down, they are operating on schedule as predicted.

On screening cargo, I would have to say I was agnostic about this technology for a while because the imaging was not quite great. It was also the issue of slowing down. You had to stop trucks to do it, but the new screening technology, in 15 seconds, you get an image plus a radiation signature at this very low cost.

This technology exists. Deploying it in all the world's major ports is a \$500 million price tag. Again, that is 3 days in Iraq, that is four F-22 fighters. That is taking a system central to our economy and making it more secure. It is not something the U.S. Government would have to pay every bit of. It would help if developing countries would provide assistance to do it. It is not a cure-all system, and I would be concerned about just relying on a single-point approach, which is getting the radiation image, getting the stuff.

But here is what that would do for you; if you have the image of everything that came through, you can develop software that starts to spot anomalies. Basically, you know what sneakers look like. You know what a shipment of underwear looks like. You know all the various stuff that is out. Right now all we have is a piece of paper. We do not quite really know what it looks like unless you really get the nitty-gritty, and there are some field agents that do it. But the technology would be able to scan that and say, hey, there is something here that does not belong here.

Mr. LOBIONDO. How close are we to something like that?

Mr. FLYNN. It exists. It has been fielded and tested. We can do it. We have done it at various places here in the U.S. Again, I pushed to try it in the world's busiest place, because if you can do it there, you can do it anywhere. And that turns out to be a HIT terminal in Hong Kong, so we will see how it goes.

The other thing that allows you to do is you can delegate—

Mr. LOBIONDO. Excuse me just a minute. Now, I am very interested in that system. They are going to—Hong Kong is going to do this on every cargo container?

Mr. FLYNN. They are going to do it on every truck coming into the gate, into the terminal, and another modern terminal in Hong Kong is going to do it for when something comes off the barges before it is loaded in a large ship to deal with the transshipment problem, which is a huge vulnerability.

Mr. LOBIONDO. And they feel that the throughput is not going to stifle their productivity?

Mr. FLYNN. They are going to run it for 3 months and see how it goes. But the port of Hong Kong is 24 hours, 7 days a week, 365 days a year. HIT terminal can do 10 post-Panamic ships simultaneously, 3 to 4 gantry cranes per ship, 30 moves per hour per crane. If you want to talk about a place that worries about throughput, the terminal was built in 1992 for 3.1 million TEUs. Today it is pushing through 5-1/2 million on the same footprint. They work boxes six high. It is an extraordinary bit of systems engineering, but it is also a case where technology lines up. It is so automated a system, you can police it. There are very few people on the terminal. Everything has to be precisely where it needs to

be, or else it would cause basically constipation in the port. So their ability to maintain it is quite high.

So we are going to see. I would be in a position hopefully a month from now to come back and talk about this, and you would be in a position to do this as well. This is a venture capital operation by one company, SCIC, and in the port of Hong Kong, terminal operators have agreed to do it as a proof of concept. So it will be something I think it is worth your pursuing, asking how the results went to see if it works. If it does not work, then we know we have to go back to the drawing board. But the sense here is, as I see it, it looks quite promising.

The last thing I want to point out, it is not just the images so you can basically help the Customs eye so you can develop some software, but one of the real issues we have is if we shut down the system, how do we restore it? How do we restore public confidence? How do we get the container ships moving again? Every day there are 15 days of containers out there at sea, and if we have not vetted them properly—and the people have panicked; the mayor of L.A. does not want a ship coming in because something just happened on Port Elizabeth, we want to be able to point to something, why we can let that ship come in.

What we would be able to do is replay the tape of every container on there, our Customs official could look at it, and then basically say the reason why, Mr. Mayor, you can—we feel comfortable letting the ship come in is because we just, with our team, scrutinized every container on it. We sent the Coast Guard out to check the vessel. We can bring that ship in. We do not have to shut down the trade system to sort this thing out. So it is a powerful tool.

The last part is it does allow you to give foreign Customs officials—you can delegate this to them because inspector A is going to have a tape that can be back here in the U.S., so if they waive something through because of the issue of corruption, and you can immediately identify they should not have, it creates an honesty system that allows you to delegate, to not just oversee Customs agents, but potentially private players as well; because you can have your governmental oversight remotely to spot check and keep it, and that allows you to get at the volumes.

So I think it is a powerful tool. And along with that, you should also be asking about what the results of operations of, say, Commerce are. These are for tracking devices, the smart boxes, how they work, what are their false alarm rates, those kinds of things. But the technology is available. It is a question of how do we harness it, what do agencies do when they get the information, what are the protocols when we find there is a problem. It is more an issue of structure of government and resources that it has to deal with this than it really is of the tools that are out there. Really, the heavy lift is process more than it is that the tools are there.

Mr. LOBIONDO. Do you have any additional recommendations for how we are handling intelligence in this area?

Mr. FLYNN. Well, really, I want to very much echo the 9/11 Commission's message about reaching out to the private sector. This has been a particularly difficult issue in the maritime arena, because so much of the maritime industry is actually owned by foreign companies. You know, there is no major container line in the

United States, outside of Matson Line, that does Jones Act kind of activity. The American Presidential Line is now owned by the Singaporeans; Sealand is now owned by Maersk A.P. Mueller. So when you are talking about securedness, you cannot talk about it by just reaching out to domestic players. The U.S. Government has a very difficult time trying to figure out how to sit down with international counterparts. But what the incentive is for the foreign terminal operator to get involved in this conversation—and, specifically, I have worked with John Meredith, who is the Group Managing director of Hutchinson Port Holdings—his incentive for dealing with this is a fear that the only tool in America's tool bag is a kill switch if something goes wrong. He has 35 ports in the world. He moves 41 million containers each year. If we throw a kill switch, his entire operation implodes. So he wants to provide—he has a market case for wanting to help the U.S. Government solve this problem so his whole enterprise does not implode.

So one of the things I would say is you really need to reach out to this community. And they have eyes and ears, and they have opportunities as well that they would make available for our people to go to their facilities and learn more about how they work and how they operate.

Another very critical area, I would say, is the challenge that Customs and Coast Guard is facing, and it is a problem across the board with critical infrastructure protection. There is very little resident expertise inside the U.S. Government about how these sectors and networks work. I had very little as a Coast Guard officer, until I got sort of out of the operational side and got more in the academic side and the work they have been doing since. You get a little piece of the elephant, but you do not see the big picture. One of the things that I have found the private sector very willing to do is to host people coming in and learning about their industry.

Customs has the job of policing supply chains. There are very few Customs officers who understand supply chains. It is, I think, a central issue that was completely overlooked in creating the Department of Homeland Security. We have taken what was once a very simple task, the issue of looking at a passport for an immigration official in your face. Now, all of a sudden, we are asking our frontline agents to basically multitask across the issues of immigration, food and agriculture, and Customs at one face of the border, to be able to be comfortable dealing with international counterparts, to work within a complex industry in supply chains and so forth here, to use new technologies, and we are doing it on the backs of GS-9s, with an OJT training basis which these agencies operate on.

