AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 109–282

PORT SECURITY

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MAY 17, 2005

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

U.S. GOVERNMENT PRINTING OFFICE

25–728 PDF WASHINGTON : 2006

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

TED STEVENS, Alaska, *Chairman*

JOHN McCAIN, Arizona
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
GORDON H. SMITH, Oregon
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DeMINT, South Carolina
DAVID VITTER, Louisiana

DANIEL K. INOUYE, Hawaii, *Co-Chairman*
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

LISA J. SUTHERLAND, *Republican Staff Director*
CHRISTINE DRAGER KURTH, *Republican Deputy Staff Director*
DAVID RUSSELL, *Republican Chief Counsel*
MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
SAMUEL E. WHITEHORN, *Democratic Deputy Staff Director and General Counsel*
LILA HARPER HELMS, *Democratic Policy Director*

CONTENTS

	Page
Hearing held on May 17, 2005	1
Statement of Senator Inouye	1
Prepared statement	56
Statement of Senator Lautenberg	53
Prepared statement	53
Statement of Senator Bill Nelson	76
Statement of Senator Rockefeller	50
Statement of Senator Stevens	1
Prepared statement	56
Statement of Senator Vitter	75

WITNESSES

Godwin, Jean, Executive Vice President/General Counsel, American Association of Port Authorities	57
Prepared statement	58
Hereth, Rear Admiral Larry, U.S. Coast Guard	13
Prepared statement	14
Jacksta, Robert, Executive Director, Border Security and Facilitation, U.S. Customs and Border Protection	8
Prepared statement	10
Koch, Christopher L., President/CEO, World Shipping Council	60
Prepared statement	62
Ruppersberger, Hon. C.A. "Dutch", U.S. Representative from Maryland	2
Prepared statement	5
Skinner, Richard L., Acting Inspector General, Department of Homeland Security	18
Prepared statement	20
Wrightson, Margaret T., Director, Homeland Security and Justice Issues, U.S. Government Accountability Office	24
Prepared statement	26

APPENDIX

Collins, Thomas H., Admiral, U.S. Coast Guard, letter, dated February 25, 2005, to Hon. Harold Rogers, Chairman, Subcommittee on Homeland Security, Appropriations Committee	94
Koch, Christopher L., letter, dated June 14, 2005, to Hon. Ted Stevens	79
Response to Written Questions Submitted to Jean Godwin by:	
Hon. Daniel K. Inouye	81
Hon. Frank R. Lautenberg	81
Response to Written Questions Submitted to Rear Admiral Larry Hereth by:	
Hon. Maria Cantwell	85
Hon. Daniel K. Inouye	91
Response to Written Questions Submitted to Robert Jacksta by:	
Hon. Daniel K. Inouye	92
Hon. Bill Nelson	82
Response to Written Questions Submitted to Richard L. Skinner by:	
Hon. Daniel K. Inouye	80
Hon. Frank R. Lautenberg	81
Response to Written Questions Submitted by Hon. Daniel K. Inouye to Margaret Wrightson	82

PORT SECURITY

TUESDAY, MAY 17, 2005

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

The Committee met, pursuant to notice, at 10 a.m. in room SR–253, Russell Senate Office Building, Hon. Ted Stevens, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

The CHAIRMAN. Let me open by saying this hearing was at the suggestion of Senator Inouye, and we're trying to find ways to improve security and all modes of transportation. I'm pleased to have an opportunity to review these issues.

Just a week ago, I spent the major part of the day at the Los Angeles Port, which has grown so large that it's hard to realize. Their terminals are out in San Bernardino for the sort of freight that's coming off of vessels, and they're building three railroads to move that freight to those terminals, because of lack of space right in the area of the port itself, so that means that the security in that port is about 100 miles wide. We have an enormous problem with security.

I welcome the interest of my great friend from Hawaii. Senator Inouye?

STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Senator INOUYE. Mr. Chairman, I thank you very much. I have a statement here, but I'm just concerned that, when we speak of security, I think the average American thinks of airports. They don't realize that we spend less than 10 percent for ports; 20 percent of the global trade is maritime, and, of that amount, we have about 4 percent; but, whatever it is, our ports are always filled, and yet I don't think that our security there is sufficient, just like our borders.

But I'd like to know what we should be doing. The Coast Guard is overwhelmed. They're doing a great job. All of the new security agencies are trying their best, but their best may not be sufficient, so we're here to listen, believe me, sir.

The CHAIRMAN. Let me say that we have a series of votes that are going to start, so we do hope that the witnesses will recognize that timeframe and limit their statements so that we can go through the list. We have a list of six people who are going to tes-

tify between now and 11:10, so may I urge the witnesses—all the statements will be put in the record in full; if we're going to have a chance to ask questions and to get your responses to our questions, we'll have to limit the statements.

Mr. Ruppersberger?

STATEMENT OF HON. C.A. "DUTCH" RUPPERSBERGER, U.S. REPRESENTATIVE FROM MARYLAND

Mr. RUPPERSBERGER. Yes, OK. Well, thank you, Chairman Stevens, Co–Chairman Inouye, Members of the Committee, Senator Rockefeller, Senator Lautenberg.

I'm honored to be here today to participate in this critical discussion. And with your consent, Mr. Chairman, I have prepared a summary of my complete testimony to read into the record today, and I would ask that my entire testimony be submitted into the record, as well.

The CHAIRMAN. All of the statements that have been submitted will be in the record, as well.

Mr. RUPPERSBERGER. Thank you.

Now, Mr. Chairman and Members of the Committee, my main point to you today is that America's first-responders should not be Congress's second thought. Whether you call it port or maritime security, each of us understands three very fundamental principles:

Number one, securing our Nation's more than 359 sea, river, and land ports is a broad, varied, and complex goal.

Number two, it is simply not possible, nor do I believe it is practical, to protect all of our ports against every possible threat. The reality of limited resources and over 95,000 miles of coastline means we must focus on good intelligence for credible threat information and prioritize our spending accordingly.

Number three, our ports are absolutely critical to our Nation's economic security. In the world of just-in-time commerce and the global marketplace, our ports are attractive to terrorists to either import weapons for destruction or to shut down the global supply chain and cripple our economy. Either possibility makes port security a high priority for this Congress.

The best example of this was in the fall of 2002, when the shippers and dockers went on strike at the West Coast ports. That cost our United States economy $1 billion a day.

Port security is broad and a complex issue, largely due to the reality that ports are sprawling commercial hubs, usually centrally located in geographically diverse areas. Our working ports stretch across coastlines, riverways, and harbors, moving agricultural, mineral, petroleum, and paper products to connect with highways and railways for transport. Tons of goods are imported and exported through our ports every day in bulk in containers as well as roll-on/roll-off vehicles. Our ports are also home to some of our most beloved recreational activities, such as boating, fishing, and cruises, all of which contribute to our economy and our every way of life.

With so many distinguished experts in port security following me on the other panels, I would like to focus my discussion today on one key piece of the security puzzle: the issue of security clear-

ances, both in the general national-security sense and within the specifics of the port-security realm.

From my many roles in the local government as a county executive during and after the aftermath of 9/11 as a former prosecutor, to my current roles at the federal level, as a Member of the House Permanent Select Intelligence Committee, as Co–Chair of the Congressional Port Security Caucus, and as the Congressional Representative to both the Port of Baltimore and NSA, National Security Agency, I believe a modernized, working, security-clearance system is vital to defending our homeland, including our ports.

The Federal Government needs to take further action to ensure that the ability to share information is neither obstructed by a lack of clearance nor by bottlenecks that persist today. Our current security-clearance system is not working. The problem is not just jeopardizing our port security, it is also jeopardizing our national security. Many of the state, local, and business interests, and even some federal officials, do not have the information they need to keep our country safe because they don't have the proper security clearances. The problems stem from basic situations, where workers don't know how to fill out an application, to the more complicated, where one department is not sharing information with another. We're still using a security-clearance system set up to fight the Cold War, even though the Iron Curtain fell years ago and we are now fighting the war on terror. The process is fragmented, confusing, cumbersome, and long.

There are approximately three million individuals at the federal, state and local, and private-sector levels with some level of security clearance. It is estimated that 480,000 clearances are stuck in some sort of a backlog. The average security clearance takes over 1 year to complete. If there is any sort of problem along the way, it can take months, or even years, longer. There are inconsistencies within investigations, polygraph analysis, levels of security, and criteria considerations.

In the 108th Congress, Congressman Waxman, former Congressman Bell, and I asked GAO to look at two critical questions regarding port security specifically, and homeland security in general. The report is being released today.

First, we asked them to look at the issue of information sharing within the port-security domain, and investigate how it is working. Second, we asked them to look at port security as it relates to businesses that are connected to the port, and how funding is prioritized. Specifically, we asked them to investigate the risk-management approach being employed by the Department of Homeland Security in funding and grant decisions.

The GAO report is entitled "Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention." It is the first report GAO is delivering on that request. We asked GAO to review the processes set in place to improve information sharing within maritime security following in our post–9/11 world with the passage of the Homeland Security Act of 2002 and the Maritime Transportation Security Act of 2002.

The Coast Guard has an awesome task of protecting our waterways and securing our Nation's ports. For over 200 years, the

Coast Guard has patrolled and protected our coastlines, which totals today over 95,000 miles. The Coast Guard is doing a good job based on their massive jurisdiction and the funding it has received, but more needs to be done.

After the passage of the MTSA, the Coast Guard reorganized. Each of the country's 359 ports created Area Maritime Security Committees and Interagency Operational Centers to coordinate multiple local, state, and federal agencies, along with private-sector shareholders. This is a good thing. This is about sharing information with local, state, and the private sector. The goal is to facilitate the meaningful necessity of information sharing which is so important to protect our ports. Each committee designated one member, who is expected to have the proper clearance to be able to analyze classified intelligence information, one member of the 359 ports.

The GAO report found that only 28 of the 359 members had submitted the proper paperwork to get a security clearance. That means less than 10 percent of our Nation's ports have access to critical information to keep us safe. Even if all of the remaining 331 members applied for clearance today, it would take at least 1 year to get them cleared. Al Qaeda is not going to wait until workers get clearance to attack our country and our way of life.

We've identified the problem. Now let's address one of the many solutions. These solutions could not be achieved overnight, but they are some initial steps that will start a long journey to fix this problem.

To start, and as a result of the hard work GAO is reporting today, I have introduced a bipartisan amendment with Chairman Tom Davis of Virginia, to the Homeland Security authorization bill expected on the House floor this week. Mr. Chairman, I have brought a copy of that amendment, submitted to the House Rules Committee today, and I would ask that it be inserted into the record, as well.

[The information referred to follows:]

Amendment to H.R. 1817 Offered by Mr. Ruppersberger of Maryland and Mr. Tom Davis of Virginia

At the end of title V, insert the following new section:

SEC. _____.IMPROVING THE SECURITY CLEARANCE PROCESS FOR STATE AND LOCAL FIRST RESPONDERS.

(a) ESTABLISHMENT OF ASSISTANCE FOR SECURITY CLEARANCE DESK.—Section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458; 50 U.S.C. 435b) is amended by redesignating subsection (i) as subsection (j) and by inserting after subsection (h) the following new subsection (i):

"(i) ESTABLISHMENT OF ASSISTANCE FOR SECURITY CLEARANCE DESK.—

"(1) Not later than 90 days after the selection of an agency pursuant to subsection (c), the head of the entity selected pursuant to subsection (b) shall, in consultation with the Department of Homeland Security Office for State and Local Government Coordination, direct the establishment, within any federal department, agency, or entity, of an Assistance for Security Clearance Desk (in this subsection referred to as the 'ASC Desk') to assist State and local personnel referred by any federal departments, agencies, or other entities for the purpose of obtaining personnel security clearances.

"(2) The ASC Desk shall provide information, assistance, and guidance on the processes by which State and local personnel apply for personnel security clear-

ances; initiate and process personnel security investigations and periodic reinvestigations; have personnel security clearances adjudicated; and access information related to the database established and maintained pursuant to subsection (e).

"(3) The ASC Desk shall publish the information, assistance, and guidance required under this section on a Government-maintained website, shall present such information, assistance, and guidance in a format that is easily accessible to State and local personnel, and shall operate a live, in-person, toll-free telephone service to answer questions about the information, assistance, and guidance provided.".

(b) INCORPORATION OF STATE AND LOCAL FIRST RESPONDERS INTO FEDERAL SECURITY CLEARANCE PROCESSES.—Section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458; 50 U.S.C. 435b) is amended—

(1) in subsection (a)(6), by inserting ", and any State and local personnel," before "to access classified information";

(2) by adding at the end of subsection (a) the following new paragraph:

"(9) The term 'State and local personnel' has the meaning provided in subsection 892(f)(3) of the Homeland Security Act of 2002 (6 U.S.C. 482(f)(3)).";

(3) in subsection (c)(1)—

(A) by adding ", as well as State and local personnel," before "who require access to classified information"; and

(B) by striking "security clearances of such employees and contractor personnel" and inserting "such security clearances"; and

(4) in subsection (e), by inserting ", and State and local personnel," after "or government contractor personnel".

Mr. RUPPERSBERGER. This amendment creates a Help Desk, called the ASC Desk, which stands for the Assistance to Security Clearance Desk. This Help Desk is for state and local individuals applying for security clearances. It will guide individuals through the application, investigation, and adjudication process. While agencies still retain the power and authority they have under current law, the ASC Desk will help our first-responders on the front lines having so much trouble getting through our complicated security-clearance process. This security-clearance issue is a problem not only facing the maritime industry, but also facing many federal agencies. All will benefit from this solution.

It is also important that Ambassador Negroponte, the new Director of National Intelligence, and his office have the same tools to keep our families and communities safe. Terrorists do not care if we are Republicans or Democrats when they target us, so we, as Members of Congress, must work together to solve this problem. It is our responsibility to oversee these changes and to ensure that we fix this problem to protect our country from a terrorist attack.

I appreciate the opportunity to appear before you today.

[The prepared statement of Mr. Ruppersberger follows:]

PREPARED STATEMENT OF HON. C.A. "DUTCH" RUPPERSBERGER, U.S. REPRESENTATIVE FROM MARYLAND

Thank you Chairman Stevens, Co-Chairman Inouye and Members of the Committee. I am honored to appear before you today to participate in this critical discussion. With your consent Mr. Chairman, I have prepared a summary of my complete testimony to read into the record today and I would ask that my entire testimony be submitted into the record as well.

Mr. Chairman and Members of the Committee, my main point to you today is that America's first responders should not be Congress's 2nd thought.

Whether you call it port or maritime security, each of us understands 3 very fundamental principles:

1. Securing our Nation's more than 360 sea, river and land ports is a broad, varied and complex goal.

2. It is simply not possible nor do I believe it is practical to protect all of our ports against every possible threat. The reality of limited resources and over 95,000 miles of coastline means we must focus on good intelligence for credible threat information and prioritize our spending accordingly.

3. Our ports are absolutely critical to our Nation's economic security—in the world of "just in time" commerce and the global marketplace—our ports are attractive to terrorists to either import weapons for destruction or to shut down the global supply chain and cripple our economy. Either possibility makes port security a high priority for this Congress.

Port security is broad and a complex issue largely due to the reality that ports are sprawling commercial hubs usually centrally located in geographically diverse areas. Our working ports stretch across coastlines, river ways and harbors moving agricultural, mineral, petroleum, and paper products to connect with highways and railways for transport. Tons of goods are imported and exported through our ports every day in bulk and containers as well as roll-on/roll-off vehicles. Our ports are also home to some of our most beloved recreational activities such as boating, fishing, and cruises—all of which contribute to our economy and our very way of life.

With so many distinguished experts in port security following me on your other panels, I would like to focus my discussion today on one key piece of the security puzzle—the issue of security clearances both in the general national security sense and within the specifics of the port security realm.

From my many roles in local government (as a County Executive during and in the aftermath of 9/11, as a former prosecutor) to my current roles at the federal level (as a Member of the House Permanent Select Committee on Intelligence, as Co-Chair of the Congressional Port Security Caucus, and as the congressional representative to both the Port of Baltimore and NSA), I believe a modernized working security clearance system is vital to defending our homeland, including our ports.

The Federal Government needs to take further action to insure that the ability to share information is neither obstructed by a lack of clearance nor by "bottlenecks" that persist today. Our current security clearance system is not working. This problem is not just jeopardizing our port security. It is also jeopardizing our national security. Many of the state, local, and business interests and even some federal officials do not have the information they need to keep our country safe because they don't have the proper security clearances.

The problems stem from basic situations where workers don't know how to fill out an application . . . to the more complicated where one department is not sharing information with another. We are still using a security clearance system set up to fight the Cold War even though the Iron Curtain fell years ago and we are now fighting the War on Terror. The process is fragmented, confusing, cumbersome, and long.

There are approximately 3 million individuals at the federal, state, local and private sector levels with some level of a security clearance. It is estimated that 480,000 clearances are stuck in some sort of a backlog. The average security clearance takes over one year to complete. If there is any sort of a problem along the way, it can take months or even years longer. There are inconsistencies within investigations, polygraph analyses, levels of scrutiny, and criteria considerations.

In the 108th Congress, Congressman Waxman, former Congressman Bell and I asked GAO to look at two critical questions regarding port security specifically and homeland security in general. The report is being released today. First, we asked them to look at the issue of information sharing within the port security domain and investigate how it is working. Second, we asked them to look at port security as it relates to businesses that are connected to the port and how funding is prioritized. Specifically, we asked them to investigate the risk management approach being employed by the Department of Homeland Security in funding and grant decisions. The GAO report entitled "Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention" (GAO–05–394) is the first report GAO is delivering on that request. We asked GAO to review the processes set in place to improve information sharing within maritime security following in our post-9/11 world with the passage of the Homeland Security Act of 2002 and the Maritime Transportation Security Act (MTSA) of 2002.

The Coast Guard has an awesome task of protecting our waterways and securing our Nation's ports. For over two hundred years, the Coast Guard has patrolled and protected our coast lines—which today totals over 95,000 miles. The Coast Guard is doing a good job based on their massive jurisdiction and the funding it has received but more needs to be done.

After the passage of MTSA, the Coast Guard reorganized and created 359 Area Maritime Security Committees and Interagency Operational Centers in ports across the country to coordinate multiple local, state and federal agencies along with private sector stakeholders. The goal is to facilitate the meaningful necessity of information sharing to protect our ports. Each committee designated one member who is expected to have the proper clearance to be able to analyze classified intelligence information.

The GAO report found that only 28 of the 359 members had submitted the proper paperwork to get a security clearance. That means less than 8 percent of our Nation's ports have access to critical information to keep us safe. Even if all of the remaining 331 members applied for clearance today, it would take a least a year for them to get cleared. Al Qaeda is not going to wait until workers get clearance to attack our country and our way of life.

We've identified the problem. Now let's address one of the many solutions. These solutions can not be achieved overnight but there are some initial steps that will start a long journey to fix this problem. To start and as a result of the hard work GAO is reporting today, I have introduced a bipartisan amendment with Chairman Tom Davis of Virginia to the Homeland Security Authorization bill expected on the House floor this week. Mr. Chairman, I have brought a copy of that amendment submitted to the House Rules Committee today and I would ask that it be inserted into the record as well.

This amendment creates a help desk called the ASK Desk, which stands for the Assistance to Security Clearance Desk. This help desk is for state and local individuals applying for security clearances. It will guide individuals through the application, investigation and adjudication processes. While agencies will still retain the power and authority they have under current law, the ASK Desk will help our first responders on the front lines having so much trouble getting through our complicated security clearance process.

This security clearance issue is a problem not only facing the Maritime Industry but also facing many federal agencies. All will benefit from this solution. It is also important that Ambassador Negroponte, the new Director of National Intelligence, and his office have the same tools to keep our families and communities safe.

Terrorists do not care if we are Republicans or Democrats when they target us so we as Members of Congress must work together to solve this problem. It is our responsibility to oversee these changes and ensure that we fix this problem to protect our country from a terrorist attack.

I appreciate the opportunity to appear before you today.

Senator INOUYE. Congressman, did you say that the average time span required for security investigation is over 1 year?

Mr. RUPPERSBERGER. Over 1 year. That's the information that we have.

Senator INOUYE. And that we——

Mr. RUPPERSBERGER. And sometimes even longer.

Senator INOUYE.—that we have over 480,000 waiting?

Mr. RUPPERSBERGER. That's an estimate, but that's—about 480,000. Complaints from all aspects. You know, one of the key elements in fighting terrorism is good intelligence, and it's also the relationship between our intelligence agencies and our private sector, some of the larger and smaller corporations. And wherever we go—and I think Senator Rockefeller would confirm this, and he's a Member of the Senate Intelligence Committee—that it's constant complaints about how they can't get the clearance, it just takes so long. It's an antiquated process, and, until we fix that process——

My staff just handed me some information—450,000 backlog, 850,000 waiting. So that's a serious process, not only with respect to our ports, but for the safety of our country. I mean, that's why we have a new Director of Intelligence. And hopefully that will be one of Ambassador Negroponte's high priorities.

Senator INOUYE. And did you say that only 10 percent of our ports have personnel who have been cleared to——

Mr. RUPPERSBERGER. Well, no, what you have is, the Coast Guard, who has an awesome responsibility, and they have put together what they call Maritime Security Committees in each one of their ports. And these committees are really the local, and state governments, and people involved working within the port. And that's almost like a strike-force concept. The main focus for the Coast Guard is information sharing. And what happens is that, with respect to information that the Coast Guard has, if it's classified, they have this information that could help protect the ports, but if the members on that committee, especially a designated member, do not have their clearances, they cannot share that information unless the clearances are there. That has to be fixed. Information sharing is one of the most important aspects of intelligence.

Ten percent of Coast Guard identified committee stakeholders, that's all that has been cleared. And then, when they start the clearance process today, if we would go with the way it's working now, it would take 1 year. As I said in my testimony, Al Qaeda is not going to wait for us to get cleared.

Senator INOUYE. Thank you.

The CHAIRMAN. Thank you.

Any questions?

Thank you very much.

Mr. RUPPERSBERGER. Thank you.

The CHAIRMAN. The first panel is Robert Jacksta, Executive Director of Border Security and Facilitation, in Customs; Larry Hereth, Rear Admiral in the Coast Guard; and Mr. Skinner, Acting Inspector General of the Office—in Homeland Security; and Margaret Wrightson, Director, Homeland Security and Justice Issues, GAO.

Let us proceed in the order in which I've announced them. And we'll have—I think if you'd wait until the time the GAO witness is before us before you put up those panels, it'll be better.

Senator ROCKEFELLER. You can't read them, anyway.

The CHAIRMAN. Mr. Jacksta, then Mr.—then Admiral Hereth, then Mr. Skinner, then Ms. Wrightson. Let's have your statements, and then we'll ask questions.

STATEMENT OF ROBERT JACKSTA, EXECUTIVE DIRECTOR, BORDER SECURITY AND FACILITATION, U.S. CUSTOMS AND BORDER PROTECTION

Mr. JACKSTA. Good morning, Mr. Chairman, Senator Inouye, and distinguished Members of the Committee.

Thank you for this opportunity to update the Committee on U.S. Customs and Border Protection, CBP, efforts to strengthen maritime security.

CBP, as the guardian of the Nation's borders, safeguards the homeland foremost by protecting the American public against terrorism and instruments of terror. Today, trained CBP officers, technology, automation, electronic information, and partnerships with trade and foreign governments are concepts that underpin CBP's port security and antiterrorism initiatives. These concepts extend our zone of security outward and reinforce the components of our layered defense strategy.

My remarks today will focus on progress related to the Customs Trade Partnership Against Terrorism, C–TPAT, the Container Security Initiative, CSI, our non-intrusive inspection technology, and implementation of the Maritime Transportation Security Act.

As the Customs Trade Partnership Against Terrorism has evolved, we have steadily added to the rigor of the program. In order to join C–TPAT, a participant must commit to increasing its supply chain security to meet minimal supply-chain-security criteria. Perhaps most importantly, participants also make a commitment to work with their business partners and customers throughout their supply chain to ensure that those businesses also increase their supply-chain-security. Moreover, CBP has worked towards addressing a number of areas, as recommended by GAO. Today, CBP validation is based on risk, using a quantitative risk-assessment tool to identify certified members with high-risk supply chains.

In addition, CBP has published a C–TPAT strategic plan clearly articulating program goals and strategies. CBP has also completed a C–TPAT human-capital plan, which addresses recruitment, training, and workload issues.

Finally, steps have been taken to automate key processes and implement the records-management system to document key decisions and operational events, including decisions made through the validation process and tracking member status. Within 3 years, our experience has grown greatly with the C–TPAT program, and we continue to work very diligently to ensure member compliance.

To meet our priority mission of preventing terrorism and terrorist weapons from entering the United States, CBP has also partnered with other countries on our Container Security Initiative. Almost 26,000 seagoing containers arrive and are offloaded at United States seaports daily. In Fiscal Year 2004, that equated to 9.6 million containers. Under CSI, we are partnering with our foreign governments to identify and inspect high-risk cargo at foreign ports before they are shipped to our seaports and pose a threat to the United States. Today, CSI is operational in 36 foreign ports.

In January 2004, CBP partnered with four C–TPAT importers to incorporate a container-security device into the container sealing-device process. This enhances container security. The initial phase of this initiative was designed to evaluate logistical and operational aspects, evaluate the technology being utilized, and collect and analyze technology-related data.

Currently, CBP is conducting a second phase of activities in cooperation with the C–TPAT members. This expansion utilizes an enhanced version of the container-security device evaluated during previous activities and will incorporate additional sensing capabilities. The second-phase test will incorporate 16 different trade lanes, touching three continents, and seven CSI ports.

Non-intrusive technology is another cornerstone in our layered approach. Technologies deployed to our Nation's ports of entries include large-scale X-ray and gamma-imaging systems, as well as a variety of portable and handheld technologies, to include our recent focus on radiation-detection equipment. CBP has 166 large-scale NII systems deployed to our Nation's ports of entry. There are 59 of these large-scale systems deployed to our seaports.

CBP is also moving quickly to deploy nuclear and radiological-detection equipment to our ports of entry. CBP has deployed over 400 radiation-isotope-identifier devices, and nearly 500 radiation portal monitors (RPMs). CBP is also implementing the deployment of RPMs in the maritime environment, with the ultimate goal of screening 100 percent of all containerized imported cargo for radiation.

Additionally, CBP has deployed personal radiation detectors in quantities necessary for ensuring that there is 100 percent coverage at primary inspection sites, where the final point of contact with CBP takes place.

CBP, in concert with our sister agencies, continues to work toward maritime security, as mandated by the Maritime Transportation Security Act. Efforts include the establishment of the DHS Commercial Operational Advisory Committee (COAC), a subcommittee to assist DHS with the trade perspective on cargo security-performance standards under the MTSA. The COAC recommendations have assisted CBP with understanding the trade community's concerns and priorities. Further, recommendations are assisting CBP's development of a proposed rule requiring that loaded containers be appropriately secured.

CBP is also supporting the implementation of additional MTSA-related issues in coordination with TSA and the Coast Guard. These include the U.S. Coast Guard International Port Security Program, Area Maritime Security Committees, port vulnerability assessments, and the Transportation Worker Identification Credentialing.

Mr. Chairman, Members of the Committee, I believe CBP has demonstrated, and will continue to demonstrate, its leadership and commitment to maritime security efforts. Thank you for the opportunity to testify. I will be happy to answer any questions you may have.

[The prepared statement of Mr. Jacksta follows:]

PREPARED STATEMENT OF ROBERT JACKSTA, EXECUTIVE DIRECTOR, BORDER SECURITY AND FACILITATION, U.S. CUSTOMS AND BORDER PROTECTION

Good morning Mr. Chairman, Senator Inouye, and distinguished Members of the Committee. Thank you for this opportunity to update the Committee on U.S. Customs and Border Protection's (CBP) efforts to strengthen maritime security.

CBP, as the guardian of the Nation's borders, safeguards the homeland—foremost, by protecting the American public against terrorists and the instruments of terror; while at the same time enforcing the laws of the United States and fostering the Nation's economic security through lawful travel and trade. Today, trained CBP Officers, technology, automation, electronic information, and partnerships with the trade and foreign governments are concepts that underpin CBP's port security and anti-terrorism initiatives. These concepts extend our zone of security outward and reinforce the components of our layered defense strategy.

My remarks today will focus on progress related to the Customs-Trade Partnership Against Terrorism (C–TPAT), the Container Security Initiative (CSI), Non-Intrusive Inspection (NII) and Radiation Detection Technology (RDT), and the implementation of the Maritime Transportation Security Act of 2002 (MTSA).

Customs-Trade Partnership Against Terrorism (C–TPAT)

As the Customs-Trade Partnership Against Terrorism (C–TPAT) has evolved, we have steadily added to the rigor of the program. In order to join C–TPAT, a participant must commit to increasing its supply chain security to meet minimal supply chain security criteria. Perhaps most importantly, participants also make a commitment to work with their business partners and customers throughout their supply chains to ensure that those businesses also increase their supply-chain-security. By

leveraging the influence of importers and others on different participants in the supply chain, C–TPAT is able to increase security of United States bound goods to the point of origin (i.e., to the point of container stuffing). This reach is critical to the goal of increasing supply-chain-security.

Moreover, CBP has worked towards addressing a number of areas as recommended by the General Accountability Office. Today, CBP initiates validations based on risk, using a quantitative risk assessment tool to identify certified members with high-risk supply chains. CBP's new validation objective identifies and validates high-risk supply chain components, while engaging C–TPAT members with the greatest leverage over their foreign components of the international supply chain. This refined validation objective allows CBP to direct resources accordingly, where they can have the most impact in meeting the overall objectives of the C–TPAT program. In late October 2004, in discussions with the trade community, we began drafting more clearly defined, minimum-security criteria for importers wishing to participate in the C–TPAT program. After months of constructive dialogue, we developed minimum security criteria designed to accomplish two important goals: first, to offer flexibility to accommodate the diverse business models represented within the international supply chain; and second, to achieve CBP's twin goals of security and facilitation. The minimum-security criteria for importers became effective on March 25, 2005.

In addition, CBP has published the C–TPAT Strategic Plan, clearly articulating program goals and strategies, and completed the C–TPAT Human Capital Plan, which addresses recruitment, training and workload issues.

CBP recognizes the need for effective measures to determine the success of the program. While new measures are under development, C–TPAT currently uses quantifiable workload measures, but gauging deterrence and prevention remains a challenging task. We continue our efforts in this area, focusing on effective measures that help gauge the success of C–TPAT partnership.

Finally, steps have been taken to automate key processes, and implement a records management system to document key decisions and operational events, including decisions made through the validation process, and tracking member status. With 3 years' experience in the program, C–TPAT has successfully increased supply-chain-security through the voluntary enrollment and enhancement of supply-chain-security by the private sector, and learned much about the program and its participants.

The Container Security Initiative (CSI)

To meet our priority mission of preventing terrorists and terrorist weapons from entering the United States, CBP has partnered with other countries on our Container Security Initiative (CSI). Almost 26,000 seagoing containers arrive and are off loaded at United States seaports each day. In Fiscal Year 2004, that equated to 9.6 million cargo containers annually. Because of the sheer volume of sea container traffic and the opportunities it presents for terrorists, containerized shipping is uniquely vulnerable to terrorist exploitation. Under CSI, which is the first program of its kind, we are partnering with foreign governments to identify and inspect high-risk cargo containers at foreign ports before they are shipped to our seaports and pose a threat to the United States and to global trade. Today, CSI is operational in 36 ports. CBP is working towards strategically locating CSI in additional locations focusing on areas of the world where terrorists have a presence. CBP will continue expanding the CSI security network by using advanced technologies while optimizing resources such as the National Targeting Center as a communications hub coordinating domestic and international communication. Through a framework for security and facilitation of global trade, endorsed by the World Customs Organization, CBP intends to strengthen trade data and targeting by promoting harmonized standards for data elements, examinations and risk assessments. Further, to inspect all high-risk containers before they are loaded on board vessels to the United States, CBP plans to continue fostering partnerships with other countries and our trading partners.

CBP Smart Box Initiative

In January 2004, CBP partnered with four C–TPAT importers to incorporate a Container Security Device (CSD) into the container sealing process, along with sealing standards and techniques, in order to develop and implement a Smart Box designed to enhance container security. The initial phase of the initiative was designed to evaluate the logistical and operational aspects, evaluate the technology being utilized, and collect and analyze technology-related data. Data collected during the initial phase, as well as subsequent phases, will be used to assist CBP in developing minimum standards for a Smart Box.

Currently, CBP is conducting a second phase of activities in cooperation with a total of 14 C–TPAT members. This expansion utilizes an enhanced version of the CSD evaluated during previous activities and will incorporate additional sensing capabilities. This second phase test will incorporate 16 different trade lanes touching 3 continents (North America, Europe and Asia) and 7 CSI ports.

Other efforts include participation in the evaluation of technology designed to incorporate additional sensing capabilities with the goal of providing six sided container security. The Department of Homeland Security (DHS) Science and Technology (S&T) Directorate lead this effort. CBP personnel are active members of an Integrated Process and Product Team (IPPT) and are working in coordination with DHS S&T to identify and evaluate future technologies.

Non-Intrusive Inspection and Radiation Detection Technologies

Non-Intrusive Inspection Technology (NII) is another cornerstone in our layered strategy. Technologies deployed to our Nation's sea, air, and land border ports of entry include large-scale X-ray and gamma-imaging systems as well as a variety of portable and hand-held technologies to include our recent focus on radiation detection technology. NII technologies are viewed as force multipliers that enable us to screen or examine a larger portion of the stream of commercial traffic while facilitating the flow of legitimate trade, cargo, and passengers.

CBP has 166 large-scale NII systems deployed to our Nation's air, land, and sea ports of entry. There are 59 of these large scale systems deployed to seaports on both coasts and the Caribbean. The systems include the Vehicle and Cargo Inspection System (VACIS), Mobile VACIS, Truck X-ray, Mobile Truck X-ray, Rail VACIS, Mobile Sea Container Examination Systems, and the Pallet Gamma-ray system. CBP is also moving quickly to deploy nuclear and radiological detection equipment, including Personal Radiation Detectors (PRDs), Radiation Isotope Identifier Devices (RIIDs) and Radiation Portal Monitors (RPMs) to our ports of entry. CBP has deployed over 400 RIIDs and nearly 500 RPMs. CBP is also initiating the deployment of RPMs in the maritime environment with the ultimate goal of screening 100 percent of all containerized imported cargo for radiation. A variety of configurations have been developed and CBP is working with stakeholders to ensure that radiation screening does not significantly impact operations within a port. During the upcoming year CBP looks forward to working with the new DHS Domestic Nuclear Detection Office to couple these varying configurations into a cohesive global architecture to greatly increase the Nation's radiological and nuclear detection capability. Additionally, CBP has deployed PRDs in quantities necessary for ensuring that there is 100 percent coverage at primary, the first point of contact. Currently, over 10,000 PRDs have been deployed. Used in combination with our layered enforcement strategy, these tools currently provide CBP with a significant capacity to detect nuclear or radiological materials.

Maritime Transportation Security Act of 2002 (MTSA) CBP, in concert with our sister agencies, continues to work towards maritime security mandates as outlined in the Maritime Transportation Security Act of 2002 (MTSA). Efforts include the establishment of a DHS Commercial Operational Advisory Committee (COAC) subcommittee. As requested by the Border and Transportation Security Directorate (BTS), a COAC subcommittee was formed to assist DHS with a trade perspective on cargo security performance standards under MTSA.

The COAC's recommendations have assisted CBP with understanding the trade community's concerns and priorities. Further, under the direction of BTS, recommendations are assisting CBP's development of a proposed rule requiring that loaded containers be appropriately secured by use of an International Organization for Standardization (ISO)-compliant high security seal and verified by the carrier prior to being transported by vessel to the United States. CBP is also supporting the implementation of additional MTSA related issues in coordination with BTS, USCG, and the Transportation Security Administration (TSA). These include:

- USCG International Port Security Program—CBP CSI teams work in concert with USCG to conduct joint assessments of foreign ports.
- Area Maritime Security Committees (AMSC)—CBP senior field office managers are participating in the USCG led AMS Committees.
- Port Vulnerability Assessments—CBP field offices participated in the USCG port assessments addressing cargo security operations.
- Transportation Worker Identification Credentialing (TWIC)—CBP is coordinating with TSA and USCG to assist their efforts to develop this program.

Conclusion

Mr. Chairman, Members of the Committee, I have outlined a broad array of initiatives and steps towards enhancing maritime security. I believe CBP has demonstrated and will continue to demonstrate its leadership and commitment to maritime security efforts, and we anticipate that working with our sister agencies under the Department of Homeland Security we will further these efforts.

Thank you again for the opportunity to testify. I will be happy to answer any questions you may have.

The CHAIRMAN. Thank you very much.

Admiral.

STATEMENT OF REAR ADMIRAL LARRY HERETH, U.S. COAST GUARD

Admiral HERETH. Good morning, Mr. Chairman and distinguished Members of the Committee.

I look forward to discussing the Coast Guard's role to secure our ports and ensure the safe and efficient flow of commerce.

The Coast Guard's overarching security goal is to prevent terrorist attacks within the U.S. maritime domain. Doing so requires a risk-based approach to identify and intercept threats, ideally before they reach our shores. Our Nation's maritime transportation system, as mentioned before, is extensive. Protecting this system is a significant challenge. A maritime terrorist attack, with its associated ripple effect, would have a severe impact on the Nation's economy; so, clearly, this is a system we must protect.

Since trade is global, and terrorism is global, we felt obligated and necessary to build a global security regime. Our domestic and international efforts have focused on implementation of MTSA and the corresponding International Ship and Port Facility security code, or the ISPS Code, as it's known. We've collaborated with 147 other countries at the International Maritime Organization to build a new and substantial security code that applies to vessels and to port facilities around the entire world. The international requirements mirror the domestic standards set forth in MTSA.

To complement the new security standards, we worked in parallel with the International Standards Organization to develop an implementation guide to aid companies as they put this—into practice this major change. The IMO and ISO have been key allies in developing the requirements and practical standards that lead to consistency and greater compliance. This international approach provides an efficient and effective security regime that can be checked by all our trading partners, not just the United States.

Implementation, however, has been a big challenge to all the stakeholders. With over 9,000 U.S. vessels, 3,200 U.S. facilities, and 8,000 foreign vessels that trade with the United States, we have a huge challenge before us.

I am pleased to report, however, that the compliance rates are near 99 percent across the board. This was due, in large measure, to the collaboration and excellent relationships we have with industry and with trade associations. You will hear from two of those trade associations in the later panel. The efforts of the AAPA and—American Association of Port Authorities and the World Shipping Council are representative of the helpful advice and support we received throughout the standards-development phase, and are to be commended.

I also note that, as required by MTSA, we have established an International Port Security Program that works in concert with other federal agencies to identify foreign ports posing a potential security risk to the international marine transportation system. To date, we have visited 23 countries. Five countries are currently on our Port Security Advisory List, because they have not implemented the new international standards.

There are, however, long-term challenges ahead. In the post–MTSA ISPF period, we realized the Coast Guard was planning or beginning work on numerous additional security projects. Those efforts were spread out amongst many various offices, and there was also a lot of interagency coordination underway in those efforts. To address this, we developed an inventory of projects to help us refine, align, and coordinate our efforts. Taken together, this list of projects represents the next wave of improvements to maritime security.

Cargo security is another challenge, a long-term challenge that deserves comment. Customs and Border Protection has the lead role in cargo security, and the Coast Guard works to coordinate with our sister agency to align respective agency roles and responsibilities.

When cargo is moved on the waterborne leg of the trade route, the Coast Guard has oversight of the cargo's carriage requirements and the care needed for that cargo while it's in transit, both on the vessel and at the port facility. Customs, CBP, has authority over the cargo contents and the container improvements. Using the information provided through the Coast Guard's 96-hour notice-of-arrival rule and Customs' 24-hour cargo-loading rule, we can act to control vessels, and, thus, their cargoes, that pose an unacceptable risk to our ports. With Coast Guard officers posted at Customs', CBP's, National Targeting Center, we have improved agency coordination, and our collective ability to quickly take appropriate action exists when notified of a cargo problem.

Identity security is another vulnerability that must be addressed. Domestically, the Coast Guard is now supporting TSA to implement the Transportation Worker Identity Credential, and we'll do everything we can to expedite that process.

With regard to foreign seafarers, we presently have a multi-agency workgroup tasked to define the potential improvements possible and provide a proposed course of action. That involves a number of different agencies, including Justice, State, Transportation, and a variety of elements from DHS.

Thank you, again, for the opportunity to testify today. I will be pleased to answer any questions at the appropriate time.

[The prepared statement of Admiral Hereth follows:]

PREPARED STATEMENT OF REAR ADMIRAL LARRY HERETH, U.S. COAST GUARD

Introduction

Good morning Mr. Chairman and distinguished Members of the Committee. It is a pleasure to be here today to discuss the Coast Guard's role in securing our ports in order to facilitate the safe and efficient flow of commerce.

On September 10th, 2001, our primary maritime focus was on the safe and efficient use of America's waterways. However, as a result of the events of 9/11, we have made great progress in securing America's waterways, without impeding commerce. The men and women of the U.S. Coast Guard and the Department of Home-

land Security remain committed to improving maritime homeland security each and every day through continued interagency cooperation and assistance from our partners at the local, state, and international levels as well as maritime industry stakeholders.

Reducing Maritime Risk

The Coast Guard's overarching security goal is to prevent the exploitation of, or terrorist attacks within, the U.S. maritime domain. Doing so requires a threat-based, risk-managed approach to identify and intercept threats well before they reach U.S. shores. The Coast Guard accomplishes this by conducting layered, multi-agency security operations nationwide; while strengthening the security posture and reducing the vulnerability of our ports, with the initial focus being our militarily and economically strategic ports. As we seek to reduce maritime risk, we continually strive to balance each of the Coast Guard's mission requirements to ensure minimal degradation in service to the American public. Looking at their accomplishments, it is clear that Coast Guard men and women continue to rise to the challenge and deliver tangible and important results across both homeland security and non-homeland security missions.

Today's global maritime safety and security environment requires a new level of operations specifically directed against terrorism without degrading other critical maritime safety missions. Most importantly, the Coast Guard must exercise its full suite of authorities, capabilities, competencies and partnerships to mitigate maritime security risks in the post-9/11 world.

In terms of threat, vulnerability, and consequence, there are few more valuable and vulnerable targets than the U.S. maritime transportation system.

- **Threat:** While the 9/11 Commission notes the continuing threat against our aviation system, it also states that "opportunities to do harm are as great, or greater, in maritime or surface transportation." From smuggling to piracy, suicide attacks to the threat of weapons of mass destruction, the threats are many and varied.
- **Vulnerability:** The maritime transportation system annually accommodates 6.5 million cruise ship passengers, 51,000 port calls by over 7,500 foreign ships, at more than 360 commercial ports spread out over 95,000 miles of coastline. The vastness of this system and its widespread and diverse critical infrastructure leave the Nation vulnerable to terrorist acts within our ports, waterways, and coastal zones, as well as exploitation of maritime commerce as a means of transporting terrorists and their weapons.
- **Consequence:** Contributing nearly $750 billion to the U.S. gross domestic product annually and handling 95 percent of all overseas trade each year—the value of the U.S. maritime domain and the consequence of any significant attack cannot be overstated. Independent analysis and the experiences of 9/11 and the West Coast dock workers strike demonstrates an economic impact of a forced closure of U.S. ports for a period of only 8 days to have been in excess of $58 billion to the U.S. economy.

Lingering and new maritime safety and security gaps continually present themselves and it is these risks we will continually work to reduce. The Coast Guard guides its efforts by implementing policies, seeking resources, and deploying capabilities through the lens of our maritime security strategy.

Implement the Maritime Strategy for Homeland Security

Considering the vast economic utility of our ports, waterways, and coastal approaches, it is clear that a terrorist incident against our marine transportation system would have a disastrous impact on global shipping, international trade, and the world economy, in addition to the strategic military value of many ports and waterways.

The elements of the Coast Guard's *Maritime Strategy for Homeland Security* are in direct alignment with the DHS' strategic goals of Awareness, Prevention, Protection, Response and Recovery. These elements serve as guiding pillars in our efforts to reduce America's vulnerabilities to terrorism by enhancing our ability to prevent terrorist attacks and limit the damage to our Nation's ports, coastal infrastructure and population centers in the event a terrorist attack occurs. A brief overview of the core elements of that strategy with particular emphasis on creation and management of a robust security regime is presented here in the following paragraphs.

Enhance Maritime Domain Awareness (MDA)

First, we seek to increase our awareness and knowledge of what is happening in the maritime arena, not just here in American waters, but globally. We need to

know which vessels are in operation, the names of the crews and passengers, and the ship's cargo, especially those inbound for U.S. ports. Maritime Domain Awareness (MDA) is critical to separate the law-abiding sailor from the anomalous threat.

The core of our MDA efforts revolve around the development and employment of accurate information, intelligence, and targeting of vessels, cargo, crews and passengers—and extending this well beyond our traditional maritime boundaries. All DHS components are working to provide a layered defense through collaborative efforts with our interagency and international partners to counter and manage security risks long before they reach a U.S. port. There are two hallmarks to today's security environment; complexity and ambiguity. Improving MDA will help us to simplify the complex and clarify the ambiguous and prove invaluable to facilitating effective resource, operational, and policy decision-making.

Create and Oversee Maritime Security Regime

Second, to help prevent terrorist attacks we have developed and continue to improve an effective maritime security regime—both domestically and internationally. This element of our strategy focuses on our domestic and international efforts and includes initiatives related to MTSA enforcement, International Maritime Organization regulations such as the ISPS Code, as well as improving supply chain security and identity security processes.

Before 9/11 we had no formal international or domestic maritime security regime for ports, port facilities, and ships—with the exception of cruise ships. Partnering with domestic and international stakeholders, we now have both a comprehensive domestic security regime and an international security convention in place. Both have been in force since July 1, 2004. In executing the requirements of the Maritime Transportation Security Act (MTSA) and the International Ship and Port Facility Security (ISPS) code, the Coast Guard has:

- Reviewed and approved over 9,600 domestic vessel security plans and 3,100 domestic facility security plans;
- Overseen the development of 43 Area Maritime Security Plans and Committees;
- Verified security plan implementation on 8,100 foreign vessels;
- Completed all domestic port security assessments for the 55 militarily and economically strategic ports;
- Visited 22 foreign countries to assess the effectiveness of anti-terrorism measures and implementation of ISPS code requirements. An additional 10 countries are scheduled for visits by June 2005 with the goal of visiting all of our approximately 140 maritime trading partners; and
- Oversaw the continuing development of the National Maritime Security Plan.

Aside from the statistics, MTSA and ISPS are truly landmark achievements within the maritime industry. Through a variety of measures, or layers, of regulatory requirements, these two regimes complement each other and have gone far to reduce vulnerabilities within the global maritime transportation system, the general framework of which includes:

- **Physical Security:** The first pillar of this framework is physical security. Through the implementation of the MTSA, we have significantly hardened the physical security of our ports. Roughly 3,100 of the Nation's highest risk port facilities have implemented mandatory access control measures to ensure that only authorized persons are able to gain access. They have established designated restricted areas within the facility gates and facility owners and operators are now required, under federal regulations, to implement screening protocols for ensuring that cargo-transport vehicles and persons entering the facilities are inspected to deter the unauthorized introduction of dangerous substances and devices. At the facility gates, containers are required to be checked for evidence of tampering and cargo seals are checked.
- **Identity Security:** Identity verification is the second critical element of port security, recognizing that we must know and trust those who are provided unescorted access to our port facilities and vessels. The 9/11 Commission report noted that the September 11th hijackers obtained and used government-issued identification cards such as driver's licenses. The Commission recommended that forms of identification be made more secure. Congress partially addressed this issue in the Maritime Transportation Security Act of 2002 with the requirement for the Transportation Workers Identification Card or TWIC. However, merchant mariner documents are, by statute, identification documents, yet they contain virtually no security features. This, among other reasons, is why the Commandant, the Secretary of Homeland Security and the President have pro-

posed a complete update of the merchant mariner credentialing statutes. We cannot, and must not, continue with business as usual in the area of mariner credentialing. The specter of a terrorist obtaining and using a merchant mariner credential to access and attack vital areas of a strategic port is one that is very real. The changes we have proposed will enable the Department to heighten the security of all mariner credentials in partnership with the mariners themselves and the maritime industry.

The Coast Guard is also working very closely with the Transportation Security Administration (TSA), the lead for implementation of the Transportation Worker Identification Card (TWIC), to assist in the implementation of this new credentialing program. Just over six months ago, TSA approached the Coast Guard and asked for assistance in implementing the TWIC in the maritime mode through a regulatory project. The Coast Guard is fully supportive of this regulatory effort and will do everything within our ability to assist TSA in the development of this rulemaking.

- **Cargo Security:** Cargo security encompasses the process of ensuring that all cargo bound for the U.S. is legitimate and was properly supervised from the point of origin, through its sea transit, and during its arrival at the final destination in the U.S.

  Since Customs and Border Protection (CBP) has the lead role in maritime cargo security, the Coast Guard has worked in concert with our sister agency to align respective agency roles and responsibilities regarding international trade. When a cargo is moved on the waterborne leg of the trade route, the Coast Guard has oversight of the cargo's care and carriage on the vessels and within the port facility. The Coast Guard also oversees the training and identity verification of the people who are moving the cargo. CBP has authority over the cargo contents and container standards. Using the information provided through the Coast Guard's 96-hour notice of arrival rule and CBP's 24-hour cargo loading rule, we can act to control vessels, and thus their cargoes, that pose an unacceptable risk to our ports. With Coast Guard officers posted at CBP's National Targeting Center, we continuously improve agency coordination and our collective ability to quickly take appropriate action when notified of a cargo of interest. As a further improvement, the trade community can file required passenger and crew information via an electronic notice of arrival and departure system. This streamlines the process for industry and improves our ability to apply targeting and selectivity methods.

  The Coast Guard has worked hard to align all of our regulatory and policy development efforts with CBP. We meet regularly to discuss policy, we participate on inter-agency regulation development teams, and we sit on the Operation Safe Commerce Executive Steering Committee. Between DHS, CBP, and the Coast Guard, we coordinate the work of our various Federal Advisory Committees so that we all understand the trade community's concerns and priorities. Now that MTSA and the ISPS Code are fully implemented, we are monitoring compliance and carefully noting issues for future improvements to the regulatory framework.

  Looking at specific cargo-related initiatives, the Coast Guard fully supports the Container Security Initiative and the Customs-Trade Partnership Against Terrorism. We look forward to the results of Operation Safe Commerce, which will highlight technologies and business practices that will bring improved, layered security throughout the supply chain. We also agree with CBP's view that international compliance and the establishment of international standards are needed to help gain global compliance. In this way, the International Standards Organization and the International Maritime Organization have achieved great success in institutionalizing both safety and security standards, many times incorporating industry standards by reference. A multilateral approach provides a more efficient and effective security regime. Compliance with a common, acceptable standard is checked by all our trading partners, not just the U.S. The evidence of success can be directly measured in the level of compliance. A prime example is the success of the ISPS Code implementation evidenced by the 98 percent compliance rate achieved by foreign vessels arriving in U.S. ports.

- **Culture of Security:** Finally, and perhaps most importantly we have been able to take important steps to instill a culture of security within a system previously focused almost exclusively on efficiency. Reducing the vulnerabilities of our vessels and ports required a cultural shift to put security at the top of the agenda rather than as an afterthought. It is centered on the people who must implement the new security measures. Under our MTSA regulations, facilities

and vessels are required to designate individuals with security responsibilities, including company security officers, facility security officers, and vessel security officers. These individuals must have knowledge, thorough training and equivalent job experience. They must be familiar with, and responsible for, implementation of the specific security measures outlined in their facility/vessel security plans and they must be knowledgeable in emergency preparedness, the conduct of security audits, and security exercises. In addition, facility security officers must have training in security assessment methodologies; current security threats and patterns; recognizing and detecting dangerous substances and devices, recognizing characteristics and behavioral patterns of persons who are likely to threaten security; and techniques used to circumvent security measures.

Increase Operational Presence. Third, we seek to better protect critical maritime infrastructure and improve our ability to respond to suspect activities by increasing our operational presence in ports, coastal zones and beyond,—to implement a layered security posture, a defense-in-depth. Our collective efforts to increase operational presence in ports and coastal zones focus not only on adding more people, boats and ships to our force structures, but making the employment of those resources more effective through the application of technology, information sharing, and intelligence support.

Improve Response and Recovery Posture. Finally, we are improving our ability to respond to and aid in recovery if there were an actual terrorist attack. Understanding the challenge of defending 26,000 miles of navigable waterways and 361 ports against every conceivable threat at every possible time, we are also aggressively working to improve our response capabilities and readiness. While many of the increases in MDA and operational presence augment our collective response and recovery posture, we must also incorporate initiatives that will increase our ability to adequately manage operations and coordinate resources during maritime threat response or recovery operations.

The Coast Guard is implementing the new National Response Plan across all operations. The Incident Command System is our mandated crisis management system, and we have years of practical experience in its use. At the local level, each port is ready with port-specific and even sub-area specific, response plans. All law enforcement agencies, public service providers, and port stakeholders have participated in the plan development process.

The Coast Guard has confidence that if a maritime transportation security incident (TSI) should occur in one of our ports, the local responders (Coast Guard Sector Commander or Captain of the Port, other federal agencies, state and local authorities, and partners in industry) will immediately react with mitigation, response, and recovery activities in that port and region. At the same time, we are continuing to refine tools and analysis to aid senior leadership in their ability to rapidly respond to a crisis, minimize damage, and aid in recovery operations.

Conclusion

After experiencing the most horrific act of terrorism on U.S. soil on 9/11, all sectors of the maritime community rallied together to strengthen the security of the maritime transportation system. The tremendous successes in this endeavor is due, in large part, to the cooperation and prompt measures taken by government and industry working together as partners. Much work remains to be done to reduce America's vulnerabilities to terrorism and other maritime security threats but with the continued support of the Congress and Administration, I know that we will succeed in delivering the robust maritime safety and security America expects and deserves well into the 21st Century.

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

The CHAIRMAN. Thank you.

Mr. Skinner?

STATEMENT OF RICHARD L. SKINNER, ACTING INSPECTOR GENERAL, DEPARTMENT OF HOMELAND SECURITY

Mr. SKINNER. Thank you. Mr. Chairman, Mr. Co-Chairman, Members of the Committee, thank you for the opportunity to be here today.

I would like to summarize three issues from my prepared statement that I have submitted for the record. One, the Department's effort to detect radioactive material in cargo security; challenges facing the Coast Guard; and the Department's Port Security Grant Program.

Concerning the detection of radioactive materials, as this Committee knows, ABC News reported that twice it successfully smuggled depleted uranium into the country. The depleted uranium arrived in ocean-going cargo containers that were shipped from Indonesia and Turkey. In both cases, the containers were targeted as high risk for additional screening, but, nonetheless, were allowed entry without detection.

In September of 2004, we issued a classified report. We cited several weaknesses that allowed this to happen. The Department has since enhanced its ability to screen targeted containers for radioactive emissions by deploying more sensitive technology at its seaports, revising protocols and procedures, and improving the training of its personnel.

At the request of four congressional committees, we initiated a follow-up audit to determine whether the Department had implemented our recommendations and to examine other technologies that could increase the Department's radiation-detection capability.

Concerning Coast Guard challenges, in September 2004 we reported that the Coast Guard's willingness to work hard and long hours, use innovative tactics, and work closely with other departmental components allowed it to achieve its mission-performance goals. However, to sustain its mission performance, the Coast Guard faces significant barriers; most importantly, the deteriorating readiness of its fleet vessels.

The workload demands of the Coast Guard will only continue to increase as it implements the Maritime Transportation Security Act, MTSA. It must conduct risk assessments of all vessels and facilities on or near the water, develop national and area maritime transportation security plans, and improve port facility and vessel security plans. In addition, growing homeland security demands, such as added port and coastal security patrols, increase the Coast Guard's operating tempo. The Coast Guard reported that mission sustainment is at risk due to the cutters and aircraft that are aging, obsolete, and require replacement. Currently, the Coast Guard has experienced serious cracking in the hulls of its 110-foot cutters and the engine power loss on its HH–65 Dolphin helicopters. These problems adversely affect the Coast Guard's mission readiness and, ultimately, mission performance.

Finally, concerning Port Security Grants, today the Transportation Security Administration, the U.S. Coast Guard, and the Department of Transportation's Maritime Administration have collaborated to award over $560 million for over 1,200 projects. This does not include, however, the most recent round of grants, totaling $141 million, which the Department announced this past week.

In January of this year, we reported on several important issues relating to strategic direction, priority-setting, and general administration of the program.

First, the program's strategic effectiveness is hindered because it is attempting to reconcile three competing requirements or ap-

proaches: the competitive program mandated by Congress through its appropriations, MTSA's grant authority, which was not funded through appropriations, and risk-based decision-making. These competitive approaches were clouding the direction of the program.

Second, the program did not have the benefit of critical infrastructure-protection information now being developed by the Department's Information Analysis and Infrastructure Protection Directorate. Consequently, Port Security Grants were awarded without basic data about our national port-security priorities.

Third, grant award decisions were made with the intent of expending all available funding and spreading funds to as many applicants as possible. The Department funded projects despite dubious scores by its evaluators, raising questions about the merits of many of the projects. It appeared that headquarters and field reviewers did not always share a common understanding of program objectives or eligibility criteria. In addition, the program transferred 82 projects that were not funded, valued at $75 million, to the Department's Urban Area Security Initiative, despite previously determining that those projects did not merit funding.

Another dilemma for the program related to the circumstances under which private entities might obtain grant funding. DHS did not have a formal policy to govern financial assistance to private entities, including those that own and operate high-risk port facilities. Some of the grants to private companies were within their financial means, and many were for basic security measures that should have been considered as normal cost of doing business.

Furthermore, grant recipients had spent only a small portion of their awards. Of the $515 million awarded between June 2002 and December 2003, including the $75 million provided under the Department's Urban Area Security Initiative, grant recipients had expended only $107 million, or 21 percent of their awards, as of September 30th, 2004. We determined that many of the recipients were simply not prepared to put their grant funds to use. Furthermore, we determined that the Department did not have sufficient resources to monitor the progress, or lack thereof, of individual projects.

The Department generally agreed with our recommendations to improve the design, management, and oversight of the program. The Department advised us that it intended to use a new risk-based formula to award the $150 million budgeted for Port Security Grants during 2005.

We are now studying how the Department has modified the program, particularly the criteria that it would use to make grant award decisions and whether those modifications satisfy our recommendations.

Mr. Chairman, Mr. Co-Chairman, Members, this concludes my remarks. I'll be happy to answer any questions you may have.

[The prepared statement of Mr. Skinner follows:]

PREPARED STATEMENT OF RICHARD L. SKINNER, ACTING INSPECTOR GENERAL, DEPARTMENT OF HOMELAND SECURITY

Mr. Chairman, Mr. Co-Chairman and Members of the Committee:

Thank you for the opportunity to be here today to discuss the work of the Office of Inspector General (OIG) regarding port and maritime security. I would like to address three areas related to security: preventing terrorist weapons from entering the

United States, maritime security challenges facing the U.S. Coast Guard (USCG), and the Port Security Grant Program. These areas involve major components of the Department of Homeland Security (DHS) and its wide-ranging operations. Each has been the subject of oversight by the OIG and my comments are drawn from our reports, which are available on the OIG website at www.dhs.gov/oig.

Preventing Terrorist Weapons From Entering the United States

Since September 11, 2001, the Department of Homeland Security's Bureau of Customs and Border Protection's (CBP) priority mission is detecting and preventing terrorists and terrorist weapons from entering the United States. A major component of its priority mission is to ensure that oceangoing cargo containers arriving at the seaports of entry are not used to smuggle illegal and dangerous contraband. To test controls over importing weapons of mass destruction, ABC News was successful in two attempts at smuggling depleted uranium into the country. On September 11, 2002, ABC News reported that a 15-pound cylinder of depleted uranium was shipped from Europe to the U.S. undetected by CBP. On September 11, 2003, ABC News reported that the same cylinder was smuggled to the U.S. from Jakarta, Indonesia, again undetected.

In the first smuggling event, ABC News reported that a steel pipe containing a 15-pound cylinder of depleted uranium, which was shielded with lead, was placed in a suitcase and accompanied by ABC News reporters by rail from Austria to Turkey. In Istanbul, Turkey, the suitcase was placed inside an ornamental chest that was crated and nailed shut. The crate containing the suitcase was then placed alongside crates of huge vases and Turkish horse carts in a large metal shipping container, and then loaded onto a ship that left Istanbul. Based on data contained in the Automated Targeting System, the crate was targeted as high-risk for screening by the U.S. Customs Service (Customs). ABC News broadcast on September 11, 2002, that Customs failed to detect the depleted uranium carried from Europe to the United States.

During the second smuggling event, ABC News placed the same cylinder of depleted uranium into a suitcase, and then placed the suitcase into a teak trunk. The trunk, along with other furniture, was loaded into a container in Jakarta, Indonesia, and then transshipped to the U.S. from Tanjung Pelepas, Malaysia. This shipment was also targeted as high-risk for screening and subsequently inspected by CBP personnel, but was then allowed to proceed from the port by truck.

In a classified September 2004 report, *Effectiveness of Customs and Border Protection's Procedures to Detect Uranium in Two Smuggling Incidents*, we cited several weaknesses that occurred at the time of the two incidents that made the container inspection process ineffective. The protocols and procedures that CBP personnel followed at the time of the two smuggling incidents were not adequate to detect the depleted uranium. CBP has since enhanced its ability to screen targeted containers for radioactive emissions by deploying more sensitive technology at its seaports, revising protocols and procedures, and improving training of CBP personnel.

At the request of four congressional committees, we recently initiated a follow-up audit to determine the status of CBP's implementation of the recommendations made in our September 2004 report. In addition, we will review other relevant technologies and implementation plans recommended by entities associated with CBP's efforts to increase the detection capability of the radiation portal monitors that are deployed domestically and internationally.

Maritime Security

The Coast Guard's willingness to work hard and long hours, use innovative tactics, and work through partnerships in close inter-agency cooperation has allowed it to achieve mission performance results goals. However, to improve and sustain its mission performance in the future, the Coast Guard faces significant barriers, most importantly the deteriorating readiness of its fleet assets. The Coast Guard faces three major barriers to improving and sustaining its readiness to perform its legacy missions:

1. The lack of a comprehensive and fully defined performance management system impedes the Coast Guard's ability to gauge its performance, allocate resources effectively, and target areas for improved performance.

2. The workload demands on the Coast Guard will continue to increase as it implements the Maritime Transportation Security Act of 2002 (MTSA). This complex work requires experienced and trained personnel; however, the Coast Guard has in recent years suffered from declining experience levels among its personnel.

3. Sustaining a high operating tempo due to growing homeland security demands, such as added port, waterway, and coastal security patrols, will tax the Coast Guard's infrastructure including its aging cutter and aircraft fleet.

The lack of a comprehensive and fully defined performance management system impedes the Coast Guard's ability to gauge its performance, allocate resources effectively, and target areas for improved performance. The Coast Guard has yet to define a performance management system that includes all the input, output, and outcomes needed to gauge results and target performance improvements, balance its missions, and ensure the capacity and readiness to respond to future crises or major terrorist attacks. For example, for search and rescue, the number of mariners in distress saved is a good indicator of outcome; however, resource hours under-represent the effort put into this mission by omitting the many hours of watch standing at stations. Without more complete information, the Coast Guard has limited ability to identify and target cost effective improvements to mission performance.

The workload demands on the Coast Guard will continue to increase as it implements the MSTA. Under MTSA, the Coast Guard must conduct risk assessments of all vessels and facilities on or near the water; develop national and area maritime transportation security plans; and approve port, facility, and vessel security plans. This complex work requires experienced and trained personnel, presenting a major challenge for the Coast Guard, which has in recent years suffered from declining experience levels among its personnel. Since the Coast Guard largely relies on experienced senior personnel to coach and train junior personnel and new recruits on the job, mission performance is at risk.

In addition to implementing MTSA, growing homeland security demands, such as added port, waterway, and coastal security patrols, result in a continued high operating tempo. Sustaining this high operating tempo will be a major challenge for Coast Guard personnel and will tax its infrastructure, especially its aged cutter and aircraft fleet. The Coast Guard reported that mission sustainment is at risk due to cutters and aircraft that are aging, technologically obsolete, and require replacement and modernization. Currently, the Coast Guard is experiencing serious cracking in the hulls of the 110 foot cutters and engine power loss on the HH–65 Dolphin helicopters, resulting in operating restrictions. These problems adversely affect the Coast Guard's mission readiness and ultimately mission performance.

The Port Security Grant Program

The Department's Port Security Grant Program is designed to reduce the vulnerability of American ports to potential terrorist attacks by enhancing facility and operational security. The Transportation Security Administration, the U.S. Coast Guard, and the Department of Transportation's Maritime Administration have collaborated to award over $560 million for over 1,200 projects. My office reviewed the design and goals of the program, the roles and responsibilities of participating agencies, and the grant evaluation and selection process. The bulk of our analysis focused on grant award decisions in rounds two and three. The results of our review are discussed in our January 28, 2005 final report, *Review of the Port Security Grant Program (#OIG–05–10).* We identified several important issues relating to the strategic direction of the program, the program's support of national infrastructure protection priorities, and the general administration of the program. I would like to briefly talk about those results.