At any given time, 30 percent of the naval officer core is in training and education. We have recognized this is a sophisticated environment. They need to learn and be at the top of their game. We have none of that capability for the frontline men and women who are doing so much of this stuff.

So these are real big issues. But it comes back to, I think, something that we really—it is a challenge and I do not know how this committee takes on it here, but it is one I have tried to raise, is that any given day how much are we willing to spend on what we call national security and the tools that we provide for that versus

what we are now saying homeland security is. Homeland security is a part of national security and we need to rethink whether another dollar for missile defense may be better spent going to speed up the Coast Guard's deepwater program, or better spent going to the Port of L.A. and Long Beach so it can actually have a vulnerability plan done. But we have nowhere in this town to have that conversation, because the oversight for national security dollars is stovepiped in OMB and the congressional oversight all the way through, so we have this quirkiness.

Critical infrastructure protection. In the budget identified this year, there is \$14.1 billion that OMB says is going to critical infrastructure protection, and \$7.6 billion of that is to protect U.S. military bases. Tom Ridge gets \$2.9 billion for everything else.

Now, I know why I attack the United States overseas, the USS Cole and embassy, that is America. But if I am here, what am I going to target, the port of San Diego or the port of L.A. Long Beach? But we have this quirky system right now where there is Port Elizabeth or the port of Long Beach, it is just the property tax owners of the county or cities of those areas that are responsible for the security of those ports. I think there is a real equity issue there that we need to debate about. And given its vital importance for our very way of life, and that we know terrorists are targeting this infrastructure, we have to rethink about where we are setting priorities, I think, by looking at the whole picture, not just a slice of what we call homeland security.

Mr. LOBIONDO. Dr. Flynn, I thank you very much. We very much appreciate your thoughts and we are going to do our best to try to keep the heat turned up here.

Mr. FLYNN. Great. I commend the committee for all it has done.

Mr. LOBIONDO. Thank you very much.

With that, the committee will stand adjourned.

[Whereupon, at 4:08 p.m., the subcommittee was adjourned.]

COUNCIL ON FOREIGN RELATIONS

58 EAST 68TH STREET • NEW YORK • NEW YORK 10021
Tel 212 434 9400 Fax 212 434 9875

“The Ongoing Neglect of Maritime Transportation Security”

Written Testimony before

a hearing of the

Subcommittee on Coast Guard and Maritime Transportation
Committee on Transportation and Infrastructure

United States House of Representatives

on

“The 9/11 Commission’s Maritime Transportation Security Proposals”

by

Stephen E. Flynn, Ph.D.
Commander, U.S. Coast Guard (ret.)
Jeane J. Kirkpatrick Senior Fellow in National Security Studies

Room 2167
Rayburn House Office Building
Washington, D.C.

2:00 p.m.
August 25, 2004

“The Ongoing Neglect of Maritime Transportation Security”

by

Stephen E. Flynn

Jeane J. Kirkpatrick Senior Fellow

For National Security Studies

Chairman LoBiondo and distinguished members of the House Subcommittee on Coast Guard and Maritime Transportation. I am the Jeane J. Kirkpatrick Senior Fellow in National Security Studies at the Council on Foreign Relations. I am honored to be appearing before you this morning to discuss the vitally important issue of maritime transportation security. This has been a topic that has been a focus of my professional life for better part of a decade. As I have testified on eight occasions over the past three year, I believe maritime transportation is one of our nation’s most serious vulnerabilities, and we are simply not doing enough to respond to the terrorist threat to this critical sector.

The nation owes an enormous debt of gratitude to the commissioners and the dedicated staff of the 9/11 Commission. Their report should serve as an antidote for anyone in Washington who thinks that we can afford to take a business-as-usual approach to confronting the threat of catastrophic terrorism. From my perspective, the report makes three central points central to understanding our post-9/11 world. First, that the attacks on New York and Washington were a meticulously planned and executed campaign directed by a tenacious enemy intent on exploiting America’s most glaring vulnerability—its largely unprotected homefront. Second, prior to 9/11, the U.S. government was neither focused on nor effectively organized to confront this threat—and that neither Democrats nor Republicans are blameless for that unhappy state of affairs. Third, that despite the horror of that day and the passing of nearly three years, there is much work to be done towards making the critical infrastructure that underpins U.S. power less of a soft target.

I would be less than candid if I did not acknowledge that the hearing today sparks within me a sense of déjà vu. Prior to 9/11 I had the privilege to work with former Senators Gary Hart and Warren Rudman and the U.S. Commission on National Security/21st Century. As the members of this committee know, that commission concluded after three years of study in its final report released in January 2001, that the greatest national security challenge for the United State was the threat of catastrophic terrorism and that the federal government was not organized to confront that threat. Like the 9/11 Commission, the Hart-Rudman Commission was a blue-ribbon, bipartisan group chartered by Congress. Unfortunately, in our case, that did not prevent Washington from largely ignoring the report. This hearing and the others underway this month when Congress is usually in recess suggests that things may be different this time around. For the sake of our nation, I certainly hope that this will be the case, and that the recommendations of this Commission will be acted upon with dispatch.

I am confident that the 9/11 Commission would readily acknowledge that, had they had more time, one of the areas they would have spent it is on would have been in

fleshing out their recommendations for improving transportation security specifically, and critical infrastructure protection more generally. This is not the strongest part of their report. Still, the Commission has performed a valuable service by documenting:

- (1) That during the decade before September 11, 2001, counter-terrorism measures as a part of border security was not seen as a national security matter and were largely neglected.
- (2) That there remains a serious lack of balance in our investment in protecting the transportation sector with over ninety percent of the nation's annual investment in TSA going to aviation—and virtually all of that has been dedicated to only passenger security.
- (3) That the risk of harm is great or greater in the maritime and surface transportation modes.
- (4) That TSA still not has developed an integrated strategic plan for the transportation sector nor has it developed plans to protect the individual modes of transportation.

Based on my assessment of the state of transportation security both before and since 9/11, I agree with all these findings. I would add to that list my concern that many of the helpful measures being pursued by the administration in the area of maritime transportation security are not being adequately resourced to address the threat to this sector. Specifically, in my testimony today, I will point out the critical shortcomings in the major post-9/11 security initiatives that deserve the immediate attention of the White House and the Congress.