First, the program's strategic effectiveness is hindered mainly because it is attempting to reconcile three competing approaches: the competitive program mandated by Congress, MTSA's grant authority, and risk-based decision making. These competing approaches are clouding the direction of the program. The program is under pressure to help defray the costs of the MTSA security mandates that broadly affect the maritime industry. MTSA included a grant authority intended to equitably distribute funds for this purpose, but the appropriations legislation did not fund the MTSA port security grant program and required a competitive grant program focused on securing national critical seaports. However, the resulting program must base award decisions on the universe of applications submitted—which may or may not include the most critical needs. In addition, the evaluation and selection process emphasized awarding funds to as many applicants as possible. Hence, the program attempted to balance the competitive program that objectively evaluates the quality of the applications with the need to broadly disperse funds to assist with MTSA compliance, while at the same time incorporating risk-based eligibility criteria and evaluation tools to prioritize projects.

Second, the program did not have the benefit of national key asset and critical infrastructure protection information now being developed by the Information Analysis and Infrastructure Protection (IAIP) directorate. Program administrators and IAIP, which is responsible for developing strategies for protecting the Nation's crit-

ical infrastructure, did not collaborate to integrate the program with broader national security initiatives. Thus, port security grant award decisions were made without sufficient information about our national priorities.

Third, grant award decisions were made with the intent of expending all available funding and spreading funds to as many applicants as possible. The program funded projects despite dubious scores by its evaluators against key criteria, raising questions about the merits of 258 projects costing $67 million. It appeared that headquarters and field reviewers did not share a common understanding of program objectives or eligibility criteria. Frequently, they did not agree about the eligibility or merit of projects and did not consistently document their rationale for recommending or not recommending funding. We pointed out the need for the program to look more closely at the first three criteria (whether the grant proposal was in an area of high risk, addressed a critical security need/vulnerability, and provided high risk reduction), which were well conceived and should have carried more weight.

In addition, the program forwarded an additional 82 projects to the Office of Domestic Preparedness to be funded at a cost of $75 million under the Urban Area Security Initiative, despite previously determining that these projects did not merit funding.

Another dilemma for the program is the question of where the private sector's responsibility for preventing terrorism ends and where the Federal Government's responsibility begins. At the time of our report, DHS did not have a formal policy to provide financial assistance to private entities, a group that includes those that own and operate high risk facilities. Even though private entities have applied for and received substantial funding, we did not conclude that the program should limit funding to the private sector per se. However, some of the grants to private companies were within the financial reach of the applicants and many were for basic security measures that should have been considered normal costs of doing business. For example, some of the projects were for anti-theft purposes and not related to terrorist attack prevention or deterrence.

Furthermore, after three rounds, recipients spent only a small portion of the entire amount awarded. Of the $515 million awarded between June 2002 and December 2003, including $75 million provided under the Office for Domestic Preparedness' Urban Area Security Initiative, grant recipients had expended only $106.9 million, or 21 percent of total program awards as of September 30, 2004. As a result, the majority of projects had not been completed and the program had not yet achieved its intended results in the form of actual improvements to port security.

This brings us to the status of our recommendations. In response to our draft report, DHS concurred with 11 of our 12 recommendations. In our final report, we strongly encouraged DHS to fully implement our recommendations before proceeding with the next round of port security grants. DHS' Office of State and Local Government Coordination and Preparedness (SLGCP) received $150 million in the FY 2005 budget for round five of the Port Security Grant Program. SLGCP officials informed us that they were going to make substantive changes to the design of the program to make it more risk-based, and while it appears they have, we have not evaluated the effect of these changes.

We recently received DHS' action plan, which discusses corrective actions taken and planned in response to our recommendations. The action plan generally appears to be responsive to our recommendations. For example:

- We identified numerous projects within ports not on the list of strategic or controlled ports. The program developed and implemented a funding distribution model that targeted 66 ports as eligible under the program.
- We noted the lack of a policy for funding private sector projects. The action plan refers to a decision by the Secretary that private entities may apply for a grant, but must provide matching funds of 50 percent.
- Program administrators did not collaborate with IAIP on broader national security initiatives. SLGCP is taking steps to improve information sharing with, and participation of, IAIP in the selection and evaluation process.

However, we are also reviewing additional information supporting the action plan. In addition, we have not had the opportunity to review guidance that will be issued for those SLGCP, USCG, TSA, CBP, IAIP, and MARAD personnel who will be evaluating projects. The revised grant application package was just released this past week. We are studying how DHS has modified the program—particularly the criteria program administrators will use and how they will apply it during the evaluation process—and whether those modifications satisfy our recommendations. We expect to communicate this information to SLGCP in the near future.

Mr. Chairman, Mr. Co-Chairman, this concludes my prepared statement. I will be pleased to answer any questions you or the Members may have.

The CHAIRMAN. Thank you very much, Mr. Skinner.

Ms. Wrightson? Now, I know that you have some charts you wish to put up. What are those?

Ms. WRIGHTSON. Actually, I—we prepared the charts so that my remarks can be as short as possible so that we can leave time for dialogue, so, while they're putting them up, I'm just going to go ahead and start.

The CHAIRMAN. Well, tell us. I can't read them. I don't know about the rest of——

Ms. WRIGHTSON. Oh, goodness. They are about as big as we thought we could get in the car.

The CHAIRMAN. They are all in your testimony?

Ms. WRIGHTSON. Yes, they are.

The CHAIRMAN. Yes, I think you can take them down, then. Thank you very much.

[Laughter.]

Ms. WRIGHTSON. OK.

The CHAIRMAN. Thank you very much.

I am pleased to have your statement and understand your study.

STATEMENT OF MARGARET T. WRIGHTSON, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. WRIGHTSON. Good morning, Mr. Chairman, Senator Inouye, and other distinguished Members.

I'm pleased to be here today to discuss the Nation's efforts to improve maritime and seaport security.

Since the terrorist attack of September 11th, GAO has responded to numerous requests for reports and testimonies on this issue. In fact, in the past few years we've issued more than 20 products, all of which contained recommendations.

My statement today covers a wide range of that work, but, in the interest of time, I'm going to highlight only our major findings and conclusions.

First, since September 11th, the Federal Government and port stakeholders have taken extensive actions to improve port security. Together, these actions have helped to improve security in three ways: identifying and reducing vulnerabilities of potential targets, helping to secure the flow of containers to port gateways, and improving maritime domain awareness so that stakeholders have an informed view of port activities through intelligence, information sharing, and new technologies to identify and respond to threats.

Second, while it may have been necessary to move quickly at the outset, attempting so much so fast has resulted in a range of problems that should be corrected, and soon. These problems can be grouped into three main categories: concerns about faulty program design and implementation, concerns about inadequate coordination, and concerns about maintaining the financial support needed to continue implementing the security enhancements.

Last, as it becomes clear that the price of improved port security will be measured in billions, we must develop better mechanisms for assessing progress and assuring that resources are focused on

the most important priorities. Approaching 4 years after the terrorist attacks, performance measures to define outcomes and measure progress have not been implemented, nor is there a robust framework for systematically managing risk. A sustainable strategy for maritime security requires both.

Turning to our detailed findings, given the scope and complexity of the programs, and the speed with which they were rolled out, it is not surprising that we have found a host of problems. While some of these may be resolved with time as the programs mature, others are more challenging.

The first challenge is the failure of many of these programs to incorporate necessary planning. For example, our review showed that TWIC, C–TPAT, CSI, Megaport, AIS, and the Port Security Assessment and Compliance Program all experienced major planning problems, ranging from inadequate or nonexistent human capital, projects, or strategic planning, to faulty project management, such as a lack of clear timeframes, milestones, and risk mitigation. Until such planning elements are incorporated, there will be too little assurance that program results will be delivered on time and on target.

Inadequate coordination is the second area to highlight. Unfortunately, the list of programs with coordination problems is as long as the list for planning problems, yet establishing a viable port-security regime cannot be accomplished with agencies at the federal level that are working in stovepipes or by the Federal Government alone as Congressman Ruppersberger ably stated earlier.

There is perhaps no better way to highlight what can happen when coordination breaks down than the delayed attempt to develop the Transportation Worker Identification Credential.

TSA began TWIC in 2002, while it was part of DOT. At that time, TSA said the first cards would be issued in 2004. We are now nearly halfway through 2005, and TWIC is still in the prototype phase, with critical policy decisions still to be made that are as basic as who will be eligible to receive the card.

Part of TSA's problems can be traced to breakdowns in coordination between TSA and DHS. Moreover, outside DHS, TSA has failed to sustain the support of port stakeholders who feel excluded. Without internal and external support and agreement, and, I might add, a comprehensive plan for managing this program, which does not now appear to be in place, the program is at risk of further delays, increased costs, and less-than-satisfactory outcomes.

Before concluding, two additional matters are worth mentioning. First, notwithstanding the effort and resources represented by these programs and the people at this table, it is difficult, if not impossible, to know how far we have progressed in making ports more secure.

One reason is a lack of overall goals and measures. For example, although the Coast Guard regularly reports how well it is doing rescuing mariners in distress, it is still struggling to develop and implement a performance measure for port-security activities.

Second, we cannot afford to protect everything against every risk. More care must be taken to prioritize resources toward the greatest risk.

Notwithstanding some progress, much remains to be done before a common framework for risk management is systematically applied to policy and resource allocation decisions in DHS, let alone the Federal Government.

In conclusion, urgency in the wake of 9/11 may help to rationalize the mistakes and missteps described today; however, the need for quick action at the start should not be used to justify poor planning and management today. In the final analysis, the race to better security must be run as a marathon, not a sprint. In port security, as in homeland security, we're ready for midcourse corrections, including, we hope, the expeditious implementation of GAO's recommendations and a closer focus on goals, measures, and risk management. This is because lasting success depends less well on how quickly the programs were begun than on how carefully they are carried out.

Mr. Chairman, that concludes my statement. I hope we engage in a dialogue about these really important issues.

[The prepared statement of Ms. Wrightson follows:]

PREPARED STATEMENT OF MARGARET T. WRIGHTSON, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss the Nation's efforts to improve seaport security. More than 3 years after the terrorist attacks of September 11, 2001, seaport security continues to be a major concern for the Nation. For example, many seaport areas are inherently vulnerable, given their size, easy accessibility by water and land, large numbers of potential targets, and proximity to urban areas. Also, the large cargo volumes passing through seaports, such as containers destined for further shipment by other modes of transportation such as rail or truck, also represent a potential conduit for terrorists to smuggle weapons of mass destruction or other dangerous materials into the United States. The potential consequences of the risks created by these vulnerabilities are significant as the Nation's economy relies on an expeditious flow of goods through seaports. A successful attack on a seaport could result in a dramatic slowdown in the supply system, with consequences in the billions of dollars.

Much has been set in motion to address these risks in the wake of the September 11, 2001, terrorist attacks. Both Congress and the Administration have been active, through legislation, presidential directives, and international agreements, in enhancing seaport security. Key agencies, such as the Coast Guard, the Customs Service, and the Transportation Security Administration (TSA), have been reorganized under the new Department of Homeland Security (DHS) and tasked with numerous responsibilities designed to strengthen seaport security. Many of these tasks were required by the Maritime Transportation Security Act of 2002 (MTSA).[1]

My testimony today draws primarily on the work we have done in responding to congressional requests for information and analysis about the Nation's homeland security efforts (see app. I for a list of recent reports and testimonies we have issued). We conducted our work in accordance with generally accepted government auditing standards, and the scope and methodology for this work can be found in the respective products. Over the course of completing this work, we have made a number of recommendations for specific agencies, which can be found in appendix II. While this body of work does not cover every program or action that has been taken, it does encompass a wide range of these actions. My testimony will (1) provide an overview of the types of actions taken by the Federal Government and other stakeholders to address seaport security, (2) describe the main challenges encountered in taking these actions, and (3) describe what tools and approaches may be useful in charting a course for future actions to enhance security.

Summary

Seaports are vulnerable on many fronts and the actions taken to secure them can be divided into three main categories: reducing vulnerabilities of specific targets within seaports, making the cargo flowing through these seaport gateways more secure, and developing what is called "maritime domain awareness"—a sufficiently in-

formed view of maritime activities by stakeholders involved in security to quickly identify and respond to emergencies, unusual patterns or events, and matters of particular interest. Within each category, several actions have been taken or are underway. For example, assessments of potential targets have been completed at 55 of the Nation's most economically and militarily strategic seaports, and more than 9,000 vessels and over 3,000 facilities have developed security plans and have been reviewed by the Coast Guard. Customs inspectors have been placed at some overseas seaports and partnerships struck up with some private sector stakeholders to help ensure that the cargo and containers arriving at U.S. seaports are free of weapons of mass destruction (WMD) or a radiological "dirty bomb." New assets are budgeted and are coming online, including new Coast Guard boats and cutters and communication systems. Finally, new information-sharing networks and command structures have been created to allow more coordinated responses and increase awareness of activities going on in the maritime domain. Some of these efforts have been completed and others are ongoing; overall, the amount of effort has been considerable.

The efforts we have reviewed over the past 3 years, many of which were quickly implemented to address pressing security needs, have encountered challenges that could significantly affect their success. Some of these challenges are likely to be resolved with time, but some reflect greater difficulty and therefore merit more attention. The more complex challenges take three main forms:

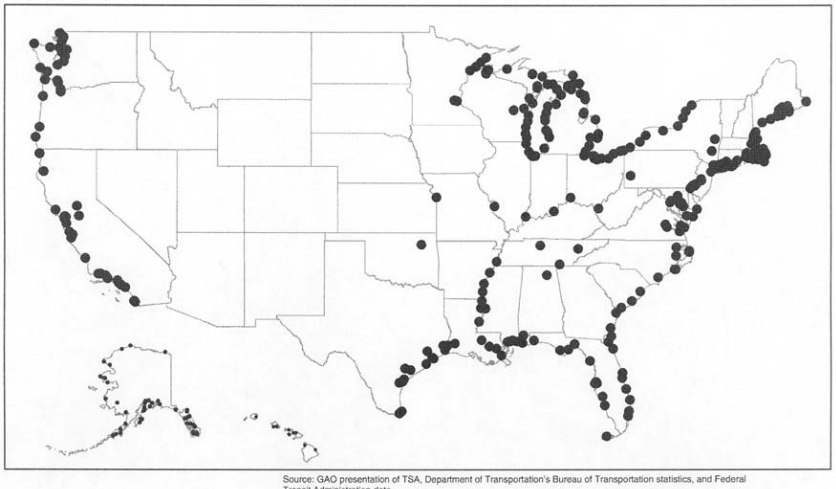
- Program design and implementation: Some agencies have failed to design programs and planning components, such as human capital plans and performance measures, that are necessary to successfully implement their programs and ensure they are effective. For example, U.S. Customs and Border Protection (CBP) started implementation of two key container supply-chain-security initiatives before taking adequate steps to develop plans and strategies to effectively manage critical aspects of the programs such as human capital and achievement of program objectives.
- Coordinating security efforts with stakeholders: Many private sector companies and governmental agencies are involved in seaport security efforts, and in some cases progress has been hampered because of difficulties in communication and coordination between parties. For example, deadlines in the development of an identification card for transportation workers have been missed due in part to a lack of communication and coordination between TSA and DHS.
- Funding security improvements: Economic constraints, such as declining revenues and increased security costs, make it difficult to provide and sustain the funding necessary to continue implementing security measures and activities by maritime stakeholders including the Federal Government. Consequently, many stakeholders rely heavily on the Federal Government for assistance, and requests for federal grant funding far outstrip the funding amounts available. For example, although more than $560 million in grants has been awarded to seaport stakeholders since 2002 under federal grant programs for implementation of security measures and activities, this amount has met only a fraction of the amount requested by these stakeholders.

As actions to enhance homeland security continue, and as it becomes clearer that the price of these actions will be measured in the billions of dollars, it is likely that increasing attention will turn to assessing the progress made in securing seaports and determine where future actions and funds should be allocated to further enhance security. Although there is widespread agreement that actions taken so far have led to a heightened awareness of the need for security and an enhanced ability to identify and respond to many security threats, assessing the degree of progress in making the Nation more secure is difficult. Thus far, seaport security actions—and homeland security activities in general—lack performance measures to define what these activities are intended to achieve and measure progress toward these goals. As Congress and the Nation continue to evaluate how much security is enough, more attention on defining these goals and measures will likely be needed by stakeholders. Doing so is all the more important because, as groups such as the 9/11 Commission have pointed out, no amount of money can totally insulate seaports from attack by a well-funded and determined enemy. These realities suggest that the future focus in applying resources and efforts also needs to incorporate an approach to identify and manage risk—that is, on assessing critical infrastructure, determining what is most at risk, and applying sound measures designed to make cost-effective use of resources and funding.

Background

The vast U.S. maritime system contains more than 300 seaports and 3,700 cargo and passenger terminals. These seaports dot not only our seacoasts, but also major lakes and rivers (see fig. 1). Much of the Nation's commercial maritime activities, however, are concentrated in about a dozen major seaports, such as Los Angeles/Long Beach, New York/New Jersey, and Houston.

Figure 1: Location of U.S. Seaports



Source: GAO presentation of TSA, Department of Transportation's Bureau of Transportation statistics, and Federal Transit Administration data.

The Nation's seaports are economic engines and a key part of the national defense system. More than 95 percent of the Nation's non-North American foreign trade (and 100 percent of certain commodities, such as foreign oil) arrives by ship. Cargo containers, approximately 7 million of which entered the country in 2002, are central to an efficient transportation network because they can be quickly shifted from ships to trains and trucks and back again. Because of these efficiencies, the U.S. and world economies have become increasingly reliant on cargo containers to transport their goods. With regard to national security, the Departments of Defense and Transportation have designated 17 U.S. seaports as strategic because they are necessary for use in the event of a major military deployment. Thirteen of them are commercial seaports.

While the terrorist attacks of September 11, 2001, did not involve seaports, they called attention to ways in which seaports represent an attractive and vulnerable terrorist target. Various studies have pointed out that significant disruptions could result from a seaport-related attack. For example, the Brookings Institution has estimated that costs associated with U.S. seaport closures resulting from a detonated weapon of mass destruction could amount to $1 trillion. The firm of Booz, Allen, and Hamilton studied the potential cost of discovering an undetonated weapon of mass destruction at a U.S. seaport and placed the cost of a 12-day closure of seaports at approximately $58 billion. An actual closure of seaports along the West Coast occurred for 10 days in 2002 due to a labor dispute. According to one estimate, the cost of this closure to the national economy for the first 5 days was estimated at $4.7 billion and increased exponentially after that.[2] Similarly, if one or more of the 17 strategic U.S. seaports (or the ships carrying military supplies) were successfully attacked, not only could massive civilian casualties be sustained and critical infrastructure lost, but the military could also lose precious cargo and time and be forced to rely heavily on already burdened airlift capabilities.

Many Actions Have Been Taken or Are Underway To Address Seaport Security

Since September 11, 2001, a number of actions have been taken or are underway to address seaport security by a diverse mix of agencies and seaport stakeholders. Federal agencies, such as the Coast Guard, U.S. Customs and Border Protection (CBP), and TSA, have been tasked with responsibilities and functions intended to make seaports more secure, such as monitoring vessel traffic or inspecting cargo and containers, and procuring new assets such as aircraft and cutters to conduct patrols

and respond to threats. In addition to these federal agencies, seaport stakeholders in the private sector and at the state and local levels of government have taken actions to enhance the security of seaports, such as conducting security assessments of infrastructure and vessels operated within the seaports and developing security plans to protect against a terrorist attack. The actions taken by these agencies and stakeholders are primarily aimed at three types of protections: (1) identifying and reducing vulnerabilities of the facilities, infrastructure, and vessels operating in seaports, (2) securing the cargo and commerce flowing through seaports, and (3) developing greater maritime domain awareness through enhanced intelligence, information-sharing capabilities, and assets and technologies.

Identifying and Reducing the Vulnerabilities of Facilities, Infrastructure, and Vessels

Seaports facilitate the freedom of movement and flow of goods, and in doing so they allow people, cargo, and vessels to transit with relative anonymity. While seaports contain terminals and other facilities where goods bound for import or export are unloaded and loaded, or where people board and disembark cruise ships or ferries, seaports also often contain other infrastructure critical to the Nation's economy and defense, such as military installations, chemical factories, powerplants, and refineries. The combination of assets, access, and anonymity makes for potentially attractive targets. The facilities and vessels in seaports can be vulnerable on many fronts. For example, facilities where containers are transferred between ships and railroad cars or trucks must be able to screen vehicles entering the facility and routinely check cargo for evidence of tampering. Chemical factories and other installations where hazardous materials are present must be able to control access to areas containing dangerous goods or hazardous substances. Vessels, ranging from oil tankers and freighters to tugboats and passenger ferries, must be able to restrict access to certain areas on board the vessel, such as the bridge or other control stations critical to the vessel's operation.

Given the wide range of potential targets, an effective security response includes identifying targets, assessing risks to them, and taking steps to reduce or mitigate these risks. An essential step in this process is to conduct a security or vulnerability assessment. This assessment, which is needed both for the seaport as a whole and for individual vessels and facilities, identifies vulnerabilities in physical structures, personnel protection systems, processes, and other areas that may lead to a security breach. For example, this assessment might reveal weaknesses in an organization's security systems or unprotected access points such as a facility's perimeter not being sufficiently lighted or gates not being secured or monitored after hours. After the vulnerabilities are identified, measures can then be identified that will reduce or mitigate the vulnerabilities when installed or implemented.

Most actions to identify and reduce the vulnerabilities within seaports were specifically required by the Maritime Transportation Security Act of 2002 (MTSA). Passage of MTSA was a major step in establishing a security framework for America's seaports. This security framework includes assessment of risks, access controls over personnel and facilities, and development and implementation of security plans, among other activities. Table 1 shows some of the actions that have been taken and programs that are in the process of being implemented to carry out this framework.[3]

Table 1: Examples of Actions Taken and Programs Underway to Identify and Reduce Vulnerabilities

Action or program	Description
Conducting security assessments and developing security plans for facilities and vessels	MTSA and its implementing regulations require designated owners or operators of maritime facilities or vessels to identify vulnerabilities and develop security plans for their facilities or vessels. The plans were reviewed and approved by the Coast Guard. Since July 1, 2004, the Coast Guard has been conducting inspections of these facilities and vessels to ensure the plans have been implemented. The Coast Guard completed inspections of the facilities by December 31, 2004, and is scheduled to complete inspections of the vessels by July 1, 2005.
Conducting security assessments and developing seaport-wide security plans	To meet another MTSA requirement, the Coast Guard led efforts to conduct a seaport-wide security assessment of each of the Nation's seaports and develop a security plan for the seaport zone. In carrying out these efforts, the Coast Guard worked with a wide variety of stakeholders, such as state and local governments, law enforcement, owners and operators of facilities and vessels, and trade and labor organizations.
Development of the Transportation Worker Identification Credential (TWIC)	TWIC is designed to respond to various statutory provisions relating to transportation related worker identification including MTSA, which requires a biometric identification card be issued to individuals requiring unescorted access to secure areas of seaport facilities or vessels. This credential is being designed to be a universally recognized identification card accepted across all modes of the national transportation system, including airports, railroad terminals, and seaports.
Port Security Assessment Program	Separate from MTSA requirements, the Coast Guard established a program after September 11, 2001, to assess vulnerabilities of the Nation's 55 most strategic commercial and military seaports. The program has changed considerably since its inception and now includes a geographic information system (GIS) to help identify and provide up-to-date information on threats and incidents, as well as provide accessible information to help develop security plans.

Source: GAO analysis of Coast Guard and TSA data.

The amount of effort involved in carrying out these actions and implementing these programs has been considerable. For example, after following an aggressive time frame to develop regulations to implement the requirements of MTSA, the Coast Guard reviewed and approved the security plans of the over 3,000 facilities and more than 9,000 vessels that were required to identify their vulnerabilities and take action to reduce them. Six months after July 1, 2004, the date by which the security plans were to be implemented, the Coast Guard reported that it completed on-site inspections of all facilities and thousands of vessels to ensure the plans were being implemented as approved. In addition to its work on the security plans and inspections, the Coast Guard completed security assessments of the Nation's 55 most economically and militarily strategic seaports.

Securing the Cargo Flowing Through Seaports

While the facilities, vessels, and infrastructure within seaports have vulnerabilities to terrorist attack, the cargoes transiting through seaports also have vulnerabilities that terrorists could exploit. Containers are of particular concern because they can be filled overseas at so many different locations and are transported through complex logistics networks before reaching U.S. seaports. From the time the container is loaded for shipping to the time the container arrives at a seaport, the containers must go through several steps that involve many different participants and many points of transfer. Each of these steps in the supply chain presents its own vulnerabilities that terrorists could take advantage of to place a WMD into a

container for shipment to the United States. A report prepared by the National Defense University's Center for Technology and National Security Policy stated that a container is ideally suited to deliver a WMD or a radiological "dirty bomb." While there have been no known incidents yet of containers being used to transport WMDs, criminals have exploited containers for other illegal purposes, such as smuggling weapons, people, and illicit substances. Such activities demonstrate the vulnerability of the freight transportation industry and suggest opportunities for further exploitation of containers by criminals, including terrorist groups.

In general, the actions taken thus far are aimed at identifying, tracking, and scrutinizing the container cargo shipments moving into the country. Most of these actions are being done by CBP, the DHS agency responsible for protecting the Nation's borders and official ports of entry. CBP uses a layered approach that attempts to focus resources on potentially risky cargo containers while allowing other cargo containers to proceed without disrupting commerce. This approach includes the actions and programs shown in table 2. Several of these actions involve a strategy of moving primary reliance for security away from control systems at U.S. seaports of entry and toward improved controls at points of origin and along the way.[4]

Table 2: Examples of Container Security Actions

Action	Description
Automated Targeting System (ATS)	A computer model reviews documentation on all arriving containers and helps select or target containers for additional scrutiny.
Supply Chain Stratified Examination	Supplements ATS by randomly selecting additional containers to be physically examined. The results of the random inspection program are to be compared with the results of ATS inspections to improve targeting.
Container Security Initiative (CSI)	Places staff at designated foreign seaports to work with foreign counterparts to identify and inspect high-risk containers for weapons of mass destruction before they are shipped to the United States.
Customs-Trade Partnership Against Terrorism (C–TPAT)	Cooperative program between CBP and members of the international trade community in which private companies agree to improve the security of their supply chains in return for a reduced likelihood that their containers will be inspected.
Operation Safe Commerce	Begun by the private sector and now administered by DHS's Office of Domestic Preparedness, efforts center on (1) ensuring that containers are loaded in a secure environment at the point of product origin, with 100 percent verification of their contents; (2) using such technology as pressure, light, or temperature sensors to continually monitor containers throughout their overseas voyage to the point of distribution in the United States; and (3) using cargo-tracking technology to keep accurate track of containers at all points in the supply chain, including distribution to their ultimate destinations.
Megaports Initiative	In 2003, the Department of Energy (DOE) initiated the Initiative to enable foreign government personnel at key seaports to use radiation detection equipment to screen shipping containers entering and leaving these seaports for nuclear and other radioactive material that could be used against the United States or its allies. Through the Initiative, DOE installs radiation detection equipment at foreign seaports that is then operated by foreign government officials and port personnel working at these seaports.

Source: GAO analysis of CBP and DOE data.

The table also shows Operation Safe Commerce, initiated by the private sector and now administered by DHS's Office of Domestic Preparedness, which employs a similar strategy. This action, in pilot-project form that was initially funded by $58

million appropriated by Congress, is intended to help strengthen the security of cargo as it moves along the international supply chain in containers.[5] In late 2004, the second of two initial phases of the project was concluded. This phase involved identifying the security vulnerabilities of 19 separate supply chains and trying out technologies, such as container seals or sensors, and their integration with governmental policies, logistic processes and procedures that could mitigate those vulnerabilities. The project has received additional funding of $17 million that has been targeted to conduct a third phase in which the best technologies and practices identified in the first two phases will be further tested on a high number of containers for their effectiveness and tamper resistance on three separate supply chains. A report on the best practices identified in the first two phases is expected to be issued in June 2005, and completion of the third phase is expected by October 2006.

The other actions taken to enhance the security of cargo and commerce have been substantial. In 2002 CBP quickly rolled out the CSI and C–TPAT programs shown in table 2 and enlisted the participation of several countries and companies. By April 2005, CSI was operational at 35 seaports, located in 18 countries. Similarly, C–TPAT membership grew from about 1,700 companies in January 2003 to over 9,000 companies in March 2005. Given the urgency to take steps to protect against terrorism after the September 11, 2001, attacks, some of the actions were taken using an "implement and amend" approach. That is, CBP had to immediately implement the activity with the knowledge it may need to modify the approach later. For example, in August 2002, CBP modified the already developed Automatic Targeting System with new terrorism-related criteria.

Developing Greater Maritime Domain Awareness

The third main area of activity to enhance seaport security—maritime domain awareness—is the understanding by stakeholders involved in maritime security of anything associated with the global maritime environment that could adversely affect the security, safety, economy or environment of the United States. This awareness is essential to identify and respond to any unusual patterns or anomalies that could portend a possible terrorist attack. To be effective, maritime domain awareness must be comprehensive and include information on vessels, seaport infrastructures and facilities, shipping lanes and transit corridors, waterways, and anchorages, among other things. It must also identify threats as soon as possible and far enough away from U.S. seaports to eliminate or mitigate the threat. By effectively identifying potential threats, this awareness can be used as a force multiplier to position resources where they are needed most to respond, instead of spreading out limited resources to address all threats, no matter how unlikely they are to occur. In addition, when shared, this awareness has the potential to facilitate the coordination of efforts of local, state, federal, and even international stakeholders in responding to potential threats.

After the attacks of September 11, 2001, the Coast Guard took steps such as increasing the number of security patrols conducted within seaports and waterways that helped contribute to increased maritime domain awareness. Although maritime homeland security duties are not new to the Coast Guard, the number of hours the Coast Guard used resources (such as ships, boats, or aircraft) to carry out seaport, waterway, and coastal security activities during Fiscal Year 2003 increased by 1,220 percent from their pre-September 11, 2001, level. Relative to the rest of the Coast Guard's responsibilities, this represented an increase from 4 percent of the Coast Guard's total annual resource hours being used for seaport, waterway, and coastal security activities before September 11, 2001, to 34 percent by September 30, 2003. These activities provide an important input to maritime domain awareness as it places Coast Guard personnel out in the seaports where they can observe, report, and respond to suspect activities or vessels. In addition, these patrols provide the Coast Guard with a visible presence out in the seaport that may deter a potential terrorist attack from being carried out.

As the lead federal agency responsible for protecting the U.S. maritime domain, the Coast Guard has spearheaded an interagency approach for establishing maritime domain awareness. Within this approach are several activities and actions intended to collect information and intelligence, analyze the information and intelligence, and disseminate the analyzed information and intelligence to appropriate federal, state, local, or private seaport stakeholders. Some of these actions were required under MTSA, such as the establishment of an Automatic Identification System to track vessels, as well as creation of area maritime security committees of local seaport stakeholders who identify and address risks within their seaport. In addition to these actions, the Department of Defense and DHS formed a Maritime Domain Awareness Senior Steering Group in 2004 to coordinate national efforts to

improve maritime domain awareness. Under Homeland Security Presidential Directive 13, issued in December 2004, this steering group is required to develop a national plan for maritime domain awareness by June 2005. According to the head of the Coast Guard's maritime domain awareness program, a draft of this plan is being reviewed before it is submitted to the President. Table 3 shows some of the actions currently being taken or underway to enhance maritime domain awareness.

Table 3: Examples of Activities to Develop Maritime Domain Awareness

Maritime Domain Awareness activity	Example of activity
Collection of information and intelligence	**Automatic Identification System:** AIS uses a device aboard a vessel to transmit an identifying signal to a receiver located at the seaport and other ships in the area. This signal gives seaport officials and other vessels nearly instantaneous information and awareness about a vessel's identity, position, speed, and course. The Coast Guard intends to provide AIS coverage to meet maritime domain awareness requirements in all navigable waters of the United States and further offshore. As of May 2005, the Coast Guard has AIS coverage in several seaports and coastal areas.[a] In addition to this system, the Coast Guard is also working with the International Maritime Organization (IMO) to develop functional and technical requirements for long-range tracking out to 2,000 nautical miles. The Coast Guard proposed an amendment to the International Convention for Safety of Life at Sea (SOLAS) for this initiative, which is currently under consideration by the international body. However, according to the Coast Guard, the issue of long-range tracking is contentious internationally and it is uncertain whether the amendment will be adopted.
Analysis of information and intelligence	**Maritime Intelligence Fusion Centers and Field Intelligence Support Teams:** Centers have been established by the Coast Guard on the East and West Coasts to provide actionable intelligence to Coast Guard commanders and units. The teams also conduct initial analysis of intelligence in coordination with federal, state, and local law enforcement and intelligence agencies.
Dissemination of information and intelligence	**Area Maritime Security Committees:** The committees serve as forums for local seaport stakeholders from federal agencies, state and local governments, law enforcement, and private industries to gain a comprehensive perspective of security issues at a seaport location. Information is disseminated through regularly scheduled meetings, issuance of electronic bulletins on suspicious activities around seaport facilities, and sharing key documents. The committees also serve as a link for communicating threats and security information to seaport stakeholders. **Interagency Operational Centers:** These centers provide information 24 hours a day about maritime activities and involve various federal and nonfederal agencies directly in operational decisions using this information. Radar, sensors, and cameras offer representations of vessels and facilities. Other data are available from intelligence sources, including data on vessels, cargo, and crew. Unlike the area maritime security committees, these centers are operational in nature with a unified or joint command structure designed to receive information and act on it. Representatives from the various agencies work side by side, each having access to databases and other sources of information from their respective agencies. These currently exist in three locations: Charleston, South Carolina; Norfolk, Virginia; and San Diego, California.

Source: GAO analysis of Coast Guard data.

[a] The Coast Guard currently has AIS coverage in the following areas: Alaska (Anchorage, Homer, Nikiski, Seward, Valdez, and Juneau); Puget Sound (Seattle, Tacoma, Everett, Port Angeles, and Olympia); the Columbia River entrance; San Francisco Bay and approaches; Los Angeles/Long Beach Harbor and approaches; San Diego and approaches; Hawaii (Honolulu and Pearl Harbor); Gulf of Mexico (Houston/Galveston, Port Arthur, Berwick Bay, and Lower Mississippi River—New Orleans—Baton Rouge); South Florida (Key West, Miami, and Port Everglades); Charleston, South Carolina; Norfolk, Virginia; New York, New York; Long Island Sound (New Haven and New London); Boston Harbor and approaches; and Sault Ste. Marie, Michigan.

While many of the activities to develop maritime domain awareness are still underway, some progress has already been made. One activity in this area that we have recently looked at concerns the process of information sharing between federal and non-federal seaport stakeholders participating on area maritime security committees.[6] The Coast Guard organized 43 of these committees, covering the Nation's 361 seaports. While a primary purpose of the committees is to develop a seaport-wide security plan for their respective seaports, the committees also provide links for communicating threats and security information to seaport stakeholders—links that generally did not exist prior to the creation of the committees. The types of information shared among committee members with security clearances included assessments of vulnerabilities at specific seaport locations, information about potential threats or suspicious activities, and strategies to use in protecting key infrastructure. Our review found that the committees improved information sharing among seaport security stakeholders, including the timeliness, completeness, and usefulness of information shared.

Another aspect of improving maritime domain awareness involves having the assets to communicate and conduct patrols, and in this regard, the Coast Guard has budgeted for and is in the process of receiving substantial new resources. In 1996, the Coast Guard initiated a major recapitalization effort—known as the Integrated Deepwater System—to replace and modernize the agency's aging and deteriorating fleet of aircraft and vessel assets. The focus of the program is not just on new ships and aircraft, but also on newer, more capable assets, with improved and integrated command, control, communications and computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities. Although the program was started before the attacks of September 11, 2001, the Coast Guard plans to leverage these capabilities of the 20 year, $17 billion dollar program to enhance its maritime domain awareness and seaport security operations such as patrols and response.

Challenges for Improving Maritime Security Take Three Main Forms

Propelled by a strong sense of urgency to secure the seaports, federal agencies, such as the Coast Guard, CBP, and TSA, accomplished a considerable amount in a short time. At the same time, these actions have also shown the strains that often occur when difficult tasks must be done quickly. We have not examined every action that has been started or enhanced regarding maritime security, but our work to date has covered a number of them. It is not surprising that we have found, besides the progress made, a number of missteps, false starts, and inefficiencies. These represent challenges to overcome.

While some of these challenges will be resolved with time, analysis, and oversight, there are other challenges that bear even more careful watching, because they may prove to be considerably more difficult to overcome. I would like to highlight three of those challenges, providing examples from our recent work. These three challenges involve (1) design and implementing programs, (2) coordinating between different agencies and stakeholder interests, and (3) determining how to pay for these efforts.

Challenges in Program Design and Implementation

I will discuss today two illustrative examples related to challenges in program design and implementation that we have identified from our work. These include the (1) lack of planning and performance measures for program design and (2) lack of experienced personnel for program implementation.

Lack of Planning and Performance Measures for Program Design

One effect of having to design programs quickly is that they may lack such elements as strategic plans and performance measures needed to set program goals and monitor performance. The lack of such tools can create problems that need to be resolved as the program unfolds. For example, we have reviewed CBP's actions to establish a system meant to reliably identify potentially risky cargo containers.

Our work has shown that a need exists for additional efforts in several homeland security activities, including securing cargo, in order to help ensure the effectiveness of the approach.[7] As we noted in a July 2003 report, the former U.S. Customs Service, part of which is now CBP initiated the Container Security Initiative (CSI) in January 2002 in response to security vulnerabilities created by ocean container trade and the concern that terrorists could exploit these vulnerabilities to transport or detonate WMDs in the United States.[8] During the first year, program officials quickly designed and rolled out the initiative, modifying operations over time. The service achieved strong initial participation among the countries that it sought to enroll in the initiative, reaching agreement with 15 governments to place U.S. personnel at 24 seaports, and placing teams in 5 of these seaports. However, CBP had not taken adequate steps to incorporate human capital planning, develop perform-

ance measures, and plan strategically—factors essential to the program's long-term success and accountability. We noted, for example, that:

- More than 1 year into the implementation of the initiative, CBP had not developed a systematic human capital plan to recruit, train, and assign the more than 120 program staff that would be needed for long-term assignments in a wide range of foreign seaports, some of which could require language capabilities and diplomatic skills.
- CBP lacked performance measures for the initiative that demonstrated program achievements and established accountability. For example, the service lacked measures that assessed the impact of collocating U.S. and foreign customs officials in foreign seaports to determine which containers should be targeted for inspection.
- CBP's focus on short-term operational planning in order to quickly implement the program impeded its ability to systematically carry out strategic planning. We noted that the service did not have a strategic plan for the initiative that describes how it intends to achieve program goals and objectives. As a result, CBP lacked elements of strategic planning that would improve the management of the program and allow CBP to establish accountability for planned expenditures.

As also reported in July 2003, another program that did not take adequate steps to incorporate the human capital planning and performance measures necessary for the program's long-term success and accountability is CBP's Customs-Trade Partnership Against Terrorism (C–TPAT) program. Initiated in November 2001, C–TPAT is an initiative that attempts to improve the security of the international supply chain. It is a cooperative program between CBP and members of the international trade community in which private companies agree to improve the security of their supply chains in return for a reduced likelihood that their containers will be inspected.

During the first year, more than 1,700 companies agreed to participate in the program, and most received the key benefit—a reduced likelihood of inspections for WMDs. However, we noted similar kinds of problems to those in the CSI program. For example, we found that:

- Even as it rolled out new program elements, CBP lacked a human capital plan for increasing the number of C–TPAT staff from 10 to more than 160.
- CBP had not developed performance measures for C–TPAT that would establish accountability and measure program achievements. For example, CBP had no performance measure to assess the impact of C–TPAT on improving supply chain security practices, possibly resulting in benefits being granted to undeserving companies.
- CBP lacked strategic planning in rolling out C–TPAT, failing to communicate how it planned to implement critical program elements designed to verify that companies have security measures in place and follow through with recommended changes.

We are currently reviewing both the CSI and C–TPAT programs and will soon be issuing reports to update our earlier evaluation of these programs.

Lack of Experienced Personnel for Program Implementation

One major challenge in program implementation is the lack of experienced personnel, which is to be expected given the rapid increase in newly hired personnel since September 11, 2001. Agencies such as the Coast Guard expect to see large increases in the number of staff over the next few years to help meet new and expanded responsibilities. Consequently, they also face a challenge in absorbing this increase and training them to be fully productive. We pointed out early on that this would be a challenge for the Coast Guard,[9] and subsequent work has shown this to be the case. For example, after a Coast Guard internal review found that readiness of its multi-mission stations—the shore-based units whose responsibilities include finding and rescuing mariners in danger—had been in decline for an extended period, the Coast Guard began efforts to improve the readiness of the stations. This effort was complicated by the new homeland security responsibilities the stations assumed after the terrorist attacks of September 11, 2001. In a recent review of staffing and readiness at these multi-mission stations,[10] we found that the Coast Guard was still in the process of defining new standards for security activities and had yet to translate the impact of security-related mission responsibilities into specific station readiness requirements, such as staffing standards. Consequently, even though station staffing had increased 25 percent since 2001, the Coast Guard was unable

to align staffing resources with mission activities, which resulted in a significant number of positions not being filled with qualified personnel and station personnel working significantly longer hours than are allowed under the Coast Guard's work standards.

We also identified personnel or human capital challenges such as lack of experienced personnel related to the Coast Guard's program to oversee implementation of MTSA-required security plans by owners and operators of maritime facilities and vessels. These security plans are performance-based, meaning the Coast Guard has specified the outcomes it is seeking to achieve and has given seaport stakeholders responsibility for identifying and delivering the measures needed to achieve these outcomes. While this approach provides flexibility to owners and operators in designing and implementing their plans, it also places a premium on the skills and experience of inspectors to identify deficiencies and recommend corrective action. Because the Coast Guard had to review and assess for compliance more than 12,000 security plans for facilities and vessels, it had to rely heavily on reservists, which varied greatly in the level of their skills and experience in this area. For example, some reservists had graduate degrees in security management while others had no formal security training or experience. In June 2004, we recommended that the Coast Guard carefully evaluate its efforts during the initial surge period for inspections.[11] The Coast Guard has adjusted its inspection program to make its compliance assessments more relevant and useful, but it has not yet determined the overall effectiveness of its compliance actions.

Challenges in Coordinating Actions

Coordinating massive new homeland security actions has been an acknowledged challenge since the events of September 11, 2001, and seaport security has been no exception. On the federal side alone, we have for several years designated implementing and transforming the new DHS as a high-risk area.[12] Since the agency's inception in March 2003, DHS leadership has provided a foundation to maintain critical operations while undergoing transformation, and the agency has begun to put systems in place to operate more effectively and efficiently as an agency. In managing its transformation, however, DHS still faces such issues as forming effective partnerships with other governmental and private-sector entities.

We have made numerous recommendations related to information sharing, particularly as it relates to fulfilling federal critical infrastructure protection responsibilities.[13] For example, we have reported on the practices of organizations that successfully share sensitive or time-critical information, including establishing trust relationships, developing information-sharing standards and protocols, establishing secure communications mechanisms, and disseminating sensitive information appropriately. Federal agencies such as DHS and the Coast Guard have concurred with our recommendations that they develop appropriate strategies to address the many potential barriers to information sharing. However, as of January 2005, many federal efforts to do this remain in the planning or early implementation stages especially in the area of homeland security information sharing, including establishing clear goals, objectives, and expectations for the many participants in information-sharing efforts; and consolidating, standardizing, and enhancing federal structures, policies, and capabilities for the analysis and dissemination of information. In this regard, the issue of information-sharing across agency and stakeholder lines has emerged as a significant enough challenge that we have also designated it as a high-risk area. Here are three examples that illustrate the kinds of problems and challenges that remain related to seaport security.

Obtaining Security Clearances

While coordination of information-sharing at the seaport level appears to have improved, seaports are experiencing challenges with regards to non-federal officials obtaining security clearances. For some time, state and local seaport and law enforcement personnel have reported problems in obtaining federally generated intelligence information about their jurisdictions because they did not have a federal security clearance. However, as of February 2005—over 4 months after the Coast Guard had developed a list of over 350 non-federal area maritime security committee participants as having a need for a security clearance—only 28 had submitted the necessary paperwork for the background check. Local Coast Guard officials told us they did not clearly understand their responsibility for communicating with state and local officials about the process for obtaining a security clearance. After we expressed our concerns to Coast Guard officials in headquarters in February 2005, officials took action and drafted guidelines clarifying the role that local Coast Guard officials play in the program.

Sharing Information about Security Exercises

In a January 2005 report,[14] we reported that improvement in the coordination of state, local, and federal entities during seaport exercises was needed. While it was still too early to determine how well entities will function in coordinating an effective response to a seaport-related threat or incident, we identified four operational issues that needed to be addressed in order to promote more effective coordination. We found that more than half of the seaport exercises and after-action reports we examined raised communication issues, including problems with information sharing among first responders and across agency lines. We also found that over half of the exercises raised concerns with communication and the resources available, including inadequate facilities or equipment, differing response procedures, and the need for additional training in joint agency response. To a lesser extent, we found concerns with participants' ability to coordinate effectively and know who had the proper authority to raise security levels, board vessels, or detain passengers.

Developing a Transportation Worker Identification Credential

Beyond information-sharing, a host of challenges remain in coordinating across agency lines and in resolving issues that cut across a wide range of stakeholder perspectives. In this regard, there is perhaps no better example in our recent work than the delayed attempts to develop a major component of the security framework envisioned under MTSA—an identification card for maritime workers. The transportation worker identification credential (TWIC) was initially envisioned by TSA before it became part of DHS to be a universally recognized identification card accepted across all modes of the national transportation system, including airports, seaports, and railroad terminals, using biological metrics, such as fingerprints, to ensure individuals with such an identification card had undergone an assessment verifying that they do not pose a terrorism security risk. TSA initially projected that it would test a prototype of such a card system in 2003 and issue the first of the cards in August 2004. After TSA became part of DHS, testing of the prototype was delayed because of the difficulty in obtaining a response from DHS policy officials who also subsequently directed the agency to reexamine additional options for issuing the identification card. In addition to coordinating within DHS, TSA has had to coordinate with over 800 national level transportation-related stakeholders. Several stakeholders at seaports and seaport facilities told us that, while TSA solicited their input on some issues, TSA did not respond to their input or involve them in making decisions regarding eligibility requirements for the card.[15] In particular, some stakeholders said they had not been included in discussions about which felony convictions should disqualify a worker from receiving a card, even though they had expected and requested that DHS and TSA involve them in these decisions. Obtaining stakeholder involvement is important because achieving program goals hinges on the Federal Government's ability to form effective partnerships among many public and private stakeholders. If such partnerships are not in place—and equally important, if they do not work effectively—TSA may not be able to test and deliver a program that performs as expected. Until TSA and DHS officials agree on a comprehensive project plan to guide the remainder of the project and work together to set and complete deadlines, and TSA can effectively manage its stakeholders' interests, it may not be able to successfully develop, test, and implement the card program. We issued a report on TWIC in December 2004[16] and the Senate Committee on Homeland Security and Governmental Affairs has asked us to review the program again.

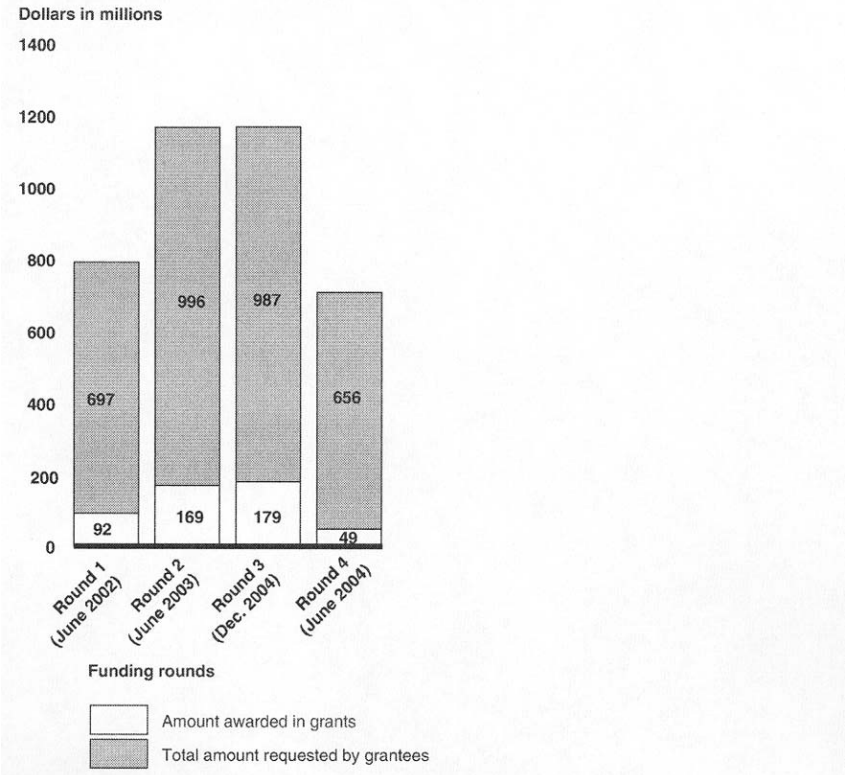
Challenges in Providing Funding for Seaport Security Actions and Initiatives

Our reviews indicate that funding is a pressing challenge to putting effective seaport security measures in place and sustaining these measures over time. This is the view of many transportation security experts, industry representatives, and federal, state, and local government officials with whom we have spoken. While some security improvements are inexpensive, most require substantial and continuous funding. For example, a preliminary Coast Guard estimate placed the cost of implementing the International Maritime Organization security code and the security provisions in MTSA at approximately $1.5 billion for the first year and $7.3 billion over the succeeding decade. This estimate should be viewed more as a rough indicator than a precise measure of costs, but it does show that the cost is likely to be substantial.[17]

At the federal level, more than $560 million in grants has been made available to seaports, localities, and other stakeholders since 2002 under the Port Security Grant Program and the Urban Area Security Initiative. The purpose of these programs was to reduce the vulnerability of seaports to potential terrorist attacks by enhancing facility and operation security. The programs funded several projects, in-

cluding security assessments; physical enhancements, such as gates and fences; surveillance equipment, such as cameras; and the acquisition of security equipment, such as patrol vessels or vehicles. Awardees have included seaport authorities, local governments, vessel operators, and private companies with facilities in seaport areas. Interest in receiving port security grants has been strong, and, as figure 2 shows, applicant requests have far exceeded available funds. We are currently examining the Port Security Grant Program at the request of several Members of Congress, and we are focusing this review on the risk management practices used in comparing and prioritizing applications. Our work is under way, and we expect to issue our report later this year.[18]

Figure 2: Comparison of Requests and Awards for Funding, Port Security Grant Program, Fiscal Years 2002-2004



Source: GAO analysis of TSA data.

Note: Figure 2 does not include $75 million that was awarded to 14 high-risk seaport areas under the Urban Area Security Initiative (UASI) by the Office of Domestic Preparedness. This program is separate from its basic UASI program, which provided formula grants to 50 urban areas for equipment, training, planning, exercise, operational needs, and critical infrastructure.

Where the money will come from for all of the funding needs is unclear. In our 2002 statement on national preparedness,[19] we highlighted the need to examine the sustainability of increased funding not only for seaport security, but for homeland security efforts in general. The current economic environment makes this a difficult time for private industry and state and local governments to make security investments and sustain increased security costs. According to industry representatives and experts we contacted, most of the transportation industry operates on a very thin profit margin, making it difficult to pay for additional security measures. Budgetary and revenue constraints, coupled with increasing demands on resources, makes it more critical that federal programs be designed carefully to match the pri-

orities and needs of all partners—federal, state, local, and private—and provide the greatest results for the expenditure.

Setting Performance Goals and Measures and Assessing Risk Are Important Next Steps

The final purpose of my testimony today is to offer observations, based on the work we have done to date, about important next steps for decision makers in charting a course for future actions. The terrorist attacks of September 11, 2001, evoked with stunning clarity the face and intent of enemies very different from those the nation has faced before—terrorists such as al Qaeda, willing and able to attack us in our territory using tactics designed to take advantage of our relatively open society and individual freedoms. The amount of activity in response has been considerable, and although there have been no serious incidents in the United States in the interim, the threat of terrorism will likely persist well into the 21st century. Thus, it is important to continue to make progress in our efforts. Beyond addressing the kinds of challenges discussed above, however, two other matters stand out. One involves developing a better understanding of how much progress has actually been made to secure our seaports; the other involves developing a better strategy to manage risk and prioritize what areas need further progress and how resources can be best allocated.

Lack of Goals and Measures Makes Determining Progress Difficult

Although there is widespread agreement that actions taken so far have led to a heightened awareness of the need for security and an enhanced ability to identify and respond to many security threats, it is difficult to translate these actions into a clear sense of how far we have progressed in making seaports more secure. One reason is that seaport security efforts, like homeland security efforts in general, lack measurable goals, as well as performance measures to measure progress toward those goals. As others such as the Gilmore Commission have stated, a continuing problem for homeland security has been the lack of clear strategic guidance about the definition and objectives of preparedness.[20] For example, the Coast Guard has a set of performance indicators for each of its non-security missions. It regularly reports on how well it is doing in rescuing mariners at sea, interdicting foreign fishing boats attempting to fish in the U.S. exclusive economic zone, or maintaining aids to navigation on the Nation's waterways. However, although it has been more than 3 years since the September 11, 2001, attacks, the Coast Guard is still in the process of developing a performance indicator for its seaport security activities that can be used to indicate what progress has been made to secure seaports. Completion of this indicator and careful tracking of it over the long term is essential to help ensure that taxpayer dollars are being spent wisely to make seaports more secure. Similarly, as discussed earlier in describing the actions taken to secure the cargo transiting through seaports in containers, performance measures are needed to determine the progress such actions are making to reduce vulnerabilities of the international supply chain.

A challenge exists in measuring progress in this area, because seaport security, like many aspects of homeland security, relies upon the coordinated actions of many stakeholders and, in many cases, upon "layers" of defenses. In this regard, we have pointed out that systems and service standards—which focus on the performance, design, and overall management of processes and activities—hold great potential to improve coordination across such dimensions and enhance measurement of continued preparedness.[21] While such standards are already being used in many parts of the private sector, creation of performance and results measures for national security in general, and seaport security in particular, remains a work in progress.

Risk Management Is an Essential Tool for Focusing Efforts Effectively

Even with clear goals and effective performance measures, it seems improbable that all risk can be eliminated, or that any security framework can successfully anticipate and thwart every type of potential terrorist threat that highly motivated, well skilled, and adequately funded terrorist groups could think up. This is not to suggest that security efforts do not matter—they clearly do. However, it is important to keep in mind that total security cannot be bought no matter how much is spent on it. We cannot afford to protect everything against all threats—choices must be made about security priorities. Thus, great care needs to be taken to assign available resources to address the greatest risks, along with selecting those strategies that make the most efficient and effective use of resources.

One approach to help ensure that resources are assigned and appropriate strategies are selected to address the greatest risks is through risk management—that is, defining and reducing risk. A risk management approach is a systematic process for analyzing threats and vulnerabilities, together with the criticality (that is, the rel-

ative importance) of the assets involved. This process consists of a series of analytical and managerial steps, basically sequential, that can be used to assess vulnerabilities, determine the criticality (that is, the relative importance) of the assets being considered, determine the threats to the assets, and assess alternatives for reducing the risks. Once these are assessed and identified, actions to improve security and reduce the risks can be chosen from the alternatives for implementation. To be effective, however, this process must be repeated when threats or conditions change to incorporate any new information to adjust and revise the assessments and actions.

Some elements of risk management have been incorporated into seaport security activities. For example, to meet the requirements of MTSA, security plans for seaports, facilities, and vessels have been developed based on assessments that identify their vulnerabilities. In addition, the Coast Guard is using the Port Security Risk Assessment Tool, which is designed to prioritize risk according to a combination of possible threat, consequence, and vulnerability. Under this approach, seaport infrastructure that is determined to be both a critical asset and a likely and vulnerable target would be a high priority for security enhancements or funding. By comparison, infrastructure that is vulnerable to attack but not as critical or infrastructure that is very critical but already well protected would be lower in priority. In a homeland security setting, possible uses of data produced from risk management efforts include informing decisions on where the Federal Government might spend billions of dollars within and between federal departments, as well as informing decisions on grants awarded to state and local governments.

As the Nation moves ahead with seaport security efforts, there are plans to incorporate risk management as part of the Nation's larger homeland security strategy. Homeland Security Presidential Directive 7, issued in December 2003, charged DHS with integrating the use of risk management into homeland security activities. The directive called on the Department to develop policies, guidelines, criteria, and metrics for this effort. To meet this requirement, the Coast Guard has taken steps to use risk management in prioritizing the protection of key infrastructure within and between seaports. We are currently in the process of assessing the progress the Coast Guard has made in these efforts. In addition, we are reviewing the extent to which a risk management approach is being used by other DHS agencies, such as the Information Analysis and Infrastructure Protection Directorate, to evaluate the relative risk faced by key infrastructure within seaports and across broad sectors of national activity, such as seaports and aviation, to help ensure funding and resources are allocated to where they are needed most. Our work is still under way and not far enough along to discuss at this time. It is likely, however, that attention to risk management will be a key part of the ongoing dialogue about the Nation's homeland security actions in general, and its seaport security actions in particular.

Concluding Observations

Managing the risks associated with securing our Nation's seaports involves a careful balance between the benefits of added security and the potential economic impacts of security enhancements. While there is broad support for greater security, the national economy is heavily dependent on keeping goods, trucks, trains, and people flowing quickly through seaports, and bringing commerce to a crawl in order to be completely safe carries its own serious economic consequences. Striking the right balance between increased security and protecting economic vitality is an important and difficult task. Considering this, three things stand out as important from the work we have conducted:

- Seaports are not retreating as a homeland security issue. They are an attractive terrorist target and are likely to remain so, because by their nature they represent a vulnerability that is always open to potential exploitation.
- Seaport security has lived up to its billing as an area in which security measures can be difficult to implement. The range of activity in seaport areas can be extremely wide, as can the range of stakeholders and the fragmentation of responsibility among them. Many of the problems we have identified with individual programs and efforts can likely be overcome with time and effort, but success is not assured. We are already seeing some efforts, such as the TWIC identification card, becoming deeply mired in problems. These activities will thus continue to demand close attention.
- The national dialogue on this issue is likely to focus increasingly in trying to determine what we are getting for our efforts and where we should invest the dollars we have. Therefore, it is critical that federal programs be designed carefully to try to match the priorities and needs of all partners—federal, state, local, and private—and use performance measures to effectively allocate funds

and resources. On this point, there is work to do, because agencies such as the Coast Guard currently lack a systematic approach for explaining the relationship between the expenditure of resources and performance results in seaport security, limiting its ability to critically examine its resource needs and prioritize program efforts. Providing answers also requires an ability to carefully assess what the key vulnerabilities are and what should be done to protect them. Only by doing this will we have reasonable assurance that we are doing the best job with the dollars we have.

Mr. Chairman, this concludes my prepared statement. I would be pleased to answer any questions that you or other Members of the Committee may have.

ENDNOTES

[1] Pub. L. 107–295, 116 Stat. 2064 (2002).

[2] Zeigert, Amy, et. al. "Port Security: Improving Emergency Response Capabilities at the Ports of Los Angeles and Long Beach." *California Policy Options 2005.* University of California Los Angeles, School of Public Affairs (Los Angeles, Calif. 2005).

[3] None of the listings in this testimony is meant to be exhaustive of all the efforts under way. The Coast Guard has a range of activities underway for reducing seaport vulnerabilities that extends beyond the actions shown here. Such activities include, among others the use of armed boarding officers, formerly known as sea marshals, who board high-interest vessels arriving or departing U.S. seaports and stand guard in critical areas of the vessels; the establishment of Maritime Safety and Security Teams (MSST) to provide antiterrorism protection for strategic shipping, high-interest vessels, and critical infrastructure; and the underwater port security system, which uses trained divers and robotic cameras to check ship hulls and piers and an underwater intruder detection system. We have not evaluated the effectiveness of these activities.

[4] Another program to help secure the overseas supply chain process is the Coast Guard's International Port Security Program. In response to being required under MTSA to assess antiterrorism measures maintained at foreign seaports, the Coast Guard established this program in April 2004 to protect the global shipping industry by helping foreign nations evaluate security measures in their seaports. Through bilateral or multilateral discussions, the Coast Guard and the host nations review the implementation of security measures against established security standards, such as the International Maritime Organization's ISPS Code. To conduct the program, the Coast Guard has assigned officials to three regions (Asia-Pacific, Europe/Africa/Middle East, and Central/South America) to facilitate the discussions. In addition, a Coast Guard team has been established to conduct country/port visits, discuss security measures implemented, and develop best practices between countries. Each year the Coast Guard seeks to visit approximately 45 countries that conduct maritime trade with the United States.

[5] The Nation's three largest container port regions (Los Angeles/Long Beach, New York/New Jersey, and Seattle/Tacoma) are involved in the Operation Safe Commerce pilot project.

[6] GAO, *Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention*, GAO–05–394 (Washington, DC: April 15, 2005).

[7] GAO, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*. GAO–03–770 (Washington, DC: July 2003); and GAO, *Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO–04–557T (Washington, DC: March 2004). In addition, we have additional work underway regarding the Container Security Initiative Program and expect to issue our report in May.

[8] GAO, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*. GAO–03–770 (Washington, DC: July 2003).

[9] GAO, *Homeland Security: Challenges Facing the Coast Guard as It Transitions to the New Department*, GAO–03–467T (Washington, DC: February 2003).

[10] GAO, *Coast Guard: Station Readiness Improving, but Resource Challenges and Management Concerns Remain*, GAO–05–161 (Washington, DC: January 31, 2005).

[11] GAO, *Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security*, GAO–04–838 (Washington, DC: June 30, 2004).

[12] GAO, *High-Risk Series: An Update*, GAO–05–207 (Washington, DC: January 2005).

[13] GAO, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues*, GAO–03–1165T (Washington, DC: September 17,

2003); and *Homeland Security: Information-Sharing Responsibilities, Challenges, and Key Management Issues*, GAO–03–715T (Washington, DC: May 8, 2003).

[14] GAO, *Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention*, GAO–05–170 (Washington, DC: January 2005).

[15] Of the facilities testing TSA's prototype, we visited ports and facilities in the Delaware River Region, including Wilmington Port Authority, the Philadelphia Maritime Exchange, and the South Jersey Port. We also visited ports and facilities on the West Coast, including those in the Port of Seattle, Port of Los Angeles, and Port of Long Beach as well as ports and facilities in Florida, including Port Everglades and the Port of Jacksonville.

[16] GAO, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, GAO–05–106 (Washington, DC: December 2004).

[17] GAO, *Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security*, GAO–04–838 (Washington, DC: June 2004).

[18] DHS has proposed consolidating homeland grant programs into a single program. Known as the Targeted Infrastructure Protection Program (TIPP), the program would lump together grant funding for transit, port security and other critical infrastructure, and eliminate specific grant programs for port, rail, truck, intercity bus, and non-governmental organizations security. In its Fiscal Year 2006 budget request, the Administration proposed $600 million for TIPP, a $260-million increase in overall funding from Fiscal Year 2005 for the specific transportation security grant programs. In Fiscal Year 2005, funding for port, rail, truck, intercity bus, and non-governmental organizations security totaled $340 million.

[19] GAO, *National Preparedness: Integration of Federal, State, Local, and Private Sector Efforts Is Critical to an Effective National Strategy for Homeland Security*, GAO–02–621T (Washington, DC: April 2002).

[20] The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *V. Forging America's New Normalcy* (Arlington, VA: December 15, 2003).

[21] GAO, *Homeland Security: Observations on the National Strategies Related to Terrorism*, GAO–04–1075T (Washington, DC: September 22, 2004).

APPENDIX I: RELATED GAO PRODUCTS

Coast Guard: Preliminary Observations on the Condition of Deepwater Legacy Assets and Acquisition Management Challenges. GAO–05–307T. Washington, DC: April 20, 2005.

Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention. GAO–05–394. Washington, DC: April 15, 2005.

Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports. GAO–05–375. Washington, DC: March 31, 2005.

Coast Guard: Observations on Agency Priorities in Fiscal Year 2006 Budget Request. GAO–05–364T. Washington, DC: March 17, 2005.

Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention. GAO–05–170, Washington, DC: January 14, 2005.

Port Security: Planning Needed to Develop and Operate Maritime Worker Identification Card Program. GAO–05–106. Washington, DC: December 10, 2004.

Maritime Security: Better Planning Needed to Help Ensure an Effective Port Security Assessment Program. GAO–04–1062. Washington, DC: September 30, 2004.

Maritime Security: Partnering Could Reduce Federal Costs and Facilitate Implementation of Automatic Vessel Identification System. GAO–04–868. Washington, DC: July 23, 2004.

Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security. GAO–04–838. Washington, DC: June 30, 2004.

Coast Guard: Deepwater Program Acquisition Schedule Update Needed. GAO–04–695. Washington, DC: June 14, 2004.