Officially July 1, 2004 marked the dawning of a new age for maritime security. The International Ship and Port Facility Security Code (ISPS) is now in force. 22,539 vessels that ply the seas and the 7,974 port facilities that serve as their on-ramps and off-ramps should be abiding by new security measures adopted by the International Maritime Organization in December 2001. Congress gave the code the force of law when it adopted the Maritime Transportation Security Act of 2002. But the new mandate has not come with the resources required to meet it. Since 9/11 Washington has provided only \$516 million dollars towards the \$5.6 billion the Coast Guard estimates U.S. ports need to make them minimally secure. In the FY2005 budget, the White House asked for just \$50 million more. Given the severe constraints on the state and local budgets within the jurisdictions where America's commercial seaports are located, it is difficult to see how these ports are in any position to bankroll the new security requirements that have been thrust upon them.

Congress also failed to authorize new funding to pay for staffing and training Coast Guard inspectors to verify that everyone is following the new rules. This is so even though the Maritime Transportation Security Act mandates that the Department of Homeland Security certify annually that ports and ships engaged in commerce with the United States are compliant with the code. The evidence to date is that much of the international maritime community is simply going through the motions. On the day the

ISPS code went into force, only one-half of the world's port facilities had gotten around to submitting their security plans—and most were thrown together in the final weeks before the deadline. In the United States, according to a GAO report released on June 30th, every one of the 2,913 facility plans submitted to the Coast Guard in early 2004 were found to be deficient. Just 120 had undertaken the necessary remedial steps to secure approval by mid-June 2004.

The Coast Guard is coping with its new compliance mandate by marshalling small teams of reserve junior officers with limited experience in marine inspections and little to no background in security to do the first round of overseas inspections. I very much worry that this approach will send the wrong message to the international maritime community. A series of inconsistent and superficial inspections will communicate to port authorities at home and abroad that the U.S. government is not really that serious about maritime security. This will lead many to decide not to make the kinds of investments they should be making to bolster security. It will also discourage those who have shown a willingness to date to be forward-leaning if they discover others are getting by with making only token efforts.

The Coast Guard is not only struggling to carry out this new assignment, but its fleet of cutters and aircraft are being pushed to the breaking point and beyond to meet the combined imperatives of its traditional missions along with its new maritime homeland security mandate. This sub-committee needs no reminder that the Coast Guard is only slightly larger than the New York Police Department even though it bears the burden of being America's first line of defense along the 95,000 miles of shoreline and the over 3 million square miles of waters that are adjacent to U.S. maritime borders. It is patrolling the nation's coastal waters with vessels and airplanes that are operating long beyond their expected service life. The result is that the already dangerous job of performing these missions is being compounded by frequent engineering casualties that put the lives of Coast Guard men and women at risk. Just this month, one of the service's largest ships, the 378 cutter GALLETTIN which was built in 1968, barely made it out of its homeport to escape Hurricane Charley when one of its main engines died. The lengthy twenty-plus year time table for replacing the Coast Guard's fleet with the Integrated Deepwater System is likely to leave the maritime environment increasingly exposed in the near term as the assets the Coast Guard now has fail far more quickly than they can be replaced. It is inexplicable to me that despite the war on terrorism, that the White House and Congress have been reluctant to accelerate its pre-9/11 schedule to modernize the Coast Guard's obsolete fleet.

Another much touted Coast Guard initiative for improving maritime security is the Automated Identification System (AIS) for tracking ships approaching and operating within U.S. ports and coastal waters. Most Americans are simply flummoxed when they learn that while the FAA can track planes flying throughout our airspace, the U.S. government currently has no means to do the same with ships. The AIS system being pursued by the Coast Guard widely misses the mark of rectifying that situation. Designed only to detect vessels within 20-30 miles of U.S. ports, the system does not provide adequate time to muster an effective response should a vessel pose a threat. This

is because most ocean-going vessels could cover that distance in 1-2 hours. We live in an age when GPS devices are being placed in cellular phones. It makes no sense why the U.S. government is not aggressively pursuing a more ambitious satellite tracking system for monitoring vessel movements once they leave a foreign port and are destined for U.S. waters.

The Customs and Border Protection Directorate at the Department of Homeland Security shares with the Coast Guard the burden of securing the maritime transportation system. CBP has been the lead agency in addressing the risk that cargo containers might be used as a poor man's missile. It has undertaken a number of initiatives since 9/11, but here again the paucity of resources being dedicated to support these efforts leaves America dangerously vulnerable to another act of catastrophic terrorism.

The Container Security Initiative (CSI) is the centerpiece of the administration's effort in this area. This well conceived program involves placing U.S. customs inspectors overseas in the port of loading to target containers for inspection before they are loading on a ship destined for the United States. To date over 24 ports, including all the largest seaports in the world, have signed agreements to participate in the CSI program. That is the good news. The not so good news and that CBP is staffing the CSI program by sending teams of just four to eight inspectors on temporary duty assignments of three to four months duration because the administration has not authorized the overseas billets for longer assignments. Inspectors are receiving no formal language or other training to prepare them for these overseas postings. Given that the teams are so small—only eight inspectors in Hong Kong which is the world largest port, they are able to inspect only the tiniest of percentages of containers.

The companion piece to CSI is the "Customs-Trade Partnership Against Terrorism" or C-TPAT. Under C-TPAT, CBP has reached out to companies and carriers involved in importing goods into the United States. It has asked them to assess the vulnerabilities of their supply chains and to put in place measures to address any weaknesses that they discover. Companies that join C-TPAT enhance the odds that CBP will view them as low-risk shippers which translates into their conveyances or shipments not being subjected to routine examinations. Like CSI, the underlying logic of the program is laudable. Unfortunately, CBP is not adequately staffed to even review the nearly five thousand initial C-TPAT applications it has received. Worse still, they do not have the manpower to provide an ongoing system that verifies that companies are actually taking tangible steps to bolster supply chain and transportation security. As a result, the regime is essentially, a "trust-but-don't-verify" approach.

What this means is that the maritime transportation system remains a very soft target for America's enemies to exploit. As we have learned from the intelligence that led to the most recent Orange alert on August 1, al Qaeda is committed to targeting critical infrastructure and is willing to invest considerable time and energy in staking it out and formulating complex plans to evade the security measures that are in place. I have little doubt that al Qaeda possesses the means to identify those users of the maritime transportation system that U.S. authorities currently view as low-security risks. I also

believe that they are fully capable of exploiting the many opportunities to intercept and compromise these legitimate shipments either at their point of origin or anywhere along the transportation route they travel. I am deeply concerned that despite the efforts made by the U.S. government to date; only an extraordinary instance of good luck would allow U.S. authorities to detect a compromised "low-risk" user in time to foil a terrorist attack.