Coast Guard: Key Management and Budget Challenges for Fiscal Year 2005 and Beyond. GAO–04–636T. Washington, DC: April 7, 2004.

Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection. GAO–04–557T. Washington, DC: March 31, 2004.

Coast Guard Programs: Relationship Between Resources Used and Results Achieved Needs to Be Clearer. GAO–04–432. Washington, DC: March 22, 2004.

Contract Management: Coast Guard's Deepwater Program Needs Increased Attention to Management and Contractor Oversight. GAO–04–380. Washington, DC: March 9, 2004.

Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers. GAO–04–325T. Washington, DC: December 16, 2003.

Posthearing Questions Related to Aviation and Port Security. GAO–04–315R. Washington, DC: December 12, 2003.

Maritime Security: Progress Made in Implementing Maritime Transportation Security Act, but Concerns Remain. GAO–03–1155T. Washington, DC: September 9, 2003.

Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors. GAO–03–770. Washington, DC: July 25, 2003.

Homeland Security: Challenges Facing the Department of Homeland Security in Balancing Its Border Security and Trade Facilitation Missions. GAO–03–902T. Washington, DC: June 16, 2003.

Coast Guard: Challenges during the Transition to the Department of Homeland Security. GAO–03–594T. Washington, DC: April 1, 2003.

Transportation Security: Post-September 11th Initiatives and Long-Term Challenges. GAO–03–616T. Washington, DC: April 1, 2003.

Coast Guard: Comprehensive Blueprint Needed to Balance and Monitor Resource Use and Measure Performance for All Missions. GAO–03–544T. Washington, DC: March 12, 2003.

Homeland Security: Challenges Facing the Coast Guard as It Transitions to the New Department. GAO–03–467T. Washington, DC: February 12, 2003.

Container Security: Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges. GAO–03–297T. Washington, DC: November 18, 2002.

Coast Guard: Strategy Needed for Setting and Monitoring Levels of Effort for All Missions. GAO–03–155. Washington, DC: November 12, 2002.

Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful. GAO–02–993T. Washington, DC: August 5, 2002.

Combating Terrorism: Preliminary Observations on Weaknesses in Force Protection for DOD Deployments through Domestic Seaports. GAO–02–955TNI. Washington, DC: July 23, 2002.

Appendix II: Previous GAO Recommendations

Agency/program	GAO recommendations
Coast Guard	**GAO Recommendations to the U.S. Coast Guard**
Automatic Identification System (AIS)	To seek and take advantage of opportunities to partner with organizations willing to develop AIS systems at their own expense in order to help reduce federal costs and speed development of AIS nationwide. (GAO–04–868)
Deepwater acquisition	Take the necessary steps to make integrated product team (IPT) members effective, including (1) training IPTS in a timely manner, (2) chartering the sub-IPTs, and (3) making improvements to the electronic information system that would result in better information sharing among IPT members who are geographically dispersed. (GAO–04–380)
	Follow the procedures outlined in the human capital plan to ensure that adequate staffing is in place and turnover among Deepwater personnel is proactively addressed. (GAO–04–380)
	Ensure that field operators and maintenance personnel are provided with timely information and training on how the transition will occur and how maintenance responsibilities are to be divided between system integrator and Coast Guard personnel. (GAO–04–380)
	Develop and adhere to measurable award fee criteria consistent with the Office of Federal Procurement Policy's guidance. (GAO–04–380)
	Ensure that the input of contracting officer's technical representatives (COTR) is considered and set forth in a more rigorous manner. (GAO–04–380)

Appendix II: Previous GAO Recommendations—Continued

Agency/program	GAO recommendations
	Hold the system integrator accountable in future award fee determinations for improving the effectiveness of IPTs. (GAO–04–380)
	Establish a time frame for when the models and metrics will be in place with the appropriate degree of fidelity to be able to measure the contractor's progress toward improving operational effectiveness. (GAO–04–380)
	Establish a total ownership cost (TOC) baseline that can be used to measure whether the Deepwater acquisition approach is providing the government with increased efficiencies compared to what it would have cost without this approach. (GAO–04–380)
	Establish criteria to determine when the TOC baseline should be adjusted and ensure that the reasons for any changes are documented. (GAO–04–380)
	Develop a comprehensive plan for holding the system integrator accountable for ensuring an adequate degree of competition among second-tier suppliers in future program years. This plan should include metrics to measure outcomes and consideration of how these outcomes will be taken into account in future award fee decisions. (GAO–04–380)
	For subcontracts over $5 million awarded by Integrated Coast Guard Systems LLC (ICGS) to Lockheed Martin and Northrop Grumman, require Lockheed Martin and Northrop Grumman to notify the Coast Guard of a decision to perform the work themselves rather than contracting it out. (GAO–04–380)
	To update the original 2002 Deepwater acquisition schedule in time to support the Fiscal Year 2006 Deepwater budget submission to DHS and Congress and at least once a year thereafter to support each budget submission, which should include the current status of asset acquisition phases, interim phase milestones, and the critical paths linking the delivery of individual components to particular assets. (GAO–04–695)
MTSA security plans	Conduct a formal evaluation of compliance inspection efforts taken during the initial 6-month surge period, including the adequacy of security inspection staffing, training, and guidance, and use this evaluation as a means to strengthen the compliance process for the longer term. (GAO–04–838)
	Clearly define the minimum qualifications for inspectors and link these qualifications to a certification process. (GAO–04–838)
	Consider including unscheduled and unannounced inspections and covert testing as part of its inspection strategy to provide better assurance that the security environment at the Nation's seaports meets the Nation's expectations. (GAO–04–838)
Multi-mission station readiness	Revise the *Boat Forces Strategic Plan* to (1) reflect the impact of homeland security requirements on station needs and (2) identify specific actions, milestones, and funding needs for meeting those needs. (GAO–05–161)
	Develop measurable annual goals for stations. (GAO–05–161)
	Revise the processes and practices for estimating and allocating station personal protection equipment (PPE) funds to reliably identify annual funding needs and use this information in making future funding decisions. (GAO–05–161)

Appendix II: Previous GAO Recommendations—Continued

Agency/program	GAO recommendations
Obtaining security clearances	Develop formal procedures so that local and headquarters officials use the Coast Guard's internal databases of state, local, and industry security clearances for area maritime committee members as a management tool to monitor who has submitted applications for a security clearance and to take appropriate action when application trends point to possible problems. (GAO–05–394)
	Raise awareness of state, local, and industry officials about the process of applying for security clearances. (GAO–05–394)
Port security assessment program	To define and document the geographic information system (GIS) functional requirements. (GAO–04–1062)
	Develop a long-term project plan for the GIS and the Port Security Assessment Program as a whole (including cost estimates, schedule, and management responsibilities). (GAO–04–1062)
Resource effectiveness	To develop a time frame for expeditiously proceeding with plans for implementing a system that will accurately account for resources expended in each of its program areas. (GAO–04–432)
	Ensure that the strategic planning process and its associated documents include a strategy for (1) identifying intervening factors that may affect program performance and (2) systematically assessing the relationship between these factors, resources used, and results achieved. (GAO–04–432)
Seaport exercises	To help ensure that reports on terrorism-related exercises are submitted in a timely manner that complies with all Coast Guard requirements, the Commandant of the Coast Guard should review the Coast Guard's actions for ensuring timeliness and determine if further actions are needed. (GAO–05–170)
Department of Energy	**GAO Recommendations to the Department of Energy**
Megaports Initiative	Develop a comprehensive long-term plan to guide the future efforts of the Initiative that includes, at a minimum, (1) performance measures that are consistent with DOE's desire to install radiation detection equipment at the highest priority foreign seaports, (2) strategies to determine how many and which lower priority ports DOE will include in the Initiative if it continues to have difficulty installing equipment at the highest priority ports, (3) projections of the anticipated funds required to meet the Initiative's objectives, and (4) specific time frames for effectively spending program funds. (GAO–05–375)
	Evaluate the accuracy of the current per port cost estimate of $15 million, make any necessary adjustments to the Initiative's long-term cost projection, and inform Congress of any changes to the long-term cost projection for the Initiative. (GAO–05–375)
U.S. Customs and Border Protection	**GAO recommendations to the U.S. Customs and Border Protection**
Container Security Initiative (CSI) and Customs-Trade Partnership Against Terrorism (C–TPAT)	Develop *human capital plans* that clearly describe how CSI and C–TPAT will recruit, train, and retain staff to meet their growing demands as they expand to other countries and implement new program elements. These plans should include up-to-date information on CSI and C–TPAT staffing and training requirements and should be regularly used by managers to identify areas for further human capital planning, including opportunities for improving program results. (GAO–03–770)

Appendix II: Previous GAO Recommendations—Continued

Agency/program	GAO recommendations
	Expand efforts already initiated to develop performance measures for CSI and C–TPAT that include outcome-oriented indicators. These measures should be tangible, measurable conditions that cover key aspects of performance and should enable agencies to assess accomplishments, make decisions, realign processes, and assign accountability. Furthermore, the measures should be used to determine the future direction of these Customs' programs. (GAO–03–770) Develop strategic plans that clearly lay out CSI and C–TPAT goals, objectives, and detailed implementation strategies. These plans should not only address how the strategies and related resources, both financial and human, will enable Customs to secure ocean containers bound for the United States, but also reinforce the connections between these programs' objectives and both Customs' and the Department of Homeland Security's long-term goals. (GAO–03–770) Use its resources to maximize the effectiveness of its automated targeting strategy to reduce the uncertainty associated with identifying cargo for additional inspection. (GAO–04–557T) Institute a national inspection reporting system. (GAO–04–557T) Test and certify CBP officials that receive the targeting training. (GAO–04–557T) Resolving the safety concerns of longshoremen unions. (GAO–04–557T)
Transportation Security Administration	**GAO recommendations to the U.S. Transportation Security Administration**
Transportation worker identification card (TWIC)	Develop a comprehensive project plan for managing the remaining life of the TWIC project. (GAO–05–106) Develop specific, detailed plans for risk mitigation and cost-benefit and alternatives analyses. (GAO–05–106)

Source: GAO.

The CHAIRMAN. Thank you very much.

Did you examine the Port of Los Angeles?

Ms. WRIGHTSON. We have been to Los Angeles numerous times in the course of working on various requests for this Committee and others. Los Angeles/Long Beach represents an incredibly critical seaport, and it suffers from a lot of the problems that are described generally in our reports—from those of TWIC to those of securing facilities and providing adequate patrols. Overall, Los Angeles, like other ports, has both security accomplishments and security gaps.

The CHAIRMAN. Did you write a separate report on it?

Ms. WRIGHTSON. We have never issued a separate report on Los Angeles. And if we did, it probably would have to be classified. We wouldn't be able to present it publicly.

The CHAIRMAN. All right. Are you aware of their secure zone versus this working zone?

Ms. WRIGHTSON. Absolutely.

The CHAIRMAN. Are you critical of that?

Ms. WRIGHTSON. Well, we would—in order to make an informed judgment about it—we would need to audit it to see what risks are mitigated and what problems remain. And we haven't done that.

The CHAIRMAN. Well, it was pointed out to me that no one goes into that secure zone unless they're known personally by about five other people.

Ms. WRIGHTSON. All ports—which Admiral Hereth is very able to tell you—have security zones around critical infrastructure. So, for example, there's a security zone around Logan Airport, there are security zones around most, and they are, to various extents, patrolled and protected. But the—I must say, in general, the efficacy—we have a lot of effort—the efficacy of these efforts, be they for domestic security or internationally, still remain to be determined. I think it would be an excellent area for your future oversight and investigation if we were to look at those.

The CHAIRMAN. Before he left, Senator Lott told me that we have appropriated a total of $515 million from June 2002 through December 2003. Of that money, only $107 million had been spent by December 2004. Are you familiar with those figures, Admiral?

Admiral HERETH. I presume you're talking about the grant—Port Security Grant Program, sir?

The CHAIRMAN. Right.

Admiral HERETH. It may be because of—the constraints on the contracts haven't been met by the grantees. But I'm not specifically familiar with the details of that. I can certainly give you some feedback, sir.

The CHAIRMAN. Senator Lott had to go to another meeting, but he's very critical of the rate of spending, in terms of the security aspects of the grants we've already made. Would you have someone contact him and see if we can get an answer for him of why the rate of spending for security, specifically appropriated for that purpose is so low?

Senator Inouye?

Senator INOUYE. Recently, a report was issued that nearly $8 billion worth of security equipment and devices used by the airports are non-functional or don't serve the purpose, and will have to be thrown away. I presume you use similar equipment in the ports, Mr. Jacksta.

Mr. JACKSTA. Yes, sir. We have—as I indicated in my opening remarks, we do have large-scale X-ray systems at the port of entries, at the seaports, somewhere in the area of about 56 actually there, to do the VACIS examination—that's an X-ray of the container as it comes off. We also use equipment such as personal radiation detectors, which are carried by the inspectors, and indicate whether there's any type of radiological signature coming from any of the containers.

We also have, and we're deploying right now, radiation portal monitors to the major seaports. We already have them installed at Newark, Jacksonville, and Boston. And this summer we'll be putting them at the L.A./Long Beach seaport area.

Senator INOUYE. And you will continue to employ them, notwithstanding the fact that the airports find them non-functional?

Mr. JACKSTA. Well, sir, I don't know whether the equipment that CBP is utilizing at the airports are basically the same type of tech-

nology—X-ray systems. We use that equipment. And, from our knowledge, the equipment is working well in helping us examine containers and luggage, that are coming into the United States.

Senator INOUYE. I would suggest you check them out.

Mr. Skinner, in your testimony you indicated that—in your grant program—that there are a considerable number of grantees who are not prepared, or don't know how, to use these funds. Did I hear correctly?

Mr. SKINNER. Yes, sir, you did. Although we did not go to each of the grantees to validate why, individually, the funds were not being spent in a timely manner, we did note, during our review, when we questioned program officials about this, that there was a slow rate of expenditure because there were considerable negotiations going on between the Department and the grant recipient trying to further define what the grant funds were to be used for. In other words, the grants were awarded before we were clear as to exactly what we intended to accomplish with those funds.

That, coupled with the fact that, at the time we were doing our review, there was only one individual that had responsibility for providing oversight and monitoring of those grants, and, as a result, the slow spending rate was never brought to light until late 2004, early 2005.

Senator INOUYE. Over the years, I've learned that just about every department, bureau, and section provides some sort of grant program, and it's not easy to get these grants. Very competitive. And most of them are highly qualified. How is it that, in your area, you say most of them don't know how to use the funds or have no experience?

Mr. SKINNER. No, sir. What we were saying was that the grantee was not prepared to use the funds. In other words, their grant application was not specific enough to allow the Department to determine what we were going to get for our money. So, once the grant was then awarded, negotiations took place.

Senator INOUYE. And not withstanding that, the grant was approved?

Mr. SKINNER. That's correct, sir.

Senator INOUYE. Did someone evaluate the grant application?

Mr. SKINNER. Yes, sir. It went through a very intensive evaluation process, both at——

Senator INOUYE. But with that intensive——

Mr. SKINNER.—the field and headquarters level.

Senator INOUYE.—you didn't see this.

Mr. SKINNER. I beg your pardon, sir?

Senator INOUYE. You didn't see the shortcoming. With the intensive——

Mr. SKINNER. Evidently not. This was not universal. There may be other reasons why the moneys were not spent. We did not go down to the grantee level. What we did identify, however, like I said, was, the fact that there was considerable negotiations going on which delayed the actual expenditure of funds.

Senator INOUYE. Well, did you find when these funds were not properly used, that they were taken back? Did the agency seek a return——

Mr. SKINNER. It's not that they were not properly used; they just were not used at all. They were still available for use. And once the Department was satisfied how the funds would, in fact, be used—after the award, after the fact—then I would suspect that they would then apply those funds and expend them.

Senator INOUYE. Thank you very much.

Just prior to your testimony, the Congressman testified, indicating that it takes over a year to get the security clearance, and that there are 450,000 awaiting clearance. Is that the situation in the ports?

Mr. JACKSTA. Well, I'd like to begin by saying that, from CBP's perspective, we have our officers and the supervisors that are engaged with the examination and making decisions on what to inspect. They have that type of clearance. We ensure that the intelligence and information that's required to get to the CBP officer is getting to the actual location and to the officers who need to have that information. So, although we would like to have more individuals with security clearance, the agency does have people available who get that information and look at it.

Senator INOUYE. Admiral?

Admiral HERETH. Yes, sir. I can add a little bit to that. We, since 9/11, have set up our own security center. We process our own security clearances for all the members of the Coast Guard and our employees. That's going fine. We've also taken the step to go back to the Department and get authorization to get up to 800 clearances for members of industry and/or trade associations. And, as the Congressman pointed out, we think that's a key feature that needs to be implemented quickly. And we have distributed authorizations around the country. We have 43 Area Maritime Security Committees, and we've asked our Captains of the Port to serve as the focal points to identify people in the Area Committees appropriate industry-segment representatives that we could communicate with, that could get—you know, get clearances, authorized security clearances, so we can talk to them about secret information and pass current information in an appropriate, timely, and transparent fashion. We believe that's a hugely positive step.

We can process those clearances in a timely fashion. I don't think it would take anywhere near a year, but it's going to take a month or two to get them through the system, but the challenge is getting the members who want the clearance to fill out the—I think it's a 17-page form. We struggle on that front. But we're trying to push through that. We're trying to do that as quickly as we can, because we think that's an important part of the communication process that needs to happen between the regulatory agencies—Coast Guard, in particular—and the industry segments that we work with in the maritime.

Senator INOUYE. Ms. Wrightson?

Ms. WRIGHTSON. Thank you, I want to add to Admiral Hereth's comments that—to shed some light on this—in terms of what's going on at ports with Area Maritime Security Committees, that's the group Congressman Ruppersberger was talking about—these were the 361 people that the Coast Guard immediately designated as in need of clearances. Of those 361, only 28 had applied, 4 months after the fact. When we went in and audited it, we found

three things as key explanatory factors. First, there was an insufficient understanding of what they were supposed to do by—by they I mean these private parties and local officials. Second, there was confusion on the part of Coast Guard onsite, as to what their roles and responsibilities were. And, third—and this is very important, going forward—we found limitations in the management information system that the Coast Guard had to troubleshoot problems.

As it always does, the Coast Guard is very nimble and has been very responsive to the recommendations that we've made to correct these problems, so one would anticipate improvements there. However, it appeared—correct me if I'm wrong—that the Coast Guard may be getting this as larger responsibility for DHS. Has that changed, or is there still talk of that?

Admiral HERETH. There must be still talk of that. Our focus has been getting the—in the instant, getting those 800 clearances in position so we can actually talk, at the secret level, with industry representatives, along with a handful of representatives inside the beltway. Because the trade associations—and I think there's 32 that we're linked with here inside the beltway—provide a key role in linking back to their members. And the credibility and the timeliness of getting information out hinges on getting those clearances in place, we think. It will be a much more effective system and a very—and a step forward for all of us.

Ms. WRIGHTSON. And if DHS piggybacks on the Coast Guard's better efforts in this area, it'll return us to the other issues I raised, which is the sustainability of the resources the Coast Guard has to do this work, and that is a very large list of requirements. And whether or not the Coast Guard has the resources—they always have the will—to do it is a different question.

Admiral HERETH. One other add-on item, sir, if I might? We envisioned an Internet portal available to industry segments, password-protected, appropriately secure, to pass sensitive, but unclassified, information. That's another important link, to share information in a continuing basis with our industry representatives so that we get information quickly about threat—changing threats, threat advisories, threat bulletins that might be useful to various industry segments. And we've done a beta test now in eight ports, and the response has been very positive, so we're going to move ahead and implement such a system. That's part of the Homeland Security Information Net, but it's an Internet portal that will be accessible to industry.

Senator INOUYE. Well, I thank all of you for the service you're rendering to the Nation. Thank you very much.

Thank you, Mr. Chairman.

The CHAIRMAN. Senator Rockefeller?

STATEMENT OF HON. JOHN D. ROCKEFELLER, U.S. SENATOR FROM WEST VIRGINIA

Senator ROCKEFELLER. Thank you, Mr. Chairman.

A couple of thoughts, questions. You have, on the—Mr. Skinner, you have—on the first page of your GAO highlights, you have this interesting statement, "This testimony makes no recommendations, but cites several reports in which recommendations were pre-

viously made." In view of what I've been hearing this morning, I find that very worrisome.

The—I would understand, I guess, that inspectors general are meant to, sort of, comment on the state of matters, but the state of matters strikes me, in all of this discussion, as one of the more depressing conditions of moving forward toward homeland security at the port level that I could have possibly imagined. And I wonder why it is that you—Ms. Wrightson, you referred to having made recommendations to one of the panelists, but you can't make recommendations to the public——

Ms. WRIGHTSON. Oh, no, that is an incorrect interpretation.

Senator ROCKEFELLER.—or to the Congress.

Ms. WRIGHTSON.—OK. That's a very good question. But what the sentence really means is that there are no recommendations contained in this written summary statement; however, on page 32 of the statement, there follows three pages of detailed recommendations that we have provided in prior reports and are publicly available in the backs of each of the individual reports we used to prepare my statement and they are recommendations for improvements in all of the problem areas I cited.

So, for example, in the program that the Admiral and I were just talking about, GAO recommended an—to take better advantage of the management-information system, to develop clearer guidance to the ports, and to facilitate—adopt DOD practices that might assist in facilitating stakeholders to fill out their applications. So——

Senator ROCKEFELLER. Previous——

Ms. WRIGHTSON.—there's a huge——

Senator ROCKEFELLER.—GAO recommendations——

Ms. WRIGHTSON.—list of recommendations, and they're public.

Senator ROCKEFELLER. Previous.

Ms. WRIGHTSON. Well, some of them were issued very recently; all are outstanding and need to be completed by the responsible agencies.

Senator ROCKEFELLER. All right.

Ms. WRIGHTSON. And you would consider these to be——

Senator ROCKEFELLER. Well, let me——

Ms. WRIGHTSON.—recommendations I'm making——

Senator ROCKEFELLER.—let me——

Ms. WRIGHTSON.—today.

Senator ROCKEFELLER.—I'm just—I'm just a little struck, frankly, by the sort of calmness at the table—at yours, that is, all of you.

Mr. Jacksta, you started out with, kind of, a list of all the good things that are being done. You, sir, were very pleased with what the Coast Guard is doing. And you both talked about what you talked about. But I just——

West Virginia is not a large state, but we have the seventh-largest inland port in the country, and I think that you're about to shift most—a lot of our workers to Louisville. I don't know whether that's true or not. I don't get a—I never have had a feeling about Homeland Security that there was any coordination.

And it may have been that the President was right when he had—his first instinct was not to do it at all, but to somehow figure out another system, that the melding of 22 agencies, or 27, or whatever it was, Mr. Chairman, just wasn't going to work. I—well,

I know we finally did it, and then—and he agreed to it. But it may have been that he was right to be skeptical.

I'm on the Intelligence Committee, as the Congressman was who testified earlier, and it's nothing but a litany of total lack of preparation wherever we turn. And we have this fascination with anything that goes wrong in Afghanistan or Iraq or anywhere else, and, obviously, 9/11 and things that go on even not of that magnitude here, but the concept of preparedness is a uniquely American one, where everybody waits on everybody else. I really believe that. That's not to be—to pick out—on you, in particular, but I think that, generally speaking, people wait for others.

I mean, I don't—this whole question about why grants aren't being used and—well, maybe they're not ready to use them, or they're not cleared to use them, and the waiting lists, and all the rest of it—it just—I'm just struck by the calmness of all of you, and by the, sort of, satisfaction you have as you describe what it is you're doing, even though on your end you're describing some of your frustrations, and then you have, I guess, two pages—32 and 33—of recommendations, some of them being previous.

Are you all hooked up onto the same computer system? "You," 27 agencies? Are you interoperable?

Mr. JACKSTA. There is the exchange of information, yes. CBP exchanges information with the Coast Guard on a regular basis. We have people that are working together, both at our National Targeting Center, as well as at the Coast Guard Intelligence Center, to make sure that the information is, first of all, getting—being looked at and making sure that it's getting out to our offices in the field. We have information provided by other agencies at our NTC. We have the FBI. We have TSA. We have ICE. We have a number of Coast Guard. So, there's people sitting there 24-by-7, working together, exchanging information.

So, I think, sir, there is a sense of urgency that—here, in the sense that we feel that it's important for us to continue to work, to exchange information, to get the equipment out there as fast as possible so that we can do the screening of the cargo and containers. We have systems in place that have the——

Senator ROCKEFELLER. But you can be—but what is it? I've always thought it was about 5 percent of cargo that was getting screened. What did you say it was?

Mr. JACKSTA. Right now, in Fiscal Year 2004, sir, for the seaport-side-of-the-house containers, we screen approximately 5.5 percent of the——

Senator ROCKEFELLER. Yes, 5 percent. I mean, how do you, kind of, live with that? In other words, do you have a chart in your mind which tells you how you get to 15, then to 50, then to 75 percent, then to 100 percent? I mean, do you have a clear idea of what has to be done? In other words, if you're all getting shafted by OMB or—were any of your testimonies cleared by OMB before you gave them?

Ms. WRIGHTSON. We didn't clear ours with OMB.

Mr. SKINNER. No, sir, ours was not.

Senator ROCKEFELLER. You understand the little problem with that, right? In other words, even if you had different thoughts, you couldn't say them, because OMB has to clear them. So, how do

you—before you go to sleep at night, how do you figure out how you're going to get to 25, 50, and 100? Everybody knows Homeland Security is underfunded. Everybody in the world knows it's underfunded. Do you ever take it higher up? You're acting—you're Deputy Director, right?

I'm finished. I'm just—I'm angry. I'm angry, Mr. Chairman. You occasionally get angry; not very often.

The CHAIRMAN. The gentleman on your right is, too.

Senator ROCKEFELLER. Is he? OK.

Senator LAUTENBERG. Thank you very much.

[Laughter.]

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

Senator LAUTENBERG. Thank you, Mr. Chairman.

First, I ask that my opening statement be included in the record as if read.

[The prepared statement of Senator Lautenberg follows:]

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

Mr. Chairman, thank you for holding this hearing on this important subject.

I served on the Port Authority of New York and New Jersey before coming to the Senate in 1983. So I have long been aware of the vital role our ports play in our Nation's economy . . . as well as potential security risks at our ports.

Obviously, the importance of port security increased exponentially after 9/11. The 9/11 Commission warned that we must not make the mistake of assuming that the next attack on our Nation will be the same as the last one. We have invested billions of dollars to improve the security of our commercial aviation system. But I worry that we have not done enough to secure other potential targets—especially our ports. To put it bluntly: we still haven't gotten serious about port security.

Mr. Chairman, our Nation has more than one thousand harbor channels, and 25 thousand miles of waterways serving 360 ports. Obviously, we cannot monitor everything that happens on every one of these waterways 100 percent of the time. But if we were serious about port security, we would focus on the ports and waterways that are most at risk.

Unfortunately, this hasn't been the case. According to the FBI, a two-mile stretch between Port Newark and the Newark Airport is the Number One potential target for terrorists in the entire country. Despite this high risk, New Jersey received only three percent of the port security grants distributed by the Department of Homeland Security last year. This was not nearly enough for a state that has two of the largest ports in the country.

Mr. Chairman, I realize that every Senator always fights for resources for his or her state. But when it comes to Homeland Security, we should place the safety of the American people above pork-barrel politics. The Maritime Security Act that the Senate unanimously approved last year included my legislation adopting a strict risk-based standard for port security grants. Unfortunately, the House never acted on that bill. The DHS Inspector General has confirmed that the Port Security Program did NOT award previous grants on the basis of risk assessment.

DHS recently announced it is accepting applications for a new round of port security grants totaling $140 million. I strongly urge DHS to follow the recommendations of its own Inspector General, and use a strict assessment of risk in determining which requests are granted.

Mr. Chairman, I thank you once again for this hearing. I also thank our witnesses, and I look forward to hearing what they have to say about the urgent issue of securing our Nation's seaports.

Senator LAUTENBERG. I make a note there that I was Commissioner of the Port Authority of New York and New Jersey when I came to the Senate, and I'm very much aware of what the significance is of our ports to our general well-being, $740 billion a year

added to our gross domestic product as a result of that. I'm very much aware. Also I want to commend each one of you for your excellent testimony. I may view things a little differently, because I supply the freneticism and you don't have to, but you do have to supply the facts, as you did, and they were wonderfully constructed, and I commend you.

And one of the things that the group at this table have in common is that, we're all very much supportive of the Coast Guard, the work that you do, Admiral, and the number of assignments that continue to grow. Yet we heard from Mr. Jacksta that the fleet is aged. I'm aware of that, since I'm aged and I have seen a lot of these boats around for a long time. But the fact of the matter is that I don't think that we've given enough resources to this—to our needs.

Mr. Chairman, I think that when we look at where we are, that we fail to recognize that the other front from the Middle East is right here at home, and that we have to spend according to our needs. And we've spent 250—we've appropriated $250 billion so far for the war effort in Iraq—and I'm for it, all the way, in order to do the best we can for our troops and to conclude the task we've taken on there—additonally we're about to add $50 billion in the Defense bill to help the war in Iraq be pursued.

When we look at the home front—and I am reminded—we're fortunate to have distinguished Chairman/Co–Chairman of this Committee, people who have experienced war up front and know what you need to protect yourself, and how you fight. This is the second front. And I remind the distinguished Senator from Hawaii, who wears the Congressional Medal of Honor, that at the time of Pearl Harbor, who lost, I think it is, Senator Inouye, 2,400 people, and on 9/11, almost 3,000 people. This tells us something about where the risk is. It's at home too.

So when we look at what the Coast Guard recommended, Mr. Chairman, for our security needs, we talked about something over $7 billion for the decade. And we're talking about $140 million to be distributed, of which my State of New Jersey, with one of the busiest ports in the country, will likely get 3 percent, $4 million. It just isn't enough money to do the job. And I think Senator Rockefeller indicated that it isn't. We don't recognize the significance. We don't recognize the risk.

As a matter of fact, if you look out here and you see the railroad tracks, and you know that some of those cars carry toxic chemicals; enough, it's said, to endanger thousands of people here; an attack on a plant, a chemical plant in New Jersey, could endanger 12 million people. What if chlorine gas was involved? If chlorine's involved, that's going to be the effect.

And so, Admiral, I ask you, What's the status of your personnel levels now?

Admiral HERETH. We've been about—since 2001, focused on MTSA implementation—port-security work, specifically. We've increased our numbers by about 800.

Senator LAUTENBERG. That's from where? What was the base?

Admiral HERETH. I can't quote you the specific base, but, at our Marine Safety Offices, we probably had 2,500 people; in our group offices, we had another 2,500 people. So, we're now in the process

of homogenizing those to gain some synergy in terms of performance. So, we have a number of folks in the Coast Guard focused specifically on those missions area.

Senator LAUTENBERG. Right. But on the total personnel in Coast Guard, are you familiar with that figure—the total requirement that are being met now by Coast Guard, fully, with its navigation, pollution control, refugee interception, et cetera, et cetera? What——

Admiral HERETH. I can't quote you a figure, sir——

Senator LAUTENBERG. OK.

Admiral HERETH.—we'll get——

Senator LAUTENBERG. I know that you're short, and I know that you've got these old vessels. And I see the guys on the Hudson River patrolling in rubber boats—in rigid-hull boats out there in all kinds of weather.

Mr. Chairman, it's just—we're not doing enough to protect our people in this second front, as I call it, at home, where we see the possibility of disaster all across our country. But we look at it particularly in places that are most obvious. Aviation, we spend a ton of money, and don't do it quite as good as we ought to. And that's part of growing pains. And if one doesn't understand what the transition is from a relatively peacetime structure into the kind of security needs we have, then one is kidding oneself. And we ought to be finding ways to finance the war at home in sufficient terms.

$7.2 billion recommended by the Coast Guard for port security over the next 10 years, and we don't come anywhere near it with $140 million proposed for this year. And we spend—and we're spending over—will have spent at least $300 billion defending Iraq, trying to help them get their institutions, their infrastructure together. Over $300 billion. And what about the ports of New York and Louisiana and across the ocean in Hawaii and Alaska?

Mr. Chairman, we have to look at these problems. These witnesses were excellent. I appreciate your presentations. I thank you, Mr. Chairman, for having this hearing.

The CHAIRMAN. Senator Inouye, any further comments?

Senator INOUYE. No, sir.

The CHAIRMAN. Gentlemen, we thank you all very much, and appreciate your—as Senator Inouye said, appreciate your service. I think you're doing a marvelous job with what you have. I didn't agree with Homeland Security, but we have to pay for what is there now, and the gentlemen are right about that. But it's one of those things. Thank you very much.

We'll now turn to panel two: Ms. Jean Godwin, Vice President, American Association of Port Authorities; and Mr. Christopher Koch, President and Chief Executive Officer of the World Shipping Council.