All this sets us up for a possible worse-case scenario where we will have a terrorist incident involving a C-TPAT company, who ships their good from an ISPS certified port facility located in a port that is a participant in CSI, aboard an ISPS certified ship, that unloads its cargo on to a train or truck upon arrival in the United States, and then sets off a weapon of mass destruction in America's heartland. Our enemies will then successfully discredit the entire regime now in place. Since no shipment will be able to be viewed as low-risk, U.S. authorities will have to attempt to inspect all shipments while it scrambles to then put a credible, verifiable security regime in place. In the interim we could bring the U.S. economy and the entire international trade system to its knees.

In short, a token security effort in the maritime transportation sector may prove worse than making no effort at all. This is because it seduces the American people into having a false sense of security that forestalls making real investments in protecting our critical infrastructure. Further, it will almost certainly generate a severe loss of public confidence in the federal government when those measures are shown to have been entirely insufficient following a successful attack. Announcing ambitious security initiatives without providing adequate resources to make them credible is dangerous business. It practically assures that we will have future hearings like this one, where blue-ribbon commissions will be testifying that too little was done to secure Americans from the real and present danger of catastrophic terrorist attacks on the United States.

Thank you Mr. Chairman for this opportunity to testify before you on this very serious issue. I look forward to responding to your questions.

**Prepared Statement of
Commissioner Jamie Gorelick and Commissioner John Lehman
National Commission on Terrorist Attack Upon the United States
Subcommittee on Coast Guard and Maritime Transportation
Committee on Transportation and Infrastructure
U.S. House of Representatives
August 25, 2004**

Maritime Transportation Security

Chairman LoBiondo, Ranking member Filner, distinguished members of the Committee, we thank you for holding this hearing on the 9/11 commission's recommendations.

Mr. Chairman, two years ago, members of Congress on both sides of the aisle worked together in a bipartisan manner to create the National Commission on Terrorist Attacks Upon the United States.

Similarly, over the past 20 months the members of the Commission, five Republicans and five Democrats, have worked together with a sense of unity and purpose. We stand together in unanimous support of our recommendations.

Today, we call upon Congress and the administration to display the same spirit of bipartisanship as we collectively seek to make our country and all Americans safer and more secure.

You asked us to address today the Commission's recommendations as they regard port, vessel, cargo and coastal security. We thank you for this opportunity.

The ability of Americans to travel safely and securely is central to the exercise of our cherished personal freedoms. The capacity to transport goods efficiently and reliably across the country and throughout the world is indispensable to our nation's economic progress. Terrorists know that. It's why they target transportation. It's why we must stop them.

Passenger vessels and cruise ships support travel and tourism for millions of people. America's ports are vital centers of economic activity, handling 95% of our nation's overseas trade. And our country's 95,000 miles of coastline are dotted with high risk facilities including nuclear power stations, oil refineries and chemical plants.

Intelligence

Mr. Chairman, much attention has been devoted to the Commission's recommendations to change the structure of the intelligence community. We are convinced that these crucial reforms will make the nation safer. But we also know that no matter how excellent our intelligence is we simply cannot expose every terrorist or discover every

plot. We have to protect the nation's critical infrastructure vigorously and in a manner this is true to our principles and values.

Maritime Security

The Department of Homeland Security—in particular the Coast Guard and the Bureau of Customs and Border Protection—is vested with enormous responsibilities to protect the maritime transportation system. These agencies are working hard to meet their mission, including implementation of the Maritime Transportation Security Act.

The department has established databases and procedures to monitor cargo, ships, port facilities, crews and passengers. These efforts are aimed at searching for anomalies indicative of high-risk cargo or terrorists on approaching ships. It established more than 100 security zones around particularly sensitive or vulnerable coastal installations, such as major naval bases, key landmarks, and industrial facilities near major cities.

All the major U.S. ports have implemented some physical security measures to prevent terrorists from gaining easy access to ships, facilities, or cargo. As part of this effort, the Coast Guard has established new rules for ships approaching the United States. Yet, Mr. Chairman, significant vulnerabilities remain.

The vast majority of all containers enter the country unchecked. Experts at GAO tell us that documentation requirements are easy to circumvent. Containers shift through the various modes in the transportation process—from trucks, to trains, to ships and back again. Containers from overseas come with risks that they may hold weapons or be used as one.

The Commission believes it is critical that the Department of Homeland Security continue to improve efforts to collect good data on the origins and content of containers. DHS needs to identify those that are suspect, and screen them.

Vulnerability studies of the nation's 50 largest ports are not scheduled to be completed for years, even though some recent assessments have found serious shortcomings in our defenses. The demand for port grants to identify and fill gaps far exceeds the resources available. This makes the Coast Guard's job more difficult, and our ports not as secure as they must be.

Lessons learned

In the aftermath of past catastrophes, such as Pan Am 103 and TWA 800, the nation reacted with a battery of initiatives to address the perceived problem. Some refer to this reactivity as “fighting the last war.” We must, of course, fill the gaps exposed by incidents. It would be irresponsible to do otherwise. But, we can't afford to simply look in the rear view mirror. We must be looking forward, anticipating and stopping the “next war.”

In the late 1990s, Mr. Chairman, the FAA's intelligence unit assessed the possibility that a terrorist group might hijack a domestic commercial flight and crash it into a landmark. We imagined such an attack. We just didn't imagine we had to do anything about it because it had never happened before. We had no "specific and credible" evidence that any group was actually plotting to conduct such an operation. In the post 9/11 world we can't afford to make that same mistake again. We have imagined attacks on our ports, and we know the devastating loss of human life and economic disruption that a major attack could cause. So have the terrorists.

As you know, Mr. Chairman, the Commission did not delve into the specific security requirements of each discrete mode of transportation. We did, however, identify certain principles that we believe apply to all modes, and to our mission of homeland security as a whole. One of those principles is to ensure that limited homeland security resources are allocated to the areas where the terrorist threat to transportation is highest, the nation's vulnerabilities are greatest, and the consequences of a successful attack most severe.

The American people understand that in a free society we cannot protect everything, everywhere, all the time. But they expect the government to make rational decisions.

We believe that to make these hard choices regarding the allocation of limited resources, the United States government must:

- identify and evaluate the transportation assets that need to be protected;
- set risk-based priorities for defending them;
- select the most practical and cost-effective ways of doing so; and
- develop a plan, budget, and funding to implement the effort.

Strategic Planning

Despite congressional deadlines, TSA has not yet finished an integrated strategic plan for the transportation sector. The specific plans for the various modes, including maritime, are not yet complete. Without such plans neither the public nor Congress can be assured we are identifying the highest priority dangers and allocating resources to the most effective security measures.

The transportation sector plan required by Homeland Security Presidential Directive 7 is critical to the security of ports because they are hubs where the various modes of transportation come together.