All of the statements that were filed this morning will appear in the record as though read. And, as a matter of fact, I forgot, I would put my opening statement in the record, as well as Senator Inouye's.

[The prepared statements of Senators Stevens and Inouye follow:]

PREPARED STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

Thank you, Senator Inouye, for requesting to chair this important hearing and for your commitment to the security of our Nation's ports.

I welcome the witnesses who are here today and I thank you for your willingness to appear to discuss the security of our Nation's maritime system. Today's hearing is one in a series of hearings that the Committee has held and will hold to fulfill its oversight responsibilities with respect to port security. The Committee will continue to exercise its jurisdiction over these matters as we work to develop ways to further improve the security of all modes of transportation, including the security of our ports.

While the Coast Guard and TSA have made progress since September 11th to bolster port security, including this Committee's work on the Maritime Transportation Security Act, much more remains to be done. To date, the Department of Homeland Security still has not yet fully implemented the requirements of the Act, and some programs have lagged behind for a variety of reasons. The challenge that we face in securing our ports is assessing vulnerabilities and allocating limited resources in an effective and efficient manner to mitigate those vulnerabilities. We must also do a better job of developing and utilizing technologies to reduce labor costs and to improve our ability to detect cargo that threatens our national security.

Senator Inouye.

PREPARED STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

I would like to thank my friend, Chairman Ted Stevens, for calling this hearing today and for allowing the Committee to exercise one of its most essential duties: oversight of the nation's seaport security system.

Port security is of particular importance to us because our states are entirely dependent upon the uninterrupted flow of maritime commerce. Many still do not realize that the entire Nation's economic livelihood depends on the continuous flow of cargo as well.

Maritime commerce is the lifeblood of international trade, and the United States is the world's leading maritime trading nation, accounting for 20 percent of global trade. Ninety-five percent of our Nation's cargo comes through the ports. Our economy is dependent on our seaports, and whether you live on the coasts or in the heartland, maritime commerce affects the daily lives of every American.

I commend the U.S. Coast Guard, the Transportation Security Administration and the Bureau of Customs and Border Protection, on their progress over the past 3 years in implementing the Maritime Transportation Security Act to make seaports more secure both here and abroad. There is much more that needs to be done, and we must move ahead. We cannot become complacent. We have built a foundation, and now it is time to build the house.

The terrorists that seek to do us harm are cunning, dynamic, and most of all, patient. While they have not successfully struck our homeland since September 11, 2001, it does not mean that they are not preparing to do so. They work 24 hours a day, studying what we do and how we do it. It is imperative that we stay ahead of them. That means we must constantly anticipate, innovate, and plan.

We must continually research and implement the most effective technologies. We must recruit, train and deploy the most skilled security force.

Later today, Senators Stevens, Rockefeller, and I will be introducing the Transportation Security Improvement Act of 2005, and port and cargo security improvements are central elements of this legislation.

Among its port security provisions, our legislation seeks to improve interagency cooperation with the further development of joint operation command centers. It clarifies the roles and responsibilities for cargo security programs, while establishing criteria for contingency response plans to resume the flow of Commerce in the event of a seaport attack.

By setting a minimum floor for research and development funding related to maritime and land security, the bill further encourages the development of effective technologies that detect terrorist threats. Finally, we make the port security grant program more risk-based and allow for multi-year funding of port security projects.

Today's hearing on port security will be the first in a series of hearings on transportation security broadly, as we evaluate ways to further strengthen the security of our ports, our aviation and rail systems, our economy, and our Nation.

I look forward to hearing from our witnesses today on how we can continue to strengthen our maritime security system.

The CHAIRMAN. We'll proceed first with you, Ms. Godwin.

And we're pleased to hear your testimony. Thank you.

STATEMENT OF JEAN GODWIN, EXECUTIVE VICE PRESIDENT/ GENERAL COUNSEL, AMERICAN ASSOCIATION OF PORT AUTHORITIES

Ms. GODWIN. Thank you. Chairman Stevens and Members of the Committee, we appreciate the invitation. And, more importantly, we very much appreciate the leadership and the support that this Committee has shown for security needs and the Port Security Grant Program.

I noticed a lot of passion in your questions. I appreciate Senator Inouye's note at the beginning about the funding disparities, the amount that's going to airports versus seaports. And we know that the Members of this Committee have our interests in mind and are always out looking to try to help us.

As you know, the Port Security Grant Program was established to provide financial assistance to protect our vital ports of entry from terrorism. Since 9/11, ports have invested hundreds of millions of their own dollars to increase their security. While the grant program has provided much-needed support to reimburse ports for some of their security costs, in the first four rounds, as you've heard, federal funding has amounted to only $565 million, which was a sixth of what was requested. The fifth round, announced last week, will provide $141 million, but actually limits eligibility to only 66 designated port areas. I encourage you all to look at the most recent round. I know some of that was done in response to the report criticizing the way that the program was funded. But, essentially, what they have done is decided to say some port areas are not even eligible to try to compete, not even to try to make their case that they deserve funding; and only those who are eligible to even submit applications will be judged.

Through the first four rounds of grants, funds have been provided to coastal states, including Alaska and Hawaii, but the value of the program, of course, is not just to coastal states. With 95 percent of our overseas trade flowing through our ports, all states and all citizens would be negatively affected by a shutdown of our seaports.

This program's been bounced around among various agencies. It started at MarAd. It was moved to TSA. And then, actually, exactly 1 year ago today, May 17th, it officially became part of the DHS Office of State and Local Government Coordination Preparedness. I know that Members of this Committee joined AAPA in raising concerns in the context of that move, to make sure that the Port Security Grant Program would remain a separate line item. And we were all assured at the time that it would. Unfortunately, fast-forward months later, and we've seen the Administration's 2006 budget proposal, which would eliminate our grant program and combine us into a critical infrastructure program, along with trucks, trains, buses, public transit, and energy facilities. This is a proposal that we strongly oppose. We think it's contrary to what this Committee intended last year in the Coast Guard reauthorization bill, which authorized a separate grant program for port security based on MTSA. Just last week, the House Appropriations

Committee voted to reject lumping these together and said that they want to see the Port Security Grant Program remain a separate line item. And we certainly would ask for your support in making sure that that is a Senate decision, as well.

Our economy, our safety, and our national defense depend largely on how we can protect our seaports. According to the 9/11 Commission report, opportunities to do harm are as great, or greater, in maritime as they are at airports. And I've heard several of you reiterate that this morning. We must focus on protection at all seaports, since ports serve as an international border, and an incident at one would surely impact all. Rather than limiting the eligibility, to certain geographic areas—we urge DHS to refocus the program on MTSA while including a cross-check to the critical infrastructure plan.

We also urge this Committee to take a leadership role in advocating for stronger funding for the current Port Security Grant Program in the 2006 appropriations process. The Coast Guard did originally estimate we'd have to spend about $5.4 billion over a 10-year period to comply with MTSA for facility security, and we have urged a funding level of $400 million for FY06.

With cargo volumes expected to double over the next 15 years, seaports across the country are expanding to meet the growing demand for their services, necessitating huge expenditures in infrastructure, equipment, and personnel that top $3 billion a year. Unfortunately, in order to pay for security enhancements, ports may have to divert funds needed to make capital investments to handle this future trade growth. We need the Federal Government to provide its share of security costs—this is a partnership—to make sure that our ports are secure today and will be able to meet the challenges and opportunities of accommodating the world trade needs of tomorrow.

Finally, we'd also like to voice our support for the TWIC program, which you've discussed earlier. We urge increased funding for the program, and also encourage DHS to enact the program quickly. We share some of the frustrations you heard earlier.

We appreciate your leadership. We stand ready to do our part in protecting America. And, again, we urge you to voice your support for a stronger appropriation in 2006 and a separate line item for the Port Security Grant Program.

Thank you.

[The prepared statement of Ms. Godwin follows:]

PREPARED STATEMENT OF JEAN GODWIN, EXECUTIVE VICE PRESIDENT/GENERAL COUNSEL, AMERICAN ASSOCIATION OF PORT AUTHORITIES

Good morning. I am Jean Godwin, Executive Vice President and General Counsel for the American Association of Port Authorities (AAPA). I thank you for inviting us to testify before your Committee on the implementation of the Maritime Transportation Security Act and vulnerabilities that remain in the maritime transportation sector. AAPA is an alliance of the leading public ports in the Western Hemisphere and our testimony today reflects the views of our U.S. members.

Prior to 9/11, security was not a top concern for most ports. 9/11 changed that and Congress and the Administration took quick action to help focus ports on this new risk. Enhancing maritime security and protecting America's seaports from acts of terrorism and other federal crimes is now a top priority for AAPA and U.S. port authorities. Much has been done since 9/11, but more is needed. Protecting America's ports is critical to our Nation's economic growth and vitality, and is an integral

part of homeland defense. Ports handle 95 percent of our overseas cargo by volume, enable the deployment of our military, and serve as departure points for millions of cruise passengers.

Protecting our international seaport borders is a responsibility shared by the federal, state, and local governments, seaports and private industry. The Department of Homeland Security takes the lead in protecting America's ports. This includes programs of the U.S. Coast Guard, the Border and Transportation Security Administration, Customs and Border Protection Service, Immigration and Customs Enforcement, and plant and animal inspection. Ports, for their part, focus on protecting the facilities where this international cargo enters and exits the country. The security blueprint for these facilities is the MTSA and its regulations.

AAPA commends the U.S. Coast Guard for its excellent job in developing regulations and reviewing all facility and vessel plans within a very short timeline. All port facilities were required to have operational port security plans by the end of 2004. These plans established a baseline to protect ports from terrorist threats. As we learn more and start to look at the vulnerabilities identified by the area maritime committees and DHS's intelligence programs, we understand more what needs to be done and make improvements to plans. More sophisticated technology can also help us harden these facilities and enhance communications with first responders. Ports also hope technology will provide a mechanism to decrease the number of personnel required to secure our ports, and enhance productivity in the movement of cargo.

Key to enhancing physical security of ports is the Port Security Grant Program. It was established after 9/11 through the Appropriations process and provides much-needed help to port facilities to harden security to protect these vital ports of entry from acts of terrorism. The program has been authorized in several bills—MTSA and Coast Guard reauthorization—although the program, as implemented, is a bit different from the current authorization bills.

Since its inception, the program has provided $565 million in grants for 1,200 projects, with Congress providing an additional $150 million in FY05. Overall, only one-sixth of all projects have been funded. With 95 percent of our overseas trade flowing through our ports, all states and all citizens would be impacted by a shutdown of our seaports. Agriculture as well as oil are two commodities that are heavily dependent on ports to ensure these products get to market. Imagine the impact of a shutdown of the ports in South Louisiana that handle much of the oil imports and grain exports for this Nation.

The level of funding and policy decisions from DHS have made this program less effective than it could be. The need is great, and in the last round, especially, DHS gave small amounts to numerous projects. Some ports had to wait to finish projects because they did not have the necessary funds to fully complete the project. The Port of New Orleans, for example, got partial funding for four gates rather than full funding for one. The MTSA states that the funds will be distributed in a fair and equitable way. However, DHS is also trying to balance risks and protect critical national seaports (as noted in the Appropriations bill). DHS faced a dilemma—if it funds only the top risks, it leaves a soft underbelly of smaller ports. If it gives a little to everyone, little gets done. The problem seems to be one of historic underfunding. We must have funds to do both—provide the needed resources for big and small ports alike.

These complaints were also echoed by DHS's Inspector General and others. In an attempt to make the grants more risk-based, in the fifth round ODP is expected to focus more on high-risk and vulnerable ports. But the funding level, and partial funding of projects, continues to be a huge constraint to progress.

There is also an inconsistency over what the grants pay for. The MTSA stated grants can pay for salaries, operation and maintenance of security equipment, and the cost of physical improvements and vulnerability assessments. But the program allowed only reimbursement of the last two items. This is due to the low level of funding. The Coast Guard estimated the cost of facility compliance with the MTSA regulations would be $5.4 billion over 10 years. AAPA supports a funding level of $400 million a year, which is significantly higher than the current budget.

And there is a new threat to this vital program. In the proposed FY06 budget, the Administration recommended eliminating the Port Security Grant Program and merging ports into a broad targeted infrastructure protection grant program. This runs counter to the intent of this Committee. Last year, this Committee included a provision in the Coast Guard Reauthorization bill to update the authorization of the program. The Act maintained that there would be a separate program specifically for port security to be based on the MTSA.

The new Targeted Infrastructure Protection Program would lump port security into a program with trains, trucks, buses and other public transit, and chemical

companies and ties these grants to the goal of protecting critical infrastructure based on relative risk, vulnerability and needs. This move would pit an underfunded border protection program (port security) against underfunded domestic protection programs. AAPA has great concerns, and encourages your Committee to voice opposition to this new structure.

Our economy, our safety and our national defense depend largely on how well we can protect our seaports. According to the 9/11 Commission Report, opportunities to do harm are as great, or greater, in maritime as they are at airports. Ports are also the only industry within this new Targeted Infrastructure Protection Program that has a statutory mandate to comply with—the MTSA—and the only one for which there is a congressionally authorized grant program, which was also created by this Committee. A separate line item is essential to ensure that ports continue to be a targeted priority in our country's war again terrorism. Cargo doesn't vote and it is often not fully recognized for the value it provides to this country in state and federal infrastructure plans. While critical infrastructure protection is important, using it as the sole criteria for making decisions on funding for port security is a bad idea. DHS proposes to do this so it doesn't have so many separate grant programs. We don't oppose merging other programs together, just the lumping of ports into this program. Seaports, like airports, are key targets and deserve a separate program.

We must focus on protection at all seaports since ports serve as an international border, and an incident at one would surely impact all ports. The MTSA has a system established to identify risks and vulnerabilities, and while some may question some of the DHS decisions on certain grants, the overall move to tying the grants to the MTSA is one that AAPA supports. This was not done in the first few rounds because the MTSA was not in effect yet. We urge DHS to refocus the program on the MTSA, while including a cross-check to the critical infrastructure plan and to keep this as a separate program, like the firefighter grants.

We also urge this Committee to take a leadership role in advocating for stronger funding for the current port security grant program in the FY06 appropriations process. As noted above, the Coast Guard has estimated that ports would have to spend $5.4 billion over a 10-year period to comply with the new MTSA. AAPA urges a funding level of $400 million in FY06. Recently, the House Appropriations Committee approved only $150 million, which is level funding. There is still much to be done to continue our progress in securing America's ports.

Ports are currently planning for a huge increase in trade in the future. Adequate federal funds will help us avoid an infrastructure crisis in the future. Industry analysts predict that within the next 15 years the approximately two billion tons of cargo that U.S. ports handle today will double. But ports are also challenged by the new security mandates of the MTSA and the need to continue to make improvements. Therefore, ports are using current dollars to pay for security, rather than capital investments needed to handle the future growth in international trade. We need the federal government to provide its share of these improvements now, so that our ports are secure today and will be able to meet the challenges and opportunities of accommodating the world trade needs of tomorrow.

Finally, AAPA would like to voice its strong support for the Transportation Worker Identification Credentialing (TWIC) program, which was authorized in the MTSA. We urge increased funding for this program and encourage DHS to make the necessary policy decisions to implement this program quickly. The MTSA required all ports to control access to their facilities, but our U.S. member ports are still waiting for the TWIC requirements before installing new technologies.

Thank you for inviting us to testify on this critical transportation security issue. Ports stand ready to do their part in protecting America. We urge your Committee to voice your support for a strong appropriation in FY06 for a separate line item for the Port Security Grant Program.

Thank you. I would be happy to answer any questions.

The CHAIRMAN. Mr. Koch?

STATEMENT OF CHRISTOPHER L. KOCH, PRESIDENT/CEO, WORLD SHIPPING COUNCIL

Mr. KOCH. Mr. Chairman, Senator Inouye, thank you for the opportunity to be here.

As we look at the question of maritime security, we find it helpful to break it out into its different components. There's ship secu-

rity. There's port-facility security. There's people—personnel security. And there's cargo security.

The Coast Guard's really done a very good job in dealing with the ships, and with the port facilities. On the people piece, there's been certain restrictions applied. All seafarers coming into the U.S. now have to have their own individual visas.

Mr. Chairman, you started this hearing by asking, "Well, what is it we should do, going forward, that we're not doing today," and I'd like to offer a couple of suggestions.

First is the Transportation Worker Identification Card (TWIC). It's been legislated as a requirement for the maritime sector. Coast Guard and TSA are working on that right now. We understand from the Coast Guard that they expect to have a rulemaking out in July of this year. And this is a necessary element to move forward.

The last piece of the puzzle really is cargo, cargo security, and it's a multifaceted strategy the government has, as you heard from Mr. Jacksta. But the starting strategy here is risk assessment. Customs today screens 100 percent of all containers before they're loaded in a foreign port, before they're put on a ship to be brought to the U.S. That is the strategy we've used, 100 percent screening. They then inspect 100 percent of all boxes they have questions about. As you heard, that's slightly over 5 percent. So, if the core strategy we're using is risk assessment, we have to look at what data is being used to make those risk judgments.

Today what we're using is what's been mandated under the "24-hour rule," the ocean carriers' bill-of-lading information, our manifest. It was a good start. Commissioner Bonner was right to do that. We support that strategy 100 percent. Our observation would be that the ocean carriers' bill of lading is a limited source of information for undertaking effective risk assessment.

Today the foreign exporter or the U.S. importer is not required to give the government any information about the goods they are bringing into the U.S. until after the goods are here. It's our belief that what really ought to be done is, for risk-assessment purposes, the importer should provide its data to Customs before vessel loading, just like the ocean carrier does, so that the National Targeting Center in Northern Virginia that screens all these shipments has the benefit of better, more robust, and more accurate information on those shipments.

Also, as you heard today, the strategy is to inspect 100 percent of all containers coming in, with radiation-inspection equipment. The goal for Customs is to have that done by the end of this year, and they're making very good progress on getting that done. There are some problems in some ports with on-dock rail, as you would have seen in L.A., but, overall, they're making very good progress on that.

Finally, there's the in-transit security piece of the issue. The biggest security vulnerability for containers is when they're stuffed at the foreign origin, but we also have to recognize that we need some measure in place to verify whether containers coming through the system have been tampered with in transit. We have proposed that the government establish a rulemaking to require seal verification on inbound containers, and DHS and Customs are working on that.

We expect that to be out as a rulemaking sometime during the course of this summer. It'll be complicated. It'll be very expensive. But we think it's an appropriate measure, moving forward.

When that's in place, it'll also stimulate and advance technology. We're spending a lot of time looking at technology issues for containers. It's quite complicated. But we do believe that when there's a seal verification requirement, it will, in fact, accelerate technology development, particularly RFID technology, that would or could make some significant improvements, going forward.

So, in terms of answering your question, Mr. Chairman, the three things that we would offer for your consideration that ought to be done: first, get better data for risk assessment for the screening process of the cargo coming in; second, support DHS as it moves forward with the TWIC initiative; and, third, recognize that a seal-verification rule will be in place in the near future, which is also going to be a big step forward.

Thank you.

[The prepared statement of Mr. Koch follows:]

PREPARED STATEMENT OF CHRISTOPHER L. KOCH, PRESIDENT/CEO, WORLD SHIPPING COUNCIL

Introduction

Mr. Chairman and Members of the Committee, thank you for the opportunity to testify before you today. My name is Christopher Koch. I am President and CEO of the World Shipping Council, a non-profit trade association of over 40 international ocean carriers, established to address public policy issues of interest and importance to the international liner shipping industry. The Council's members include the full spectrum of ocean common carriers, from large global operators to trade-specific niche carriers, offering container, roll-on roll-off, car carrier and other international transportation services. They carry roughly 93 percent of the United States' imports and exports transported by the international liner shipping industry, or more than $500 billion worth of American foreign commerce per year. [1]

I also serve as Chairman of the Department of Homelands Security's National Maritime Security Advisory Committee, as a member of the Departmental Advisory Committee on Commercial Operations of Customs and Border Protection (COAC), and on the Department of Transportation's Marine Transportation System National Advisory Committee. It is a pleasure to be here today.

In 2004, American businesses imported 10 million loaded cargo containers into the United States. The liner shipping industry transports on average about $1.5 billion worth of containerized goods through U.S. ports each day. In 2005, a projected 11 percent growth rate means that the industry will handle more than 11 million U.S. import container loads. In 2006, containerized trade growth is forecasted to increase another 10 percent, and we will need to be ready to handle more than twelve million import containers. And these trade growth trends are not expected to stop after 2006.

Consider the requirements of one customer of our industry. Wal-Mart will import roughly 360,000 FEUs (forty foot containers) this year. If you were to place that volume on trucks bumper-to-bumper in a single line, it would stretch 3,750 miles. And those volumes have to be moved efficiently at the same time as L.L. Bean's, Target's, Home Depot's, Ford's, K Mart's, Procter & Gamble's, McDonald's, Hewlett Packard's, General Motors', General Electric's, Whirlpool's, Nike's, Becks Beer, Joe's Hardware Store, and thousands of other shippers.

The demands on all parties in the transportation sector to handle these large cargo volumes efficiently is both a major challenge and very important to the American economy.

At the same time that the industry is addressing the issues involved in efficiently moving over 11 million U.S. import containers this year, we also must continue to address the unfinished task of enhancing maritime security, and do so in a way that doesn't unreasonably hamper commerce.

[1] A list of the Council's members can be found on the Council's website at *www.worldshipping.org.*

The Department of Homeland Security (DHS) has stated that there are no known credible threats that indicate terrorists are planning to infiltrate or attack the United States via maritime shipping containers. At the same time, America's supply chains extend to tens of thousands of different points around the world, and the potential vulnerability of containerized transportation requires the development and implementation of prudent security measures. Like many parts of our society, we thus confront an unknown threat, but a known vulnerability.

What is the appropriate collection of measures to address this challenge?

The Department of Homeland Security's maritime security efforts involve many different, but complementary pieces, including implementing the directives of the Maritime Transportation Security Act (MTSA).

It includes the establishment of *vessel security* plans for all arriving vessels pursuant to the International Ship & Port Facility Security Code (ISPS Code) and Maritime Transportation Security Act (MTSA).

It includes the establishment of U.S. *port facility security* plans and area maritime security plans pursuant to the ISPS Code and MTSA, and the establishment by the Coast Guard of the International Port Security Program (IPSP) pursuant to which the Coast Guard visits foreign ports and terminals to share and align security practices and assess compliance with the ISPS Code.

The Coast Guard's efforts to implement these initiatives are well developed.

It includes the Maritime Domain Awareness program, under which DHS acquires enhanced information about vessel movements and deploys various technologies for better maritime surveillance. The challenge of effectively patrolling all the coasts and waters of the United States is obviously a large one.

The MTSA directives and DHS efforts also include enhanced security for *personnel* working in the maritime area, from the requirement that all foreign seafarers have individual visas if they are to get off a ship in the U.S., to the imminent promulgation of proposed rules on the Transportation Worker Identification Credential (TWIC). Regarding the TWIC, DHS officials have indicated their intent to issue a proposed rulemaking on this issue this summer. At the request of DHS, the National Maritime Security Advisory Committee, after intensive, open and constructive dialogue amongst diverse industry and government officials, approved last Friday a detailed set of recommendations to the Department for their consideration in the development of this ambitious initiative.

And last, but certainly not least, MTSA directives and DHS efforts include an array of initiatives to enhance *cargo security*, which the Committee staff has requested that I discuss. There are several elements and programs that comprise the government's cargo security strategy, and each has a role. This morning I'd like to briefly address the following cargo security issues:

- Cargo Security Risk Assessment Screening
- Radiation Inspection of all Containers
- Enhancing In-Transit Container Security
- The Container Security Initiative
- The C–TPAT Program
- The World Customs Organization
- Container Security Technology

1. Cargo Security Risk Assessment and the National Targeting Center

The stated and statutorily mandated strategy of the U.S. Government is to conduct a security screening of containerized cargo shipments *before* they are loaded on a U.S. bound vessel in a foreign port. The World Shipping Council fully supports this strategy. The correct time and place for the cargo security screening is before the containers are loaded on a ship. Most cargo interests also appreciate the importance of this strategy, because they don't want their shipments aboard a vessel delayed because of a security concern that could arise regarding another cargo shipment aboard the ship.

In order to be able to perform this advance security screening, Customs and Border Protection (Customs or CBP) implemented the "24 Hour Rule" in early 2003, under which ocean carriers are required to provide Customs with their cargo manifest information regarding all containerized cargo shipments at least 24 hours before those containers are loaded onto the vessel in a foreign port. The Council supports this rule. Customs, at its National Targeting Center in Northern Virginia, then screens every shipment using its Automated Targeting System (ATS), which also uses various sources of intelligence information, to determine which containers should not be loaded aboard the vessel at the foreign port, which containers need to be inspected at either the foreign port or the U.S. discharge port, and which containers are considered low-risk and able to be transported expeditiously and without

further review. Every container shipment loaded on a vessel for the U.S. is screened through this system before vessel loading at the foreign load port.

The Department of Homeland Security's strategy is thus based on its performance of a security *screening* of relevant cargo shipment data for 100 percent of all containerized cargo shipments before vessel loading, and subsequent *inspections* of 100 percent of those containers that raise security issues after initial screening. Today, we understand that CBP inspects roughly 5.5–6 percent of all inbound containers (over 500,000 containers/year), using either X-ray or gamma ray technology (or both) or by physical devanning of the container.

We all have a strong interest in the government performing as effective a security screening as possible before vessel loading. Experience also shows that substantial disruptions to commerce can be avoided if security questions relating to a cargo shipment have been addressed prior to a vessel being loaded and sailing. Not only is credible advance cargo security screening necessary to the effort to try to prevent a cargo security incident, but it is necessary for any reasonable contingency planning or incident recovery strategy.

Today, while the ATS uses various sources of data, the only data that the commercial sector is required to provide to Customs for each shipment for the before-vessel-loading security screening is the ocean carrier's bill of lading/manifest data filed under the 24 Hour Rule. This was a good start, but carriers' manifest data has limitations.

Cargo manifest data should be supplemented in order to provide better security risk assessment capabilities.[2] *Currently, there is no data that is required to be filed into ATS by the U.S. importer or the foreign exporter that can be used in the pre-vessel loading security screening process*, even though these parties possess shipment data that CBP officials believe would have security risk assessment relevance that is not available in the carriers' manifest filings, and notwithstanding the fact that the law requires the cargo security screening and evaluation system to be conducted "prior to loading in a foreign port."[3] Today, cargo entry data is required to be filed with CBP by the importer, *but* is not required to be filed until *after* the cargo shipment is in the United States, often at its inland destination—too late to be used for security screening purposes.

Last fall, the COAC Maritime Transportation Security Act Advisory Subcommittee submitted to DHS a recommendation that importers should provide Customs with the following data before vessel loading:

1. Better cargo description (carriers' manifest data is not always specific or precise)
2. Party that is selling the goods to the importer
3. Party that is purchasing the goods
4. Point of origin of the goods
5. Country from which the goods are exported
6. Ultimate consignee
7. Exporter representative
8. Name of broker (would seem relevant for security check)
9. Origin of container shipment—the name and address of the business where the container was stuffed

The Council agrees with this recommendation. The government's strategy today is to inspect containerized cargo on a risk-assessment basis. Accordingly, the government should improve the cargo shipment data it currently uses for its risk assessment. An ocean carrier's bill of lading by itself is not sufficient for cargo security screening. These cargo entry shipment data elements would improve cargo security screening capabilities. If a risk assessment strategy is to remain the core of the government's cargo security system, the government needs to decide what additional advance cargo shipment information it needs to do the job well, and it must require cargo interests, and not just carriers, to provide the relevant data in time to do the advance security screening. While this is not a simple task, a next step forward requiring shipper interests to provide more data on their cargo shipments before vessel loading is appropriate. CBP and DHS officials are currently reviewing this issue.

---

[2] *See also,* "Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection," General Accounting Office Report and Testimony, March 31, 2004 (GAO–04–557T).

[3] 46 U.S.C. section 70116(b)(1). Section 343(a) of the Trade Act also requires that cargo information be provided by the party with the most direct knowledge of the information.

2. Radiation Screening

A particular security concern is the potential use of a container to transport a nuclear or radiological device. While there is no evidence that terrorists have nuclear weapons or devices, or that a shipping container would be a likely means to deliver such a device, the consequences of the potential threat—including those from a low tech "dirty bomb"—are sufficiently great that, in addition to the targeted inspection of containers discussed above, CBP is deploying radiation scanning equipment at all major U.S container ports, with the objective of being able to check every container entering the U.S. for radiation by the end of this year. CBP and the Department of Energy are also working with foreign ports to encourage the installation of radiation scanning technology abroad as well.

We understand that the Government Accountability Office is currently reviewing the effectiveness of the radiation detection equipment being used, which is clearly an important issue.

3. Enhancing In-Transit Container Security

While the most important and challenging container security issue is ensuring that containers are loaded with cargo securely in the first place, it is also important to have a system that can help determine whether a container may have been tampered with while in-transit. In September 2003, the Council, together with the National Industrial Transportation League and the Retail Industry Leaders Association, recommended to DHS that the government promulgate a container seal verification rule as the most practical way to address this issue in the near term. The Maritime Transportation Security Act Advisory Subcommittee of COAC made the same recommendation to DHS last fall. CBP and DHS are currently in the process of drafting proposed regulations on this issue. This will be a costly and challenging rule to implement, but we recognize the need to address this issue and the need for a container seal verification rulemaking.

Some of the more important issues that will need to be addressed in this rulemaking will be: the reporting process to CBP when a seal anomaly is identified, the consequences to the shipment when a seal anomaly is identified, where the seal verification is to take place, and a reasonable implementation time frame that will allow port facilities around the world to develop implementation measures.

4. Container Security Initiative

No nation by itself can protect international trade. International cooperation is essential. For ships and port facilities, the International Maritime Organization (IMO), a U.N. regulatory agency with international requirement setting authority, has responded to U.S. leadership and created the International Ship and Port Security Code (ISPS). These IMO rules are internationally applicable and are strictly enforced by the U.S. Coast Guard. There is no comparable international regulatory institution with rule writing authority for international supply chain security. For a variety of reasons, the World Customs Organization (WCO) has not acquired such an authority.

At the WCO, CBP is working diligently with other governments on a supply chain security framework that can be used by all trading nations. This framework will be useful, but will remain at a fairly high level and will be implemented on a voluntary basis by interested governments. Consequently, U.S. and foreign customs authorities must also create a network of bilateral cooperative relationships to share information and to enhance trade security. This is the Container Security Initiative. The Council supports this program and the strategy behind it.

In March, Dubai became an operational CSI port, and Shanghai and Yantian are expected to become operational soon. When they are, more than 60 percent of U.S. containerized imports will be passing through operational CSI ports, with further program growth expected. The liner shipping industry is fully supportive of these efforts by Customs authorities and hopes the program will continue to expand as expeditiously as possible.[4] A listing of operational, and soon to be operational, CSI ports follows:

[4] On May 9, the Argentine government signed a declaration of principles to become involved in CSI. The expansion of CSI to Buenos Aires will be the first CSI cooperative agreement in Latin America.

Port Name	Total CY 2003 U.S. Import TEUs (000)	Total CY 2004 U.S. Imports TEUs (000)
Hong Kong	1,885.41	1,866.32
Yantian (Shenzhen)	1,603.83	1,982.79
Shanghai	937.34	1,278.50
Busan	891.38	971.49
Singapore	478.73	494.30
Rotterdam	420.90	427.75
Bremerhaven	415.99	392.18
Antwerp	262.21	304.60
Tokyo	250.77	267.53
Laem Chabang	186.68	201.06
Nagoya	169.04	174.94
Le Havre	154.93	139.67
Genoa	153.92	144.57
Le Spezia	143.69	159.67
Kobe	111.13	119.97
Hamburg	110.93	150.01
Algeciras	109.09	81.75
Gioia Tauro	103.96	104.48
Yokohama	82.781	109.02
Livorno (Leghorn)	80.15	92.33
Felixstowe	69.54	69.51
Tanjung Pelepas	64.71	45.96
Durban	41.57	43.94
Port Kelang	41.10	39.26
Naples	40.34	29.88
Southampton	40.28	38.62
Liverpool	38.85	39.37
Thamesport	31.49	32.34
Halifax	26.39	24.38
Gothenberg	17.46	18.81
Piraeus	10.92	11.58
Vancouver	5.74	13.59
Tilbury	5.23	2.56
Marseille	4.40	1.07
Dubai	1.20	1.11
Montreal	0.27	0.72
Zeebrugge	0.08	0.02

37 CSI Ports listed: 9,875.63 TEUs (thousands) to the U.S. in 2004
Total U.S. Imports: 15,805.48 TEUs (thousands) in 2004
37 CSI Ports = 62.48 percent of total U.S. imports

One of the issues that the recent Government Accountability Office (GAO) report on CSI identified was that foreign Customs authorities are not inspecting at the foreign load port all of the containers that CBP has identified for security inspection. There are a number of relevant issues with respect to this finding, but I would note a couple of points.