The sector plan and its modal annexes must provide the detailed elements necessary to assure the public, the administration and Congress that our security systems are comprehensive, properly targeted and well conceived. This includes:

- spelling out specific goals;
- determining what security standards and practices will be employed to achieve them;
- identifying how standards will be enforced and progress measured;
- clearly establishing who's responsible for what elements of the security system; and
- recognizing how much the plans will cost and who should pay for implementation and how.

These are essential elements. It's tough work, and requires difficult decisions, but it must be done. The Commission believes that Congress should:

- set a specific date for the completion of these vital plans;
- hold the Department of Homeland Security responsible for achieving them; and
- assure that the agency has the necessary resources to implement them.

This Committee has long recognized the importance of proper planning. The Maritime Transportation Security Act required the Coast Guard to produce regional security blueprints and to evaluate the plans of facilities and vessels to protect themselves. Yet, an overarching plan to make sure that we are wisely allocating resources in support of maritime security is conspicuously absent.

The Coast Guard, as the lead maritime homeland security agency, focuses on vessel and security. The Bureau of Customs and Border Protection is largely responsible for container security. The agencies have complementary responsibilities and it is essential that they work together in a coordinated fashion. Yet we understand that a memorandum of agreement setting forth the parameters of this relationship still has not been completed. This and other vital interagency agreements to set operational policy need to be finished but are awaiting completion of the sector plan.

TSA is now almost three years old, DHS nearly two. The time for planning to plan is past. We need these vital blueprints, including the delineation of roles and missions, and we need them soon.

Layered System

In implementing our defenses, Mr. Chairman, we must never lose sight of the fact that no layer of security is foolproof. Previous aviation security panels, including the Pan Am Commission in 1990, the Gore Commission in 1997 and the National Research Council in 2002 stressed the importance of the "layered" approach to security. This means

instituting redundant defenses to assure that if one layer breaks down, another is in place to provide protection.

On 9/11 the only layer of protection to stop suicide hijackers was checkpoint screening—a layer that had a long history of problems. It was not designed to stop the short-bladed knives the terrorists carried. The passenger prescreening program was aimed at stopping bombs in checked baggage; not suicide hijackers. And the pre 9/11 hijacking response doctrine required flight crew to cooperate with hijackers, presumably because they sought transport or hostages.

Once the terrorists passed the checkpoints on 9/11, they were virtually assured of successfully hijacking the aircraft. There were no layers of security to stop them.

Layering has long been a useful tool in promoting aviation safety. We also need a layered approach for all modes of transportation security, so that no single point of failure is catastrophic.

Examining the manifest of a container is one layer of security, but identifying its origins, tracking its transport, and screening its contents are additional layers that are crucial to an effective security system.

As it plans and implements transportation security, the Department of Homeland Security must take into consideration the full array of possible enemy tactics, and assure that we have reliable layers coordinated to stop them.

Congressional Oversight

Before 9/11 FAA's security division listed the various ways in which commercial aviation could be attacked and the corresponding defenses. As the events of 9/11 proved, this matrix was incomplete.

We think it's very important that Congress provide vigorous oversight of these planning documents and their implementation. The Department of Homeland Security should be required to list all the various forms of attack that could be lodged against the nation's maritime transportation system, taking into consideration the different tactics that terrorists could employ. It should identify the layers in place to address each form of attack, and evaluate the reliability of each layer. This will help the Homeland Security Department, the administration and Congress better identify and address weaknesses we must fix. It will also help us pinpoint honestly those areas where we will remain vulnerable in the near term.

This effort should be an integral part of the planning and oversight process. Comprehensiveness, transparency, candor and accountability are the watch words.

No Transport Lists

Mr. Chairman, one of the most essential layers of security we can employ is stopping individuals that the United States government knows or strongly suspects to be terrorists from entering our country and accessing our transportation systems. One of the Commission's recommendations was to improve the use of terrorist watch lists to stop known or suspected terrorists from boarding commercial flights.

Currently, TSA provides two security watchlists to air carriers. One is a no-fly list. The second is a list of suspicious individuals who should receive special screening at the checkpoint—known as “automatic selectees.”

We understand DHS is planning to move forward with an advanced passenger information system to examine passenger and crew information for cruise ships. It seems reasonable that we should use the same lists to stop terrorists from boarding seagoing vessels as we do in the aviation sector.

Not only could this procedure stop a terrorist from boarding a vessel that he or she might intend to commandeer or sabotage, but it would help disrupt terrorist travel, an important goal in its own right.

How, Mr. Chairman, would the United States government explain it to the American people if an individual boarded and attacked a cruise liner when that person was barred from boarding a jetliner and we had the opportunity to stop them with an instantaneous electronic check?

The Commission also believes that we should continue every effort to share watchlists with nations allied in the war against terror to increase the effectiveness of immigration and transportation watchlisting. Successfully fighting global terrorism requires global cooperation.

Conclusion

In conclusion, Mr. Chairman, the Commission is mindful that our recommendations will require substantial investments of taxpayer dollars. But we have seen the devastating costs in human life and economic disruption that result from a successful attack. Our investments in homeland security are worthwhile. They are essential to the government's Constitutional duty to provide for the common defense.

We wish to thank you and this committee for holding this hearing. Our recommendations are intended to make our country safer and more secure, while preserving cherished freedoms and the American way of life. America is about freedom. Among those liberties should be the freedom from the fear of terrorism as we go about our daily lives.

We would be pleased to respond to your questions. Thank you.

###

DEPARTMENT OF HOMELAND SECURITY
UNITED STATES COAST GUARD
STATEMENT OF
REAR ADMIRAL LARRY HERETH AND MR. JAMES F. SLOAN
ON THE
9/11 COMMISSION REPORT AND MARITIME TRANSPORTATION SECURITY
BEFORE THE
SUBCOMMITTEE ON COAST GUARD & MARITIME TRANSPORTATION
COMMITTEE ON TRANSPORTATION & INFRASTRUCTURE
U.S. HOUSE OF REPRESENTATIVES
AUGUST 25, 2004

Good afternoon Mr. Chairman and distinguished Members of the Committee. It is our pleasure to be here today to discuss the Coast Guard's continuing efforts in securing our Nation's ports and waterways.

Introduction

Prior to September 11, 2001, the Coast Guard's primary focus had been on safety, law enforcement, environmental protection, and vessel traffic management. Nearly all our national and international efforts revolved around the safe and efficient movement of waterborne commerce, interdicting drugs and illegal migrants, and trade compliance. However, with support from the Administration and Congress, we have acted quickly and affirmatively to make the maritime environment more secure and ensure that it remains one of the most valuable components of our national transportation system.

The 9/11 Commission Report validates the challenges facing our Nation concerning homeland security. A terrorist incident against our marine transportation system would have a disastrous impact on global shipping, international trade, and the world economy, not to mention the strategic military value of many ports and waterways. However, the Coast Guard remains confident, thanks to a supportive team including Customs and Border Protection (CBP), the Transportation Security Administration (TSA), Immigration and Customs Enforcement (ICE), the Maritime Administration (MARAD), our collective maritime stake holders, and State and local governments that we will continue to be successful in meeting the challenge. We are committed to working with other law enforcement agencies and international counterparts as one team, working toward a common goal.

The heart of port security at the local level is the Area Maritime Security Committee (AMSC). These Committees are lead by Federal Maritime Security Coordinators and are comprised of Federal, State, and local agencies, law enforcement and security agencies, and port stakeholders. The AMSC's purpose is to provide a framework to communicate threats, identify risks, and coordinate resources to mitigate threats and vulnerabilities, including threats to critical infrastructure. They also enhance maritime situational awareness and ensure integrated maritime prevention and response operations among the local maritime community.

As an example of national level cooperation, on September 1, 2004, the Coast Guard will hold a public meeting in Washington, D.C. discussing information sharing mechanisms that will allow the Federal government to share threat information with diverse members of the maritime industry. Our combined efforts have already made America more secure, and efforts such as this September meeting will further advance the Nation's security.

In December 2001, the Coast Guard's relationship with the national Intelligence Community (IC) was formalized when the Congress amended the National Security Act of 1947 to add the Coast Guard's intelligence element as a member of the national IC. Since that time, we have received excellent support from the Director of Central Intelligence, Intelligence Community Management Staff, and other Community members. IC membership has enabled the Coast Guard to provide greater input and have a greater voice within the Community on issues of common concern relating to intelligence requirements and homeland security priorities.

The Coast Guard is a unique organization combining a broad range of authorities, responsibilities, and capabilities as a Federal law enforcement agency, U.S. armed force, emergency response organization, and member of the IC. We are well positioned as the lead federal agency for maritime homeland security and a key component for homeland defense. The Coast Guard Intelligence Program has the ability to link, fuse, analyze, and share information among law enforcement and intelligence community members. This synergy has become a mandate for intelligence and law enforcement agencies in the post-September 11th environment, and the Coast Guard intelligence organization can serve as a model for that cooperation.

Maritime Strategy for Homeland Security

The establishment of DHS put our Federal Government's awareness, prevention, protection, response, and recovery capabilities under one umbrella, improving communication and increasing cooperation among agencies. The 9/11 Commission recommended a layered security system, a concept DHS continues to advocate strongly along with risk prioritization. This model was used by CBP, TSA, MARAD, the maritime industry, and the Coast Guard as we worked together to support efforts to implement the Maritime Transportation Security Act of 2002 (MTSA) and the corresponding International Ship and Port Facility Security (ISPS) Code.

Furthermore, the Coast Guard has been given the lead in development and implementation of a comprehensive Maritime Strategy for Homeland Security that 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 current needs while maintaining a strategic outlook on the threats and opportunities of the future. The foundation for the maritime strategy is a layered defense – a proven means to enhance security in U.S. ports and waterways while concurrently facilitating commerce. The collective results of our efforts are aimed at managing and reducing maritime security risks.

Secretary Ridge is also implementing the strategic goals of Awareness, Prevention, Protection, Response, and Recovery.

Awareness - Maritime Domain Awareness (MDA)

The Coast Guard is using an interagency approach for establishing MDA. By leveraging information technology and using multiple information sources, our ability to achieve better MDA will allow us to focus our protection and response efforts more effectively on those trade transactions, individuals, and activities of interest. The core of our MDA efforts revolve around the development and use of accurate information, intelligence, and knowledge of vessels, cargo, crews, and passengers – and extending this well beyond our traditional maritime boundaries. All DHS components are working hard to 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. In the past two years, the Coast Guard has dramatically improved its organic intelligence capabilities as well as its collection, analysis, and timely sharing of intelligence information on vessels, people, and dangerous cargoes before their arrival at United States ports.

The following provides a brief overview of our collective efforts following 9/11:

- The Coast Guard is leading an interagency and joint Service effort to develop a comprehensive national MDA plan and system architecture. The 9/11 Commission's Report suggested that the government identify and evaluate transportation assets needing protection, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the efforts. A comprehensive MDA plan will address this need.
- The Coast Guard Intelligence Coordination Center (ICC), 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 (containing crew, passenger, cargo, and shipping line information) from the National Vessel Movement Center (NVMC) are analyzed using law enforcement and intelligence information and vessels of interest are identified so the Coast Guard and other agencies can appropriately respond and, if necessary, board those vessels before they reach port. The Coast Guard and CBP have exchanged personnel, enhancing data sharing between the Coast Guard Intelligence Coordination Center's COASTWATCH and CBP's National Targeting Center (NTC) which tracks inbound cargo and people data).
- The Coast Guard is establishing a network for receiving and distributing Automatic Identification System (AIS) reports (position, speed, course, cargo, etc.) from ships using existing Vessel Traffic Services in ten of our Nation's ports, waterways, and coastal areas. This initiative will progress to other strategically significant U.S. seaports and ultimately extend to nationwide coverage.
- The Coast Guard is researching technologies and systems that track vessels entering, departing or transiting U.S. waters and can track vessels bound for the United States from overseas locations. We are currently working with the International Maritime Organization (IMO) to develop functional and technical requirements for long range tracking out to 2,000 nautical miles (which is approximately the distance from shore a vessel is when they must provide their 96-hour notice of arrival). The United States is working with the IMO on an amendment for this initiative.

- There are 361 total domestic ports of which 55 are deemed militarily or economically critical (15%). Of these 55 ports, 14 Port Threat Assessments (PTAs) have been completed (27%), with 5 more scheduled for completion by the end of fiscal year 2004. The remaining 36 PTAs are planned for completion by early fiscal year 2006. Funding for PTAs is included in the fiscal year 2005 budget and will enable the Coast Guard to complete PTA's on the 55 military and economically critical ports by early fiscal year 2006.
- In partnership with the Chief of Naval Operations (CNO), the Coast Guard is working to establish 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.
- The Coast Guard, along with TSA, the Department of Energy, and other members of the Intelligence Community, work with CBP's NTC, a 24-hour, 7 day a week operation supporting enforcement and regulatory missions of the various agencies through this network of liaisons.
- As directed by MTSA, the Coast Guard established an International Port Security Program (IPSP). The program combines the knowledge and experience of CBP, TSA, and other Federal agencies in identifying foreign ports posing a potential security risk to international maritime transportation. TSA and CBP provided extensive assistance in developing this program, sharing lessons learned and best practices from TSA's Civil Aviation Security Liaison Officer program and CBP's Container Security Initiative. IPSP began visiting foreign ports in July to measure the extent of these countries' compliance with the ISPS Code.
- The Coast Guard uses a risk management system to identify high interest vessels. Those vessels are targeted for follow-up security boardings and, if determined necessary due to risk, executes vessel escorts and positive control boardings to ensure the safety of the vessel and port during their transit through U.S. waters.
- The Coast Guard established Maritime Intelligence Fusion Centers on the east and west coasts to provide tactical, actionable intelligence to Coast Guard District commanders and units. In addition, the Coast Guard established subordinate Field Intelligence Support Teams (FISTs) in key ports. These teams are actively engaged in intelligence gathering and initial analysis in coordination with Federal, State, and local law enforcement and intelligence agencies. They are "joint" in the broadest sense, providing critical top-down, bottom-up, and horizontal information sharing.