First, understanding why these containers were not inspected at the foreign ports is very important. For example if it was because local Customs intelligence had good reasons to determine there was not a significant security risk, that fact would be obviously relevant.

Second, building cooperative Customs relationships requires time, commitment and mutual trust. In order for the CBP officials stationed in CSI ports to build trust and relationships with foreign customs authorities, the CBP program must be supported with professional personnel that have long-term assignments to these positions. Foreign customs authorities would have a difficult time building cooperative relationships if the CBP personnel must rotate out of their CSI positions after a short period of time. We understand that this has been an issue in the early phases of the CSI program, and hope that any difficulties CBP may have had in getting qualified, full time people stationed to these positions is being or has been resolved. CBP will need the full support of DHS and the Department of State to ensure an effective and robust CSI program.

Third, we note that the supply-chain-security framework that is being developed by the World Customs Organization (WCO) and is expected to be approved next month, provides an important reinforcing principle that should help the CSI program, namely that the Customs administrations of exporting nations should conduct

outbound security inspection of high-risk containers at the reasonable request of the importing country. This is an international affirmation of the CSI program's principles.

Finally, if CBP ever encounters a foreign customs authority that is unwilling to inspect a container that CBP believes is high risk, it can and should issue the ocean carrier a "Do Not Load" message and that container will not be loaded aboard a vessel destined for the U.S. There is no reason why any container that CBP has identified as "high risk" can't and shouldn't be stopped and inspected before it is loaded aboard a vessel bound for the U.S. If the container is not high risk but still one that CBP wishes to inspect, it can use its discretion to inspect it at the U.S. discharge port.

5. C–TPAT

C–TPAT is an initiative intended to increase supply-chain-security through voluntary, non-regulatory agreements with various industry sectors. Its primary focus is on the participation of U.S. importers, who are in turn urged to have their suppliers implement security measures all the way down their supply chains to the origin of the goods. This approach has an obvious attraction in the fact that the importer's suppliers in foreign countries are beyond the reach of U.S. regulatory jurisdiction. In return for participating in the program, importers are given a benefit of reduced cargo inspection. The C–TPAT program invites participation from other parties involved in the supply chain as well, including carriers, customs brokers, freight forwarders, U.S. port facilities, and a limited application to foreign manufacturers.

C–TPAT has improved the security of importers' supply chains. How much it has improved security is difficult to determine or measure. GAO has produced a critical study of C–TPAT, entitled "Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security." The program is currently under scrutiny by both Congress and DHS. It is facing both fair and unrealistic criticism.

C–TPAT needs to be understood for what it is and what it is not. C–TPAT is a set of voluntary partnerships between CBP and willing industry members. C–TPAT is not a regulatory program. It should not be confused as being one. Nor should it be a substitute for regulations when the government has clear, specific things it wants industry to do to enhance security. The difficulty is that the program is in some respects ambiguous, and perhaps unavoidably so.

It is not a regulatory program, yet critics want specificity, strict enforcement, and penalties for non-compliance—features that characterize regulatory programs.

Its costs can be significant, but its benefits are necessarily limited; parties that are not importers receive no direct benefit from the program.

Its principal purpose is to try to affect the conduct of parties outside U.S. regulatory jurisdiction, yet some expect it to have an effect similar to what would occur if these parties were subject to U.S. regulatory jurisdiction.

It is a program that relies on participants' own risk assessment and allows participant's discretion and flexibility in application of the security standards. At the same time, the program tries to promote uniform and common standards of behavior through generalized "minimum standards."

When COAC posed questions that, in essence, asked what importers should do when some of their suppliers are compliant with C–TPAT standards and some are not, CBP responded in their Frequently Asked Questions that all of an importer's suppliers should be compliant or that the importer must demonstrate an ongoing commitment to get all suppliers compliant. Importers will face situations where they cannot require or ensure that all their suppliers are compliant. On the one hand, one can sympathize with the way the issue is being addressed, because CBP wants to keep pushing for full compliance, and because the program would become much more complicated if each importer's supply chain had to become divided into various levels of compliance or non-compliance. On the other hand, by not differentiating within importers' supply chains, one must either accept or not accept the proposition that each container shipment of a C–TPAT importer is likely to obtain an equivalent lowering of its risk assessment.

C–TPAT is a program that other nations' customs authorities and the WCO are examining and find conceptually attractive, yet its definition, its application and the extent of its utility are still in development and not yet settled here in the U.S. A common, global C–TPAT, "trusted shipper" type system might be a very good idea. At the same time, if many trading nations were to implement C–TPAT type programs in ways that significantly differ from each other, very significant complexities for international commerce could emerge, including the possibility of redundant and duplicative, or even inconsistent, efforts.

These are difficult issues, and one should temper criticism of the program with an appreciation for the fact that CBP has been trying very hard to make the program effectively address significant concerns in supply-chain-security in areas where it has no regulatory jurisdiction. The program is a voluntary, non-regulatory, evolving initiative.

Voluntary Partnerships: C–TPAT tries to provide general guidance for enhancing security with respect to some, but not all, aspects of supply-chain-security. It recognizes that flexibility in application is unavoidable when applied to the tens of thousands of different supply chains around the globe. For example, the new C–TPAT Importer Security Criteria have standards for fencing, facility lighting, and employee background checks and credential checking. C–TPAT importers can agree to communicate this to all their foreign suppliers and to urge their suppliers' compliance, but obviously not every business in the world involved in shipping goods to a U.S. C–TPAT importer is going to have compliant fencing, lighting, etc. This doesn't mean C–TPAT is a failure, or that a C–TPAT importer is a failure if one or more of its suppliers don't conform to the standard, and it doesn't mean that C–TPAT doesn't provide security enhancement. It means that there is an unavoidable degree of variability, imprecision and ambiguity in the program when it comes to its implementation.

Not a Regulatory Program: Many maritime and supply-chains-security issues can be, should be, and are addressed through regulatory requirements, not C–TPAT. For example, vessel security plans and port security plans are regulated by Coast Guard regulations implementing the ISPS Code and MTSA. The data that must be filed with CBP to facilitate cargo security screening must be addressed through uniformly applied regulations. Seafarer credentials and the Transportation Worker Identification Card must be addressed through uniformly applied requirements. Requirements to verify seals on import containers need to be addressed through regulations.

C–TPAT is a program that can try to address matters that are not or cannot be addressed by regulations, such as supply chain enhancements beyond U.S. regulatory jurisdiction, or matters that aren't covered by regulations, such as cooperating with CBP in providing access to information in support of investigative inquiries. C–TPAT may also be a platform from which CBP and program participants can analyze security vulnerabilities and problems and jointly develop plans that could more effectively try to address such situations. C–TPAT, however, should not be used in lieu of regulations when regulations are the more appropriate method to enhance security.

Validation: CBP has a C–TPAT validation program to confirm that participants are doing what they have said they would do, during which identified shortcomings can and should be discussed and remedial measures developed. However, the GAO report has criticized the program for conferring benefits to importers before validation has occurred and noted that the agency does not have adequate trained personnel to validate all C–TPAT participants in a timely manner.

This criticism is certainly welcomed by the private commercial security consulting business, which sees a substantial business opportunity if they can become government sanctioned security validators for C–TPAT type programs in the U.S. and around the world. Whether C–TPAT participants or the government would accept this role, how such a role would be defined and overseen, what the standards would be, whether validation by commercial parties would be required or voluntary—are all issues that are undetermined at this time.

Compliance: C–TPAT is not a regulatory regime, with specific criteria that must be applied to everyone at all times. Some of the program criteria are very general, and its criteria do not cover all aspects of security. Further, a security failure in a specific case may not involve a lack of due care and may not involve a breach of the terms of the participant's C–TPAT Agreement.

Nevertheless, CBP has recently taken the position that it can suspend a C–TPAT participant from the program—

a. Without advance notice, without discussion, and without an opportunity to cure the problem.

b. For matters that are not covered by the terms of the C–TPAT Agreement signed by CBP and the carrier (i.e., you can be kicked out of the C–TPAT program even if you have complied with the C–TPAT Agreement's terms).

c. For any violation of law or significant security breach (e.g., drugs in a container, stowaways in a container).

d. For an undefined duration.

Ocean carriers, which receive no direct benefits from CBP for participation in the program but have written their C–TPAT participation into many of their transportation contracts with shippers, have found this to be a surprising and troubling development at best. Carriers had believed that under a "voluntary partnership" program with CBP, specific security concerns would be jointly assessed to determine what measures could reasonably be taken to address any specific security shortcomings. To face no-notice suspension from a voluntary program that provides no direct benefits for events that may be highly unpredictable and under the control of third parties will significantly change the program and how it is perceived.

Evolving Initiative: C–TPAT is an evolving initiative, and industry and government will learn and adapt as it matures. For example, when the Sea Carrier portion of C–TPAT was formulated, there was no ISPS Code or Coast Guard MTSA regulation regarding vessel and port facility security plans, so C–TPAT carriers recognized the regulatory void and agreed to undertake a number of voluntary measures in this regard. Today, there are comprehensive Coast Guard regulations on these issues, and it is no longer appropriate for CBP to use C–TPAT to address the issues that the Coast Guard is addressing through its regulations. Similarly, carriers agreed in C–TPAT to participate in the electronic Automated Manifest System (AMS) for transmitting manifest information to CBP; at the time, paper manifest filings were possible. Now, electronic filing in AMS is required by regulation.

The future role of ocean carriers in C–TPAT will require further consideration and analysis. Carriers, unlike importer's foreign suppliers, are regulated parties, and CBP and the Coast Guard can and have established clear, uniformly applicable rules for them to follow. Furthermore, C–TPAT program benefits, which are basically less frequent cargo inspections, are importer benefits. Ocean carriers do not receive direct benefits from CBP for C–TPAT participation. How and where ocean carriers may fit in the program going forward remains to be seen.

As regulated entities, ocean carriers have a preference for clear, uniformly applied security regulations when an issue can be addressed through regulations. At the same time, we wish to continue to work with CBP and other DHS agencies to determine if there are appropriate ways to supplement the regulatory security regime. This will continue to require a partnership approach, clear communications, and mutual benefits.

Looking Ahead: C–TPAT is not the supply-chain-security strategy for the government—it is one layer and one piece of the evolving strategy. At the same time, the program's critics have points that won't be ignored. For example, it is difficult to believe that C–TPAT is presently sufficiently developed to actually be used as a determining criteria for what cargo would be allowed to be transported if the government had to respond to a terrorist incident involving a containerized cargo shipment, because, among other things, there is uncertainty about whether all the suppliers in an importer's supply chain comply with adequate standards that warrant such confidence.

However, it is conceivable that the program may be able to attain this kind of result if the foreign suppliers that actually stuff the containers were included in the program. The fact that foreign manufacturers (except some Mexican manufacturers) and the parties stuffing the containers are not in the program means that the most important parties in container security aren't C–TPAT program participants. Could this be addressed by adding foreign manufacturers to the program?

Perhaps so, if C–TPAT were to be able to evolve from a program that gives benefits to U.S. importers if they undertake certain actions, to a program that would give those benefits to shipments where both the U.S. importer and a foreign manufacturer or container stuffer were certified as compliant with the appropriate standards. Is there a way for a program that is constrained by resources to achieve this additional extension? Perhaps yes.

CBP, under Commissioner Bonner's leadership, has been diligently developing international supply chain security standards at the World Customs Organization, and has undertaken discussions with the European Commission and various national governments. There is a possibility to develop these efforts into a more advanced, agreed internationalization of supply-chain-security improvements

6. The World Customs Organization

In some respects, the issues surrounding the C–TPAT program are similar to those that the World Customs Organization (WCO) has been grappling with since it established a special Task Force on Security and Trade Facilitation in 2002.

Currently, the WCO is finalizing a Framework of Standards to Secure and Facilitate Global Trade that is expected to be approved at the WCO Council next month. This initiative intends to establish international standards for Customs-to-Customs cooperation concerning cargo risk assessment, advance cargo information filing and

common risk criteria, and for Customs-to-business partnership programs, like C–TPAT.

The establishment of international security standards and criteria for international supply chains and international cargo shipments is a sound and logical objective. The challenge, however, continues to be how to obtain implementation of such agreed-upon standards and criteria in the absence of a binding international instrument. The framework and its supporting documents are expected to be approved by the WCO Council through a recommendation that invites WCO members to implement it in accordance with individually established timeframes and each member country's capabilities. Thus, rather than early international acceptance and implementation of the framework, we could see the framework serve as a inducement for the establishment of bi- and multilateral Customs agreements where individual Customs authorities agree to cooperate on the establishment of joint risk assessment programs, the advance filing of common cargo information and perhaps also on the mutual recognition of each other's partnership programs. To the extent such individual Customs agreements were to cover a "critical mass" of global trade, they could eventually establish the minimum standards that all trading nations would have to implement or risk seeing their export opportunities being curtailed.

Such a development would not happen over night. Nor would the attendant benefits for business in terms of mutual recognition and simplified and uniform filing requirements. But absent an international regulatory mechanism for supply chain and cargo security, it appears to be the only currently available option internationally for creating uniformity and commonality.

As noted earlier, however, it may also be a way for the C–TPAT type system to be extended to foreign manufacturers in those nations that make a serious commitment to establish and oversee C–TPAT type programs. Today, a U.S. importer is expected to "ensure" that a foreign supplier is following C–TPAT criteria—a pretty tough challenge. If reliable foreign authorities were to certify foreign manufacturers according to standards and procedures equivalent to CBP's certification of importers, confidence in enhanced security and shipper compliance could be greatly enhanced. This may not work in all nations, but it is certainly not inconceivable to see the U.S. accepting other responsible government program certifications of their manufacturers, and foreign governments' accepting U.S. certification of theirs. This model works for ships, where foreign government certifications are accepted (but also buttressed by strong U.S. port state enforcement), and it could be considered for supply-chain-security.

7. Technology and "Smart" Containers

Technology clearly has a role in increasing the efficiency and security of containerized cargo shipments. X-ray and gamma ray non-intrusive container inspection equipment is being deployed at U.S. and foreign ports, as are radiation portal monitors and radiation detectors.

In addition to these developments, there is a discussion of "smart" containers. What makes a container "smart," however, and what the appropriate technologies may be for such an objective remain unclear.

The Council and its member lines have been working within the International Standards Organization RFID container technology working group on standards for electronic container seals, container tags and shipment tags. We expect that, once a seal verification requirement is imposed by U.S. regulation, these technologies will be seriously considered as an automated, efficient way to determine if containers have been tampered with while in transit.

There is also a discussion about the possibility of the application of shipper-applied "container security devices" (CSDs). The CSDs currently being tested by CBP only indicate whether one of the container doors has been opened. A properly applied e-seal may provide equivalent functionality. Explanations of what a CSD should accomplish vary, and a clear definition has not yet emerged. Furthermore, other issues about CSDs that have not been adequately addressed, including the radio frequency to be used and whether it would be compatible with the emerging ISO standard's frequency for e-seals, who would read the devices, how would they know which boxes have CSDs to be read, where they would be read, who would be expected to build and operate the reading infrastructure, what would be done with the information, the devices' reliability and accuracy, and what would be done with exception reporting.

There is also discussion of a "next generation" or "Advanced CSD" with more sophisticated sensors that DHS is researching, which will also need to address a number of issues, including what specifically is it that needs to be "sensed," the accuracy and reliability of the device, its cost, who applies the device, the reading infrastruc-

ture that would be needed, who would read it when and where, and the protocols for how different readings would be addressed by whom and when.

The idea of transforming containers into "smart," impregnable fortresses clearly has an appeal. Reality, however, requires addressing issues of: technology definition and standards; false positives from sensor technologies and their consequences; questions about device reliability; maintenance complexity; device failures and equipment out of service time; power needs and failures, including battery life issues; device costs; and labor issues and costs. In addition, technology can bring new security vulnerabilities that have to be considered. For example, permanent or reusable container security technology devices would require a capability to "write" new information into the device or amend existing information in the device. Such a capability would require a wide range of parties around the world to be given the capability of writing new information into container security devices, which would create troubling security vulnerabilities of third parties becoming capable of "hacking" into the devices. It is for this very reason that the ISO electronic seal standard will require that e-seals be one time use seals without the capability to write or change the information in the seal.

As different technology vendors jockey for position, some things are becoming clearer:

1. Industry and government need to cooperate and agree on what the security requirements are, and what the respective implementation roles of industry and government would be.

2. Cost does matter. A decision to invest in a particular technology applicable to the global container industry will be expensive and will require assurance that government is not likely to abruptly change requirements.

3. Whatever technology is chosen for application to international containerized cargo shipments, it will need to be a common, universally deployable technology.

4. Proprietary solutions that require a particular manufacturer's product or reading system will not be acceptable.

5. Technology vendors who push products that involve the vendor capturing, managing, and profiting from all the data generated from the device—and there are a number of these—are likely to encounter hard questions, if not strong resistance, from industry.

Cargo shipment data is the data of the carrier and the shipper, and with consent, their agents. It is appropriate for the importing and exporting nations' governments to have access to this data, but it is not appropriate for third parties to try to use technology to capture it and resell it to other commercial interests. Vendors who try to do this will need to address a number of policy and legal issues.

Summary

When addressing the issue of international supply-chain-security, we find ourselves dealing with the consequences of two of the more profound dynamics affecting the world today. One is the internationalization of the world economy, the remarkable growth of world trade, and the U.S. economy's appetite for imports—a demand that fills our ships, our ports, and our inland transportation infrastructure, a demand that will result in more than 11 million U.S. import containers this year, and more than 12 million next year, and a demand that will increasingly test our ability to move America's commerce as efficiently as we have in the past.

The other dynamic is the threat to our way of life from terrorists and the challenge of addressing the vulnerabilities that exist in the free flow of international trade, even when the specific risk is elusive or impossible to identify.

Finding the correct, reasonable balance between prudent security measures and overreacting in a way that impairs commerce is a tough challenge.

We are making real progress in addressing these challenges, but that the effort to address them more effectively must continue. In particular, it would be helpful to develop a blueprint or framework that identifies the specific security gaps and security requirements in the supply-chain-security system, so that government and industry can all understand, target and prioritize the development of appropriate solutions needed to address the appropriate, correct, and agreed requirements.

DHS continues to refine and extend its maritime and cargo security regime. This year we expect to see major rulemakings dealing with container seal verification requirements and with the issuance of Transportation Worker Identification Cards, a Departmental determination of what additional cargo shipment data needs to be

given to CBP to enhance the cargos security screening system, and a continued review of the C–TPAT program.

Mr. Chairman, the World Shipping Council and our member companies believe that there is no task more important than helping the government develop effective maritime and cargo security initiatives that do not unduly impair the flow of commerce. We are pleased to offer the Committee our views and assistance in this effort.

The CHAIRMAN. Well, thank you very much.

One of the things that was of interest to me when I went to Los Angeles was the enormous growth of waterborne imports into the U.S. I understand the economic analysis of that, it's about $40.5 billion a year coming into our ports. But, contrary to the passengers on airlines, and contrary to any other system that we've got, that is entirely free from any contribution to the security aspects we're talking about. I'm told that a 4.3 percent fee, similar to one this Committee has imposed upon airline passengers, of twice that much, would bring in at least $1.7 billion annually.

Now, what do you say about that? Why shouldn't these imports contribute to the cost of this security? Why should we constantly take it from tax money? That's what we're talking about, these additions, these amounts that each witness has asked for this morning, in effect, more money. But why not get it from the fees on these imports, like we tax the American passengers as they fly on the airlines?

Ms. GODWIN. There are fees assessed at—by ports at the local level. You're correct, there is no national or federal fee imposed on cargo that's specifically dedicated to security. There are a lot of other federal fees and taxes, obviously, on maritime——

The CHAIRMAN. Those fees that——

Ms. GODWIN.—cargo that go into the general treasury, and Customs duties attributable to maritime commerce. But a number of ports have assessed fees individually at the port for security enhancements at that particular location. And——

The CHAIRMAN. Yes, I understand they're starting that in L.A., but I don't think they've reached that magnitude, and I don't think many of the costs involved, even in the Los Angeles port, are federal costs. Having the local areas increase their revenue does not help us meet the demands that we've heard here today.

Ms. GODWIN. That's true. But when the port is collecting fees they are using it to reimburse their own costs, in terms of operations and maintenance and personnel costs, which aren't even eligible for the Port Security Grants at this point. But there are a number—as I said, a number of other federal fees and taxes attributable to maritime commerce. No amount of that funding is dedicated to security. It's just not set aside for security. I know there have been proposals discussed to take a portion of Customs duties, for example, that's collected on maritime commerce, and to set that aside to pay for security enhancements.

The CHAIRMAN. The Customs inspection fee on a cruise ship is $2 per passenger. I know of no similar fee paid to the Federal Government from imports coming into the United States.

Mr. Koch?

Mr. KOCH. Mr. Chairman, it's a fair question, but I think, really, here's where I would propose you start the analysis. The Coast Guard's analysis of what its vessel and port-facility regulations

were going to cost the industry was $8 billion over 10 years, so industry will be spending $8 billion to comply with the MTSA regulations. That cost estimate does not include the cost of the foreign flag vessels' compliance with the Coast Guard regulations. It does not include foreign ports' compliance with the ISPS Code regulations. So, there are many billions of dollars already being spent.

When looking at what additional federal funding needs to be done, I think there really needs to be some clarity as to: What would we be spending the money for? And that has been a debate that has been vaguer than it should be. It's easy to talk about how much money should be given to ports. The real question, as you heard from GAO earlier today, is, What is the money actually needed for? All port facilities today are compliant with the ISPS Code the MTSA regs. So if we're going to go ahead and look to tax commerce an additional amount, I think there really needs to be clarity given to specifically what is it that the money is going to be spent for and is there a way to make sure that the money that would be collected actually is spent on those things?

The CHAIRMAN. Well, as you know, the money that comes from air cargo, domestically, is taxed at 6.25 percent. And that goes into the FAA trust fund. We could very easily, on this Committee, create a similar trust fund. These aren't taxes, these are fees paid on cargo, and it goes into the FAA trust fund created by this Committee. I'm seriously thinking about asking this Committee to create a trust fund for port security. That would be augmented, I'm sure, by federal expenditures, augmented by other expenditures made by the ports themselves. But I—there's no question that the system needs more money, but when we faced that problem with air commerce, the passengers and the cargo paid the fee, a substantial part of it.

Senator Inouye?

Senator INOUYE. Mr. Chairman, you are absolutely correct. Right now the Administration is requesting a huge sum of money based upon passenger security fees.

My question is a very broad one. You have given us some of your problems and some of your suggestions. You have now been working on this since September 11th. Are we in better shape today, or no change at all, or worse?

Mr. KOCH. I think we're clearly in better shape. Are we where we want to be? No. I think the programs Customs has launched, in terms of the risk assessment, CSI, C–TPAT, have all enhanced security. The Coast Guard's missions in dealing with vessel security and port-facility security clearly have enhanced security. Access control is much better.

Our improvements must also recognize the volumes of containers we are moving. Last year it was 10 million import containers; this year, it'll it be over 11 million; next year, it'll be over 12 million. So, we see this enormous expansion of world trade and all the cargo moving, and we have to figure out how to improve security efficiently.

We're trying to deal with this tension between efficiently handling huge volumes of cargo and dealing with the terrorist risk to free trade and free societies. It's a very interesting cross-section of conflict.

I think we're doing well. I think we clearly need to do better. I think both AAPA and ourselves have offered suggestions to the government on how to do that, and it's going to be an ongoing effort. But improving risk assessment, improving CSI, improving overseas inspections, further deployment of the radiation inspection equipment, not only here, but abroad, all are things that will be helpful. It's going to take a little time to get there, but we are making clear progress.

Senator INOUYE. Following up on the Chairman's questioning, when we improve our security, and when we improve our process and expedite movement, a major beneficiary would be those foreign shippers. Don't you think they should pay a little fee that could bring this about?

Mr. KOCH. Well, my observation is, they are paying more today for security. A number of ports are charging security fees. Carriers are trying to pass on their costs to shippers through higher rates. The terminal operators are passing on their higher costs. So the market already is building in increased costs that are being passed on to shippers.

And, as the discussion we've had with Senator Stevens, if there are specific things that the government needs to assess a fee on for enhanced security, I think shippers would look at that. I think the frustration that has existed in this debate, up to this point, has been a generalized discussion of, "Let's spend more money," without tying it clearly to, "Spend it for what?" And it's the "spending it for what" that is the harder question, because everybody understands we need to enhance security, but the question is—let's not just create a trust fund that's a generalized trust fund that doesn't have specific needs that there's a consensus should be funded through that kind of mechanism.

Senator INOUYE. I believe it would be very helpful to the Committee if you could provide us with a report on what sort of fees that these others are paying. Because I have no idea. And what the load is like. If we did, we might think differently. That would be extremely helpful.

And, Ms. Godwin, what did you think of the Inspector General's report, the fact that it takes so long for security clearance and that some of the grantees were really not prepared to receive grant funds?

Ms. GODWIN. I think there are some very legitimate points that came out in the report. Our members have been concerned about the security-clearance issue, as well. In terms of the time lag for the grant money to be spent, I know one of the issues is that when you fill out an application to receive a grant, it's essentially an outline of what you might propose to do. You type it in on the computer. There's a limited amount of space. It's not a very detailed proposal. Once you are approved to receive a grant, there's a period of time, over months, where the sponsor—the Port Authority, in this case—might be negotiating with the Department of Homeland Security to refine that proposal, to get some specific amounts, how the money would be allocated, to really get a more definitive grant proposal approved. And once that is approved, they start the process of bidding out contracts. So, there is a fairly long time lag before the money is actually spent.

Senator INOUYE. Have you been called upon to provide an input on the process itself?

Ms. GODWIN. We've been consulted by DHS off and on in a number of different areas. I can't say that we are at the table when these decisions are being made, but they have reached out to us.

Senator INOUYE. Thank you very much.

The CHAIRMAN. Senator Vitter?

STATEMENT OF HON. DAVID VITTER, U.S. SENATOR FROM LOUISIANA

Senator VITTER. Thank you, Mr. Chairman.

Ms. Godwin, I have some concerns about the process and how those funds are distributed. Am I following things right and understanding under that new program 66 ports are eligible and there for small ports are pretty much excluded.

Ms. GODWIN. Sixty-six port areas are eligible. It depends. There may be more than one port that's within a mile of a navigation channel. But, yes, it is a limited universe of potential applicants. Their initial starting point for creating that list was based on volume, they started with the largest, in terms of volume, 129 ports in the country, based on the Corps of Engineers' data. There are a lot of ports that have less volume that are left off that list. That's correct.

Senator VITTER. From a Louisiana perspective, what I'm particularly concerned about is this focus on volume, which leaves out a lot of oil-and-gas service-related ports—for instance, in south Louisiana. Now, one of those ports that I can think of—literally one, Port Fourchon, accounts for servicing 20 percent of the Nation's oil and gas production.

Ms. GODWIN. Right.

Senator VITTER. Do you think that's a little skewed, the fact that there is this focus on volume that doesn't take into account the significance of the port activity, like that related to energy production?

Ms. GODWIN. I think that would be a good example, that would illustrate why cutting off those who can even apply in the first place is probably not the best way to look at risk—you know, risk-based decision-making. People ought to be able to come in and file an application and make their case on why they should be eligible for funding, and explain the risk-based factors about that port. Looking strictly at volume, as a starting point, and then applying a formula to that, you may see some ports left off the list that don't make any sense if you actually had the specific facts about that port.

Senator VITTER. Well, I would agree with you. And I think Fourchon, in Louisiana, is a great example, because it will never be ranked high in volume, because it's not a cargo, sort of, volume-based port; it's a port that services the oil and gas sector. And if it were shut down tomorrow, we would feel it the next day, in terms of energy availability and prices.

More broadly, could you comment on the FY05 application process as it relates to the Inspector General's findings and the 9/11 Commission Report?

Ms. GODWIN. I think they've tried to make an effort to address some of the issues that came up in the Inspector General's report.

I know one of the criticisms was having more clearly-defined criteria of how the local Captain of the Port would assess a project versus how the National Review Team would assess a project, and trying to resolve some of those areas of confusion. But we were, to be honest, caught by surprise at the idea of limiting the applicant pool in the first place.

Senator VITTER. OK. And that fundamental limitation, would you consider that basically an unfunded mandate for everybody's who's off the list?

Ms. GODWIN. It's definitely an unfunded mandate. And I remember, when I was here for the hearing that this Committee had in February, a number of Senators spoke very eloquently about the need to protect all airports in this country, not just the largest airports. And certainly the same case could be said for ports. We do not want to leave a soft underbelly somewhere in this country by a kind of arbitrary ranking. That doesn't mean that risk-based decision-making isn't perfectly appropriate, but you have to look at it in the entire context, and not prevent people from being able to at least compete for the funding and make a case.

Senator VITTER. OK. And the last question for both of you, What are your comments about the proposed consolidation of the port-security program into an overall infrastructure-security grant program?

Ms. GODWIN. As I'm sure you heard in my statement, we are adamantly opposed to it. We are thrilled that the House Appropriations Committee has taken a stand, and we strongly encourage the Senate to do the same.

Senator VITTER. Right.

Mr. KOCH. Sir, we don't really have any comments on that.

Senator VITTER. OK.

All right. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much, Senator. Glad to see you.

Senator Rockefeller?

Senator BILL NELSON. Oh, he's not here.

The CHAIRMAN. Pardon me.

Senator Bill Nelson?

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

Senator BILL NELSON. For me to be mixed up with Senator Rockefeller is, indeed, a privilege, Mr. Chairman.

[Laughter.]

Senator BILL NELSON. Mr. Chairman, having grown up in Florida on the tales and the stories of the swashbuckling days of pirates of the Caribbean, unfortunately we're starting to see a reoccurrence of those pirates of the Caribbean. We're seeing several instances that have happened off of Brazil, off of Venezuela, and off of Colombia.

And Jane's Defence Weekly, is indicating to us that new evidence shows that terrorist organizations are entering the fray with terrorists and insurgents using the sea as a launchpad for brutal acts to move operatives and to smuggle drugs and counterfeit goods to fund their operations. And it goes on to say international terrorists

are now operating in piracy areas, adopting the techniques and acts of pirates or franchising their cause to local insurgent groups.

The Caribbean's an area that I have considerable concern about port security, from the standpoint of several of the ports that I've visited in the Caribbean, and that they are supposed to be secure ports, and, in fact, they are not.

Now, with the added dimension of piracy adding to our question of defense of the homeland, I'd like to have your comments.

Mr. KOCH. Senator, I don't have direct information that would be terribly insightful on specific countries. I do know the Coast Guard has established the International Port Security Assessment Program, whose purpose is to go to these foreign countries, do assessments of the foreign port facilities, determine if they're complying with the international rules and the Coast Guard's expectations, and trying then to help them if they are not meeting them. You might want to ask the Coast Guard what their assessments have been throughout the Caribbean and at their particular places there.

I know, from the liner-industry perspective, I'm not aware of particular acts of piracy that our members have encountered in the Caribbean. There are certainly the drug cartels and cargo theft in some parts of Central America, which has clearly been a problem in the past, and it's one we're always vigilant about. But in terms of the port-security piracy issues, I suspect the Coast Guard may be able to give you some data that would not be something I could.

Senator BILL NELSON. Well, I'm interested in the answer from your standpoint. How about the port authorities, Ms. Godwin?

Ms. GODWIN. The ports in the Caribbean? I mean, they're supposed to all be in compliance with the ISPS Code. I am not aware of any that have been found not to be in compliance.

Senator BILL NELSON. OK. I can tell you they're not. And if the American Association of Port Authorities doesn't know that, then I'm concerned about it. And if the World Shipping Council doesn't know that, I'm concerned about it. Because with as little that we inspect the inbound cargo containers, and if these foreign ports are not in compliance, it seems like we've got a big hole right there.

Mr. KOCH. The Coast Guard, at the present time, has identified five jurisdictions that do not have adequate port security. I believe they're African ports. To the best of my knowledge, they have not identified any in the Caribbean, at this point. If they are not compliant, then the Coast Guard needs to put them on the list saying that they are not compliant, and that needs to be put into the Customs Targeting System so that cargo coming through those ports is targeted appropriately, as well as the vessels.

Senator BILL NELSON. OK. And then, on the basis of your answer, Mr. Chairman, what I'm going to do is proffer a number of questions to the Department of Homeland Security on this issue, because of the lack of compliance, why they're saying that these ports have complied, when, in fact, there's a huge hole in the safety net that we're supposed to be extending out beyond.

All right, let's talk about tamper-resistant containers. You know we're trying to put seals on containers. Why don't you give me the value of your opinion there?