Apart from the initiatives described above, there is consistent and steady improvement in our ability to integrate and correlate information in the field such that we can effectively respond. For example, in July a boarding team from Marine Safety Office (MSO) Philadelphia boarded the M/V CENT KAPTANOGLU to conduct an ISPS Code verification exam. During the boarding, the vessel master stated there was a bomb on the vessel that would explode when they entered Philadelphia. Within a few short hours, agents from the Coast Guard Investigative Service (CGIS), Federal Bureau of

Investigations (FBI), CBP, and local law enforcement responded to determine the veracity of the statement and search the vessel. It was quickly determined to be a hoax and the vessel's master was taken into custody. Though we have more work to do, our partnerships with other government agencies continue to improve on all fronts.

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 trade volume, location and strategic concerns, bringing the total number of operational CSI ports to 33, with ports in Thailand and Malaysia being the most recent additions to the program. Once implemented, nearly 80% 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 cargo manifest information for all modes of transportation. This information will augment that received and analyzed already at the NTC. The Trade Act also requires all modes of transportation, inbound and outbound, to provide information electronically and in advance of arrival. On May 13, 2004, programming changes were completed for the Air Automated Manifest Systems (AMS) application and a schedule for training and implementation was published in the Federal Register on March 1, 2004.
- As part of the National Infrastructure Protection Plan (NIPP), DHS is developing a Transportation Sector-Specific Plan (SSP), designed to provide overall operational planning guidance on transportation security. The Transportation Security Administration, working with the Department of Transportation (DOT) and other Federal agencies, is coordinating DHS's efforts on this initiative. The goals of the Transportation SSP are to reduce the risk of terrorism to the Nation's critical transportation infrastructure, operations, and the people who use them. It will ensure 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. As the lead agency for maritime security, the Coast Guard is responsible for developing the National Maritime Transportation Security Plan (NMTSP), which will harmonize with the Transportation SSP and critical infrastructure protection plans and support our maritime strategy.
- 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 Fiscal year 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 Coast Guard formed a Merchant Mariner Documentation (MMD) Task Force to ensure positive identity of merchant mariners sailing on U.S. flag vessels via appropriate security/background screening. Throughout 2004, the Coast Guard will provide for additional personnel support at Regional Examination Centers to conduct centralized security screening and electronic fingerprinting.
- Just last week, the International Labor Office (ILO) announced that it had received sufficient ratification for an international labor standard designed to create a new biometric identity verification system for the world's 1.2 maritime workers. The standard will go into force in February 2005.
- DHS, DOT, and the Departments of State, Justice, and Commerce 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 Coast Guard are developing a strategic plan for cargo. This initiative, known as the "Secure Systems of Transportation (SST)," will take a systems approach to cargo transportation (i.e. point of origin to point of destination), whereby existing security regimes will be enhanced through regulatory standards and new performance-based options for shippers. SST will ensure security requirements for international and domestic cargo are aligned, and will apply to bulk, break-bulk, and containerized cargo and all modes of transportation. DHS expects that the results of Operation Safe Commerce will help shape the formation of this initiative.
- The Coast Guard has completed port security assessments at 28 ports from the list of 55 top economically and militarily strategic U.S. seaports. PSA field work has been completed at 11 additional ports and reports for these will be completed by in September. All but one of the remaining 16 ports from the list of 55 will be completed in CY04. The one remaining PSA (San Francisco) will commence in CY04 and be completed during the first quarter of 2005.

Additionally, the Coast Guard has met with nearly 60 countries representing the vast majority of all shippers to the United States, 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 Coast Guard implemented strong Port State Control measures to aggressively ensure foreign vessels have approved plans and implement adequate security standards. The measures include tracking performance of all owners, operators, flag

administrations, recognized security organizations, charterers, and port facilities. Noncompliance subjects vessels to a range of control measures, including denial of entry into port or significant delay. This aggressive Port State Control regime has been coupled with the Coast Guard's inter-agency IPSP, comprised of representatives from the Department of State, Department of Defense, CBP, TSA, and MARAD, that assess both the effectiveness 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 existing 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:

- Coast Guard's Deepwater Program: A multi-year, performance-based acquisition that will replace or modernize 90 Coast Guard cutters, 200 fixed wing aircraft and multi-mission 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 coasts of America. In fiscal year 2004, the Deepwater program:
 - Began construction of the first National Security Cutter (frigate-size vessel approximately 425 feet long);
 - Will acquire an additional Maritime Patrol Aircraft (MPA);
 - Will complete design and shipboard integration of Vertical Unmanned Aerial Vehicles (VUAV) and;
 - Commenced conceptual development of the Offshore Patrol Cutter, and delivers 4 Short Range Prosecutors (cutter small boats) for use on the 123' Patrol Boat.
 - Began urgent re-engining of the Coast Guard's fleet of short-range helicopters;
 - Started rehabilitation of the 110-foot Patrol Boat fleet (extending them from 110 feet to 123 feet).

- Prior to the attacks of 9/11, the Coast Guard committed less than 2% of its assets to active port security duty. In the immediate aftermath of 9/11, that percentage surged to nearly 60%. Since then, we rebalanced asset deployments to provide roughly 28% of our assets in coverage of port security – a significant and steady increase in operational presence.
- Coast Guard Maritime Safety and 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 calendar year 2004.
- Coast Guard Maritime Safety and 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.
- The Coast Guard is coordinating with TSA and with cruise line operators to identify technology solutions for screening passengers and their belongings for potential threats. The Coast Guard and TSA are also developing methods for inspecting passengers and vehicles using established ferry transportation systems. Detection technologies and methods must be able to find threats without unduly impacting the flow of passengers and/or vehicles.
- Responding to threat assessments and in support of the Maritime Homeland Security Strategy, Coast Guard Stations Boston and Washington, D.C., were created in fiscal year 2004.
- The Coast Guard has provided support of several National Special Security Events. Thirty-five Coast Guard units, comprising a total of over 650 personnel, supported the G8 summit, and six units were involved during former President Reagan's memorial events.
- As the primary Federal maritime law enforcement agency, Coast Guard personnel provided and are providing comprehensive waterside coverage on and over the water for the Democratic and Republican National Conventions in close coordination with local, State and other Federal maritime law enforcement assets. Numerous Coast Guard units and personnel involved in these events include boat crews, law enforcement boarding teams, pilots and aircrew, support personnel and a wide variety of Coast Guard assets. Coast Guard helicopters assist in security zone surveillance and enforcement. The Coast Guard's Captains of the Port work closely with commercial shipping interests and other waterway users to minimize the effects of security zone enforcement on recreational boating, commercial fishing and the free flow of commerce into and out of the Ports of Boston and New York.

- The Coast Guard's American Waterways Watch (AWW) is an outreach program that encourages the maritime industry and the recreational boating public to report suspicious activity in the areas where they work, live and play. All are asked to report directly to the National Response Center, who will forward details via the Homeland Security Operations Center to the Information Analysis and Infrastructure Protection Directorate of the Department of Homeland Security. If criminal activity is in progress, reporting sources are asked to call 911. Team Coast Guard, active duty, reserve personnel, auxiliary, and civilian, will promote this initiative while conducting normal business.
- Homeland Security Presidential Directive (HSPD) 7 was published late last year. It requires sector-specific agencies to continue their coordination with the private sector including providing support for a sector-coordinating mechanism and the development of information sharing and analysis mechanisms in order to address threats, vulnerabilities, incidents, potential protective measures, and best practices. Utilizing our existing communication capability and industry network, the Coast Guard through its Headquarters Command Center, the Area Maritime Security Committees and the National Response Center has been providing the information sharing mechanism to ensure a means for industry to report suspicious activity that could be indicators of terrorist threats and to share threat products produced by the Department of Homeland Security. We are working to improve our information sharing process by speeding up the flow of information, ensuring the process is a "two-way street", developing a communication tool to electronically share sensitive but unclassified information, and obtaining security clearances for a limited number of industry, state and local representatives. On September 01, we plan to discuss with industry the need for a national maritime mode coordinating entity to represent the concerns of industry in regards to threats and to help guide the design and operation of the needed information sharing process that will meet the needs of industry and government.
- DHS has established the US-VISIT Program, an integrated, automated entry/exit system that records the arrival and departure of foreigners; check's their identities; and authenticated their travel documents using biometrics. The program is already on line at 115 airports and 14 seaports, and since January 2004 this system has already processed more than six million travelers and yielded nearly 800 matches to persons who were the subject of look out bulletins.

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 any possible time, we are aggressively working to improve our response capabilities and readiness. While the above increases in operational presence augment our collective response posture, additional accomplishments and future plans include:

- Secretary Ridge 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, and one fight." For the first time, there will be standardized procedures for responding to emergencies across the nation. A NIMS Integration Center will 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. Once the revisions to the National Response Plan are complete, seminars and training will be held in seven cities nationwide to conduct training on the National Incident Management System.

- Continue deployment of Rescue 21 -- the Coast Guard's maritime 911 command, control, and communications system -- in our ports, waterways, and coastal areas. Nationwide implementation is continuing 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 in communications technology.

Conclusion

Enhancing our maritime security first and foremost requires awareness -- gathering and synthesizing large amounts of information and specific data from many disparate sources to gain knowledge of the entire domain. MDA and the knowledge it imparts assists 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 Coast Guard, TSA, ICE, CBP, MARAD, State and local agencies, and our collective maritime stake holders. No single maritime stake holder, whether it is government, industry, or private sector, can do the job alone. We must continue to work together to improve security.

The Coast Guard welcomes the 9/11 Commission Report and the focus it places on the national intelligence infrastructure and maritime security. While we must remain vigilant and continue improving, the Coast Guard's maritime homeland security strategy has produced significant results since 9/11. We have a rich tradition of answering the nation's call, and we are proud of our accomplishments over the past three years. These improvements highlight the resolve of the Administration and the Congress to protect America and provide a beacon of light for us to navigate through the challenging work remaining on the horizon.

Thank you for the opportunity to testify before you today. We will be happy to answer any questions you may have

STATEMENT OF
THE HONORABLE JAMES OBERSTAR
SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION
9-11 COMMISSION HEARING
AUGUST 25, 2004

America is vulnerable to a terrorist attack. Our maritime transportation system is vulnerable to a terrorist attack. We have over 95,000 miles of coastline. We import more than 7 million shipping containers annually. Thousands of tankers carrying oil and hazardous materials enter our ports each year. And millions of vacationers enjoy their holidays on cruise ships.

Beginning July 1st, every ship and port facility was required to have implemented a security plan approved by the Coast Guard. Yet, somehow, I think we may be missing the picture.

Eighty percent of the drugs that are shipped out of Columbia by water penetrate our security and reach our shores. It would not be difficult for a narco-terrorist to smuggle a weapon of mass destruction into the United States.

Terrorist organizations have used suicide operatives to attack civilian and military maritime platforms with small boats loaded explosives. Al-Qaeda used these methods in the October 2000 U.S.S. Cole (Navy Destroyer) and in the

October 2002, M/V Limburgh (French oil tanker). Other terrorists used these methods in the April 25, 2004 attack at the Basra Oil Terminal in Iraq.

These tactics could be used against cruise ships, Liquefied Natural Gas (LNG) tankers, chemical tankers, or offshore oil facilities. For example, the LOOP oil terminal off the coast of Louisiana handles 25% of the U.S. imported oil. If a small boat with explosives were to attack that facility it could severely impact the price of gas and other oil products and the U.S. economy.

Yet, the Administration has made not developed a coherent strategy that can realistically thwart these types of attacks other than designating areas as “security zones” – which is like simply posting a “no trespassing” sign over a high security area. The Congress authorized the Coast Guard to lease additional aircraft for a West Coast Helicopter Interdiction Tactical Squadron. Yet the Administration has failed to lease these aircraft.

We could be lucky next time and discover a bumbling terrorist like an alert Customs Agent did at the ferry in Port Angeles, Washington. But maybe we won't be so lucky -- and there will be a successor to the 9-11 Commission trying to get the Government to address our security problems.

It's not too late. The turf-wars within the Department of Homeland Security need to end. We need to clarify which agency is in charge of which area of security. We don't need to have the Coast Guard and the Border and Transportation Security Directorate both operating ships on the water.

When this Committee wrote the Maritime Transportation Security Act in 2002, we viewed it as the beginning of our major involvement in improving security along our nation's waterfront. While some would say that you must centralize Congressional oversight so that one Committee has a single mission to oversee the homeland security activities of the Executive Branch, I believe that you must have an expertise in transportation to protect our nation from threats that can be launched through the transportation system. This Committee brings that expertise to the table.

I look forward to hearing from today's witnesses about what more we can do to help prevent another attack against America using our transportation system as a weapon.