Mr. KOCH. We have advocated a seal-verification rule. One is being drafted at the present time by Customs and the Department of Homeland Security. Our expectation is that that rule would require that, before a container is loaded in a foreign port for the U.S., that we will have to go verify the seal on that box. We support that, support the elements that will have to go into that rulemaking, including defining the standard of the seal and the various responsibilities of the parties to do all that. It's a big challenge, but we think it does make a lot of sense.

When that is in place—that obligation is in place—we will expect technology to be coming forward rather rapidly to help us implement that. We have been spending a lot of time investigating RFID electronic seals for containers. We don't have, yet, a standard for that technology in place that can identify the frequency and the various parameters to make it work, but we expect, by the end of this year, that that standard should be in place, and, with a seal-verification rulemaking, we'd start seeing electronic seals being put on boxes sometime in the foreseeable future.

Senator BILL NELSON. Ms. Godwin?

Ms. GODWIN. I'm not sure I can add anything to that. That's certainly an important component of cargo security, and we're hoping to see progress in that area.

Senator BILL NELSON. OK. And I will send those questions to the Department of Homeland Security, as well as questions with regard to their progress under a new law on cruise ships, that they would have to check the manifest before the cruise ship leaves the port. They had 180 days in which to implement this new law that I had a little bit to do with. We are now at day 151 of the 180 days, and I will—would like to have a written response on how they are progressing, since it's getting near the time for implementation.

Thank you, Mr. Chairman.

Senator INOUYE [presiding]. Thank you very much.

Before I call this adjournment, I'd like to announce that the record will be kept open for 2 weeks. If any of the witnesses wish to provide addendum or corrections, please feel free to do so. Some of the Committee Members are not here, but they have submitted questions, which we will forward to you, and we hope that you will be able to respond to them.

Our next hearing will be held tomorrow morning at 10 o'clock. At that time, we will receive testimony on the nomination of senior officials of the Department of Commerce.

Thank you very much.

[Whereupon, at 11:45 a.m., the hearing was adjourned.]

A P P E N D I X

WORLD SHIPPING COUNCIL
Washington, DC, June 14, 2005

Hon. TED STEVENS,
Chairman,
Senate Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Mr. Chairman:

I would like to thank you for the opportunity to testify before the Commerce Committee on May 17th regarding port, maritime and cargo security issues. The World Shipping Council, which represents the international liner shipping industry serving America's international trade, appreciates your continued oversight and leadership regarding enhancing maritime and cargo security while facilitating the free flow of legitimate commerce into and out of the United States.

One of the issues that was briefly discussed during the hearing was port security funding. As you know, during the last Congress, Senator Hollings proposed a port security container tax as an amendment to the 2004 Maritime Transportation Security Act (S. 2279). This amendment was opposed by 76 organizations, including the World Shipping Council. representing virtually every facet of U.S. maritime commerce, and the amendment was rejected during committee markup of the bill. We very much appreciated your support in opposing that amendment.

During the May 17th hearing, you asked the industry panelists, namely myself and Ms. Jean Godwin of the American Association of Port Authorities, to comment on the concept of establishing a new tax or fee on import cargo containers to pay for port security expenses. While I commented briefly on this issue during the hearing, I would like to offer the following additional comments, for inclusion in the hearing record, which I hope will assist the Committee in considering this issue.

In my oral response to your question during the hearing, I noted that, although some interests have advocated for increases in the total amount of annual Port Security Grant monies dispersed by the Federal Government, no one has yet clearly or specifically defined what it is that additional federal port security funds should appropriately pay for.

U.S. port facilities and the vessels that call on them are in compliance with the International Ship & Port Facility Security Code (ISPS Code) and the Maritime Transportation Security Act (MTSA) security regulations promulgated by the U.S. Coast Guard. Port facilities and vessels have developed and implemented approved security plans. In fact, we are not aware of a single, major U.S. port or port facility that is not currently in compliance with the Coast Guard's maritime security requirements.

The costs of implementing these security requirements have been significant. The Coast Guard has estimated that it will cost U.S. port facilities and flag vessels $8.8 billion over 10 years; however, these compliance costs are already being borne by the industry. There is no need for a new tax and a new federal funding program to address these costs.

The Coast Guard's cost estimates are the costs that would be borne by the industry to comply with its maritime security requirements, not the cost the Federal Government would bear. These cost estimates were actually on the low side. as they did not include the costs incurred by the thousands of foreign-flag vessels that were required by the Coast Guard's regulations to become certified under the International Ship and Port Facility Security (ISPS) Code or the costs incurred by foreign ports and port facilities in becoming compliant with the ISPS Code.

In addition to the costs to comply with required vessel and port facility security requirements, the maritime industry and its customers have expended substantial sums to comply with the requirements of the U.S. Government's cargo security programs. U.S. Customs and Border Protection (CBP) estimated that the cost to industry to comply with the Trade Act advance cargo information filing requirements

would amount to over $4.7 billion. Those estimates did not, however, include the millions of dollars of costs incurred by ocean carriers to implement the agency's 24 Hour Rule advance manifest filing requirements. Second, U.S. importers, ocean carriers, truckers, railroads, air carriers, brokers, and freight forwarders, among others, have expended millions of dollars each year to voluntarily implement the security requirements of the Customs-Trade Partnership Against Terrorism (C–TPAT) program. And third, later this year, the maritime industry will face another very expensive security requirement when CBP issues rules requiring installation and verification of high-security seals on all import cargo containers.

The purpose of stating this is not that the liner shipping industry is complaining about these costs. We understand the need to develop and implement prudent, enhanced maritime security measures in the fight against terrorist threats. It is important to recognize, however, that substantial costs are already being borne by the maritime industry to address and improve maritime security, and we see no basis for imposing a new, additional federal security tax on the industry.

Today, Federal agencies levy 127 taxes and fees on the maritime industry, collecting roughly $22 billion per year. Approximately $20 billion of this amount is collected in Customs fees that are not earmarked for specific purposes and are deposited in the General Fund of the Treasury. We believe that creation of an additional federal tax or fee on maritime cargo containers would be unjustifiable given the substantial revenue generated through existing taxes and fees and given the substantial expenditures the industry is already incurring to comply with new security rules.

In short, port, vessel and cargo security requirements, are currently being met and their costs borne by the maritime industry. We have seen no explanation of what unmet port security costs would justify a new federal tax. Furthermore, we note that ports have the authority, and are using their authority, to impose additional charges at the local level when such measures are needed to cover additional security costs. For example, the ports of Charleston, Savannah, Portland (Oregon), Hampton Roads, New Orleans, Houston, Mobile, Los Angeles and Long Beach have increased the fees on commerce in their port to raise additional revenues for security measures. There is no need or justification for a new federal tax to cover costs already being paid for by the industry.

Thank you for the opportunity to comment further on this important issue.

Sincerely yours,

CHRISTOPHER L. KOCH,
President/CEO.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO RICHARD L. SKINNER

Question 1. I understand you are currently conducting work on CBP's Automated Targeting System (ATS). When do you expect to have that report completed? Would you be able to testify before this Committee on that report when it is completed?

Answer. Our report, "Audit of Targeting Oceangoing Cargo Containers" (OIG–05–26), which is designated FOUO, will be released to the Congress on July 26, 2005. A public summary will be released on August 2, 2005. We would be happy to testify on our work.

Question 2. I appreciate the work your Department did on the Port Security Grant Program as it provided many insights into some of the program's problem areas that we continue to conduct oversight of and are working in consultation with the Department to rectify. I realize the guidance for this year's round of port security grants was just released last week. Have you had an opportunity to review the Department's guidelines and assess if your recommendations are being implemented?

Answer. We are reviewing the Department's FY 2005 Port Security Grant Program Guidelines and Application Kit, and evaluating the complex funding allocation model for the program, which we received earlier this month. We are encouraged by the substantive changes to the design of the program reflected in these documents. However, while it appears that substantive changes are imminent, we have not evaluated the effect of these changes—the criteria program administrators will use and how they will apply it during the evaluation process—and whether those modifications satisfy our recommendations.

We are awaiting additional details from the Department supporting its action plan in response to our recommendations. The Department has not yet provided its internal guidance that SLGCP, USCG, TSA, CBP, IAIP, and MARAD representatives will use to evaluate projects, namely, the field evaluation criteria and the National Review Process guidance. We intend to discuss the revised port security grant

application review process with program officials after reviewing this information. Upon completing our analysis, we will communicate the status of the recommendations to SLGCP.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO RICHARD L. SKINNER

Question. Your office found major problems with the port security grant program, mainly that funds are not being distributed on the basis of security risk. Have you performed any follow-up to ensure that the $140 million DHS will distribute this year won't have the same problems?

Answer. In our final report transmittal, we requested that DHS advise our office within 90 days of its progress in implementing our recommendations. In its action plan, DHS outlined steps already taken and other significant changes planned for the next round of port security grants. In addition to the Department's action plan, we are reviewing the FY 2005 Port Security Grant Program Guidelines and Application Kit, and complex funding allocation model for the program. We are encouraged by the substantive changes to the design of the program reflected in these documents. However, while it appears that substantive changes are imminent, we have not evaluated the effect of these changes—the criteria program administrators will use and how they will apply it during the evaluation process—and whether those modifications satisfy our recommendations.

We requested additional documentation in order to better understand how DHS is modifying the port security grant application review process. The Department has not yet provided its internal guidance that SLGCP, USCG, TSA, CBP, IAIP, and MARAD representatives will use to evaluate projects, i.e., the field evaluation criteria and the National Review Process guidance. We intend to discuss the revised port security grant application review process with program officials after reviewing this information. Upon completing our analysis, we will communicate the status of the recommendations to SLGCP.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO JEAN GODWIN

Question. Do you have any concerns with the recent guidance announced by DHS to award this year's appropriations of port security grant funds?

Answer. Yes, AAPA is very concerned over the recent changes in the program. Of most concern is the change to limit eligibility to the largest risk ports. DHS preselected 66 ports which are eligible for this 5th round. Nearly half of the U.S. port authorities that AAPA represents are no longer eligible for this program. The Port Security Grant (PSG) Program was established to help ports harden their infrastructure and to comply with the improvements required under the Maritime Transportation Security Act (MTSA). The language in the law call for a "fair and equitable allocation" of funds. AAPA believes that limiting eligibility is in conflict with this provision of the law. All port authorities must comply with the MTSA, and continual improvements at some ports will stop without federal help. All should be eligible.

While AAPA agrees that the program should be risk-based, we believe the definition of risk must be broadened from what we see this last round. A group of underprotected ports is also a risk to this Nation, especially in terms of importing weapons of mass destruction or smuggling in terrorists. These facilities are all international borders. The program should take into account national economic, strategic defense, regional transportation systems, availability of alternative systems to deliver critical cargos, the importance of a port's mission to federal agencies such as the Department of Defense and Department of Energy, the proximity to other terrorist targets and loss of life. The grants should go to fund security improvements to implement Area Maritime Transportation Security plans and to make improvements to facility security plans, and should not limit eligibility.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO JEAN GODWIN

Question. Given the President's budget cuts and fiscal restraints, how are we going to effectively protect our ports, particularly with respect to the port security grant program?

Answer. Each year only a small part of the homeland security federal spending is devoted to help port facilities increase security. In FY05, Congress appropriated only $150 million for the Port Security Grant Program. AAPA recommends a funding level of $400 million. In terms of priorities, maritime security is a very high priority, but far more funds go to state and local program for response and training programs. While these are important programs, prevention should be this country's first job. And maritime security, because of the economic impact of ports, their cruise and ferry passengers, and national defense assistance, should be a high funding priority. A re-allocation of priorities within the budget is the best way to address this issue. Some have proposed a fee on maritime commerce. However, the maritime industry already pays billions of dollars in user fees and taxes to the Federal Government, including $17.5 billion Customs duties collected in fiscal 2003. If a dedicated source of funding is required, AAPA believes that Customs duties should be used as a source.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO MARGARET WRIGHTSON

Question. In your report on the Transportation Worker Identification Credentialing Program, you found several problems with implementation to the program, not the least of which was the lack of a comprehensive project management plan. Do you know if TSA has satisfied this recommendation?

Answer. In July 2005 DHS provided us with an update on the actions that had been taken to implement the recommendations contained in our December 2004 report on TSA's efforts to develop the Transportation Worker Identification Credential (TWIC). In this update, DHS stated that TSA had "significant program management controls in place for the prototype program" including a Program Management Plan, a Project Quality Assurance Plan, and Risk Assessment and Mitigation Planning among other things. However, DHS did not provide any supporting documentation for us to determine whether these controls and plans collectively constitute what could be considered a comprehensive project plan for managing the remaining life of the project.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO ROBERT JACKSTA

Question 1. Last year, I successfully got included a provision in the Intelligence Reform bill that applies to cruise ships the same standards that we apply to airlines with respect to terror watch lists. My provision requires that the Department of Homeland Security check all passengers and crew manifests against the consolidated passenger watch list before they board the ship. This is vital to the security of our cruise passengers as well as to the security of our ports and the surrounding areas. It will take only one incident to cripple the cruise industry. Similarly one incident, no matter how small, can severely interrupt international commerce. I would like to know how the implementation of this cruise ship watch list requirement is progressing. The law gave DHS 180 days to implement this program. We are going on 151 days as of today. Will DHS comply with this deadline? When can I expect a briefing on the full implementation of this law?

Answer. The Advanced Passenger Information System (APIS) Final Rule (70 FR 17820 April 7, 2005) requires vessel operators to provide passenger APIS. Under the Rule, operators must submit passenger information according to the following criteria: 96 hours prior to arrival at a U.S. port for voyages over 96 hours; 24 hours prior to arrival at a U.S. port for voyages less than 96 hours; prior to departure from foreign for voyages less than 24 hours; and 15 minutes prior to departure for vessels departing the U.S.

Vessel Crew and Passenger APIS manifests are vetted against law enforcement databases maintained within the TECS/IBIS mainframe and against the anti-terror watch list, which is exported to the TECS/IBIS mainframe from the Terrorist Screening Center. In lieu of an automated notification mechanism, the CBP National Targeting Center (NTC) actively vets APIS lists to identify passengers or crew who are arriving or departing aboard commercial sea vessels. The NTC coordinates the identification, interception and examination of targeted passengers with the U.S. Coast Guard.

The vessel time requirements within APIS reflect Coast Guard regulations and were written to establish continuity between agency reporting requirements. Commercial cargo and passenger vessels board passengers and crew several hours in advance of departure. Due to the extended time needed to board a passenger vessel

or prepare the vessel to sail, CBP has determined the time requirements published within the Coast Guard regulations serve the purpose for targeting suspect high-risk passengers and crew.

CBP would welcome the opportunity to discuss the implementation of this program in greater detail. Please have your staff contact Thaddeus Bingel, Assistant Commissioner for Congressional Affairs at (202) 344–1760 to arrange a briefing on the implementation of APIS for passenger vessels.

Question 2. It is crucial that we stop dangerous cargo from reaching our shores at all. Once the cargo gets here our chances of stopping a catastrophic event are greatly reduced. We need to push our borders out and catch dangerous cargo before it leaves the home ports. However, odds are high that we will not catch everything. So we need to be able to track cargo and know as quickly and efficiently as possible if the containers have been tampered with en route. What technology is DHS looking into to maintain and ensure the integrity of the seals on the containers?

Answer. DHS is currently exploring technology designed to enhance the integrity and security of oceangoing containers, rather than the seals that are affixed to such containers. The majority of seals currently used by shippers and importers are mechanical and are not able to interface electronically with the verification process. As the technology incorporated into electronic seals (e-seals) is developed and matured, it is anticipated that such e-seal capability could be used to maintain the integrity of not only the seals but also the containers to which they are affixed. The International Organization for Standardization (ISO) is in the process of developing the accepted standards for e-seals and their use.

Question 2a. Are GPS tracking systems part of the technology?

Answer. DHS Science and Technology Directorate (S&T) is working with Customs and Border Protection (CBP) to identify and evaluate technology designed to enhance the security of ocean going containers. Such Advanced Container Security Devices (ACSDs) shall be designed to integrate with the Marine Asset Tag and Tracking System (MATTS), a tracking and communication system that would provide container-tracking capability. This technology has application to assist CBP in tracking in-bond shipments and is extensible to rail and truck transport.

Question 2b. What are the expected costs to the private industry to employ any new technologies?

Answer. Based upon current technical capabilities and rate of maturation, the cost to private industry to employ new technology that is presently under evaluation is, on an average, no greater than 50 dollars per trip over the projected 10-year average life of the container. As technology continues to develop and mature, however, it is anticipated that such costs would decrease significantly.

Question 2c. What is the time frame for deploying the next generation of container seals?

Answer. CBP is working in conjunction with DHS/S&T on the development of next generation container security technology. S&T recently issued a Broad Agency Announcement for its Advanced Container Security Device Program. This effort will result in the issuance of DHS-wide standards for next-generation Container Security Devices that provide:

- six-sided intrusion detection and alerting,
- a means for increased visibility of stuffing and transit history,
- enhanced data and information for the CBP's National Targeting Center (NTC) and the port of arrival, and
- timely reporting and communications.

Additionally, as a part of the ACSD Program, S&T has a parallel Research and Development effort for capability integration into the container, to optimally push container security development to the container manufacturers.

In managing this process, S&T has established an Integrated Process and Product Team (IPPT), which includes representatives from DHS, Department of Defense, and the Department of Transportation, to ensure a wide voice among federal agency stakeholders and to prevent development of a solely S&T solution.

A development period of approximately 3 to 5 years may be required to produce an operationally suitable and technically robust ACSD solution fulfilling the above objectives. As an immediate step, CBP has launched the "Smart Box" initiative to evaluate the logistical and operational aspects of using container security devices for intrusion detection. The Initiative's near term goal is to approve a device that would monitor and log door activity for inclusion in CBP cargo security programs. The Smart Box focuses on the testing of "off the shelf" Container Security Devices (CSD) to help address the current threat of container tampering en-route.

Question 3. I am very concerned about the Caribbean Basin area and port security. The safety and security of ports in the Caribbean Basin have a direct impact on Florida and the rest of the Nation. A significant amount of trade goes back and forth between ports in Florida and Latin America and this trade is only expected to increase in the coming years. It is crucial that the seaports that are closest to our own borders are secured. This is a particular challenge in this area because of the well-established drug trafficking routes throughout Latin America. We need to do something to address this issue and we need to do it now. We need to ensure that goods originating from these ports are safe and secure and do not pose a threat to the U.S. One way to do this, as you all at DHS have shown, is through programs like the Container Security Initiative. Many don't think about the Caribbean basin as a real security risk. In this week's Jane's Defense Weekly, however, there is an article about piracy and it maps the number of acts of piracy by region. In 2004, there were 14 reported acts of piracy just off the shores of Columbia, Venezuela, and Brazil. That is a significant number of incidents. Piracy not only poses an immense threat to the safety of the crew aboard these cargo vessels but can be an avenue for terrorists to get to our shores with deadly weapons without being detected and without having to go through the normal Customs channels. We cannot forget about the Caribbean Basin ports—these ports that are so close to our own shores. How many and which Caribbean Basin ports are currently out of compliance with the MTSA regulations or the ISPS Code?

Answer. Federal regulations to ensure the security of domestic seaports is governed by the Maritime Transportation Security Act (MTSA) and the International Ship and Port Facility Security (ISPS) Code addresses the security of international seaports. Information regarding specific port compliance with MTSA and ISPS regulations is the responsibility of the U.S. Coast Guard (USCG). It is the practice of USCG to advise CBP regarding MTSA non-compliant ports. CBP incorporates this information into the Advanced Targeting System (ATS); the ATS evaluates the risk associated with all U.S.-bound shipments to determine appropriate screening and inspection responses.

CBP has long-standing institutionalized relationships with U.S. trade operations, such as the Port and Terminal Operators through the Business Anti-Smuggling Coalition (BASC), in the Caribbean Basin. BASC is endorsed by the World Customs Organization (WCO) and is active with the Organization of American States (OAS) on Port Security and Supply-Chain-Security Initiatives. Although BASC initially had an anti-narcotics focus, terrorism has now been incorporated into their profile and security standards. At present, BASC has expanded to include: Mexico; Guatemala; Jamaica; Ecuador; Panama; Venezuela; Peru; Uruguay; the Dominican Republic; Costa Rica; Haiti and El Salvador. In each of these countries, Port and Terminal Operations remain vital segments of the supply chain that actively participate in BASC.

CBP is exploring further expansion of the Container Security Initiative (CSI) with Latin America and the Caribbean, namely in Argentina and in Brazil, with plans to conduct assessments in the Bahamas, Colombia, Jamaica. Honduras, and Panama.

Question 3a. What is DHS doing to ensure the integrity of goods and containers coming into the U.S. via the Caribbean Basin ports other than just penalizing shippers who do not comply with our regulations?

Answer. Customs and Border Protection (CBP) is looking at expanding the Container Security Initiative to Central America and South America. In South America, CBP has signed Declarations of Principle with Argentina (May 9, 2005) and Brazil (May 24, 2005) to become the first two South American ports to participate in CSI. CBP has scheduled a capacity assessment for Cartagena, Colombia for the first week in August 2005. In Central America and the Caribbean Basin, CBP has completed capacity assessments in Puerto Cortes, Honduras; Kingston, Jamaica; and Freeport, Bahamas to determine their viability in being able to support CSI. CBP will be scheduling a capacity assessment of Colon and Balboa, Panama in the near future. CBP will determine by these capacity assessments if any of these ports would be able to support a CSI program.

As part of DHS's multi-layer cargo security approach, the Science and Technology Directorate (S&T), in coordination with Customs and Border Protection (CBP), is developing technologies the ensure the security of intermodal shipping containers, such as the Advanced Container Security Device (ACSD) and the Marine Asset Tag and Tracking System (MATTS), which will actively monitor the integrity and track containers globally.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO REAR ADMIRAL LARRY HERETH

Question 1. The Port of Seattle in my state is one of the Nation's largest and most diverse port complexes. It is a major container and cruise ship port, home to the Alaska fishing fleet, supports tens of thousands of ferry riders each day and the city is one of the most sought-after tourist destinations in the world. The port is also located only blocks away from a bustling downtown. Do you believe the Coast Guard has enough resources to adequately protect a thriving port city like Seattle?

Answer. The Coast Guard does not individually possess the resources to protect an entire port such as Seattle, but works in concert with other federal, state and local authorities, as well as the port community, to protect the port. Even so, risks to any port cannot be completely eliminated. The Coast Guard is working with the port community to focus resources on reducing the greatest risks to the port.

The Coast Guard has built a strong foundation of effectively working with the maritime industry through our historical enforcement of safety and environmental protection regulations. Our Captain of the Port activities and local enforcement of regulations resulted in many well established relationships in the port community, and many venues in which to engage local stakeholders such as Port Security Committees, Port Readiness Committees, Harbor Safety Committees and OPA 90 Area Committees.

The Coast Guard also implemented regulations from the Maritime Transportation Security Act (MTSA) of 2002 on July 1, 2004. These regulations require, among other things that industry have in place vessel and facility security plans, which are tested and approved in accordance with established Coast Guard standards. These efforts have been enhanced through Congress's funding of 791 FTP in the 2005 budget for nationwide MTSA implementation.

Since 9/11, the Coast Guard has also created or acquired new or enhanced Maritime Homeland Security Capabilities including:

- 12 Maritime Safety and Security Teams.
- 15 Additional Coastal Patrol Boats.
- 80+ new Response Boats.
- The Navy has agreed to transfer five Patrol Coastal boats (PC–170s) to the Coast Guard this FY05. The Navy has agreed to continue most maintenance responsibilities on these Patrol Coastal boats for four years (through FY08).
- 8 Canine teams trained for explosive detection.
- 30+ Field Intelligence Support Teams (FIST) deployed to better collect and disseminate maritime threat information.
- Before 9/11 we had no mandatory ship-tracking requirement; we have recently forged an international agreement to accelerate the requirement for Automatic Identification System (AIS) capability. Simultaneously, we have initiated a major acquisition project for AIS. This project will allow us to deploy immediate capability, including AIS shore stations in VTS ports and aboard Coast Guard Cutters, outfitting NOAA buoys offshore and testing AIS receiving capability from a low-flying satellite. The Coast Guard has also fielded AIS at nine U.S. VTS ports and persuaded the world maritime community to accelerate AIS installation on ships.

Specifically, in Washington State

- MSST 91101 was stood up, consisting of 74 active duty and 33 reserve personnel.
- 9 Additional billets were added to conduct Port State Control and MTSA Implementation.
- 4 Additional Coastal Patrol Boats (4 of the additional 15 acquired) were homeported in the Puget Sound area.
- Deployed FIST.

Question 1a. What has the Coast Guard done since 9/11 to ensure its homeland security and other missions are accomplished in this bustling hub of commerce for the Pacific NW and the Nation?

Answer. Since 9/11, we have made great progress in securing America's waterways, while continuing to facilitate the flow of commerce. The improvements in Ports, Waterways and Coastal Security (PWCS) that are currently evident are, in large part, attributable to the passing of the watershed Maritime Transportation Security Act of 2002 (MTSA) legislation and its swift implementation by private industry and the Department of Homeland Security (DHS). This has vastly changed the

security posture of the Nation's maritime critical infrastructure and key assets (MCI/KA) and the overall preparedness of federal, state, local and private security forces. The Coast Guard is committed to a course that improves our maritime security with the ultimate goal of preventing the exploitation of, or terrorist attacks within, the U.S. Maritime Domain. Doing so requires a threat-based, risk-managed approach to identify and intercept threats before they reach U.S. shores. The Coast Guard accomplishes this by conducting layered, multi-agency security operations while strengthening the security posture and reducing the vulnerability of MCI/KA, with an increased focus on the Nation's most militarily and economically critical ports. As the Coast Guard seeks to reduce maritime risk, it must strive to balance its PWCS mission requirements with other Coast Guard non-security missions to ensure no degradation in those missions. The Coast Guard must exercise its full suite of authorities, capabilities, competencies, and partnerships to accomplish its full spectrum of missions in the post-9/11 world.

The Coast Guard is continuing to meet the challenges of our legacy missions in the Puget Sound region, as well as meeting the new challenges presented by our integration into the Department of Homeland Security and new homeland security mandates. Implementation of expanded security responsibilities is being built on the foundation provided by our existing marine safety, port security and maritime law enforcement missions, and broadens our efforts to reduce risks in the U.S. Marine Transportation System and to enforce laws and treaties. Although much work remains, we are progressively improving maritime homeland security.

The diversity of Puget Sound's maritime industry presents unique challenges that require daily cooperation between industry and government to balance the needs of commerce with those of homeland security. The security net vital to limiting vulnerabilities in Puget Sound ports consists of layered security measures that rely on the successful implementation of the MTSA and the International Ship and Port Facility Security (ISPS) Code. Implementation of MTSA and the ISPS Code were major activities during 2004. Security measures are in place for domestic and foreign vessels, domestic waterfront facilities and Puget Sound as a whole. We also maintain a Maritime Safety and Security Team (MSST) in Seattle. It was the first MSST established, and provides an expanded capability for port safety and security operations.

One of the foundations for improving maritime security is the Area Maritime Security Committee (AMSC) required by MTSA regulations. Facilitated by the U.S. Coast Guard, the Puget Sound AMSC consolidated existing port security committees and a committee that had been formed to represent Washington State Ferries and their unique concerns. The AMSC has established communications links across law enforcement and emergency response entities, identified public and private sector capabilities and responsibilities, and established a regular schedule of meetings, training and exercises to foster maintenance and continuous improvement of security measures in place to protect the port.

The AMSC is coordinating all federal, state, local and private sector maritime security efforts in Puget Sound. The 25-person AMSC encompasses a wealth of maritime knowledge, and draws talents from all aspects of industry, police and fire departments and from components of the Department of Homeland Security. Collectively, they advise the Federal Maritime Security Coordinator on security concerns and critical commercial interests unique to Puget Sound. We continue to build upon these efforts to provide rigorous maritime security for the Puget Sound region.

Question 2. There is talk about imposing fees on imports to cover the cost of port security. My concern is that some import ports are located near Canada or Mexico where infrastructure is either developed or being developed to compete with the U.S. ports for import goods. I am concerned that any fee will simply drive import goods to these other countries, especially Canada, which has a well-developed shipping and rail infrastructure. Once the cargo is diverted, it will enter the U.S., possibly by rail, and not receive all the protections it may have been subject to had it come through a U.S. gateway. This obviously undermines our security and our economic mission. In addition, as our economy in the Pacific Northwest finally is overcoming years of recession, this is not the time to cause important port business to be diverted to Canada. How do you purpose to address a scenario where U.S. security fees might send U.S.-bound import goods to these other countries causing them to receive less security scrutiny?

Answer. CBP does not propose to add any additional fees for security or regular cargo exams.

Question 3. There has been talk since shortly after 9/11 about requiring shipping containers from overseas to be equipped with mechanisms that verify that they were securely loaded and not tampered with before reaching U.S. shores. My colleague

and friend, Senator Murray has implemented pilot programs to determine the best technology to accomplish this. What needs to be done to ensure these containers are safe before entering the U.S.?

Answer. Container security is multi layered and cross-functional and requires the commitment and resources of not only the U.S. Government but also the importing community. The addition of technology designed to ensure the integrity of containers bound for U.S. shores is but one facet in securing containers. Such technology must work in conjunction with mechanical seals and sealing processes to be utilized at the point of stuffing through trusted, vetted partners such as the C–TPAT members.

Manifest data provided by the shippers and importers are a critical component to this layered approach in order to conduct targeting of potentially high-risk containers. The Container Security Initiative (CSI) provides an additional layer as such targeting is conducted at overseas locations prior to containers being laden aboard U.S. bound vessels.

The use of Non-Intrusive Inspectional (NII) equipment, such as large-scale non-intrusive inspection imaging technology and radiation portal monitors is also critical to both ensuring the integrity of containers as well as in expediting the inspection and movement of legitimate freight.

Question 3a. What more can be done in this regard and what specifically does the CG, or other branches of the Department of Homeland Security, have planned in this regard?

Answer. The Coast Guard is an active participant in Operation Safe Commerce. which is a DHS grant program testing a host of technology solutions for intermodal container security in the international supply chain. The Coast Guard is a member of the Executive Steering Committee for that project. The results of Operation Safe Commerce will help determine which technologies are mature enough to be considered for mandatory use on containers bound for the United States.

The Coast Guard is also working closely with Customs and Border Protection on the development of a proposed rule that would require the mandatory use of high security mechanical seals on containers bound for the United States. The rule is being drafted to allow the introduction of advanced technology to be incorporated with the mechanical seals as those technologies develop.

The Coast Guard is a member of the Container Security Integrated Product and Process Team (IPPT), co-led by the Science & Technology Directorate (S&T) and the Border and Transportation Security (BTS) Policy & Planning Office, which provides oversight to the development and evaluation of advanced technologies for intermodal shipping containers, such as the Advanced Container Security Device (ACSD), and for the development of the Container Security Systems Architecture.

Question 4. In your testimony to the House Transportation Subcommittee on Coast Guard and Marine Transportation on June 4, 2004, you had stated that all Area Maritime Security Plans were approved by June 1, 2004 and they would be fully implemented on or before July 1, 2004. Has this happened? If not, what is the current status of implementation and how many plans have yet to be approved?

Answer. Yes, all of the Area Maritime Security Plans have been completed, approved and implemented.

Question 5. At the time of the testimony you provided to the House Transportation Subcommittee on Coast Guard and Maritime Transportation on June 4, 2004, the Coast Guard had completed Port Security Assessments at 19 of the 55 most significant military and economic ports in the U.S. Today you state that all 55 have been completed. Can you please provide a list of any Washington State ports that were included in this figure and any other information as it relates to their respective assessments?

Answer. Port Security Assessments (PSAs) have been conducted in Seattle, Tacoma and Vancouver, Washington. These PSAs included waterway assessments of Puget Sound, Elliott Bay, Blair Waterway, Rich Passage, Budd Inlet and the Columbia River. In these areas 16 facilities and vessels were assessed from a Terrorist Operations Perspective, identifying vulnerabilities and recommending mitigating strategies. The assets visited included cruise ships, passenger ferry terminals and vessels, oil terminals, chemical terminals, bulk cargo terminals, locks and bridges. The results of the assessment are categorized as Sensitive Security Information and not public record information. However, the information is appropriately shared with those that have a need to know in law enforcement agencies, select members of the port's Area Maritime Security Committee and each individual owner/operator of the facility or vessel.

Question 6. In your testimony to the House Transportation Subcommittee on Coast Guard and Maritime Transportation on June 4, 2004, you state that, "In im-

plementing the Maritime Transportation Security Act (MTSA), the Coast Guard identified approximately 3,200 marine facilities that could be involved in a Transportation Security Incident. Nearly all of these facilities have since conducted a self-assessment and submitted a facility security plan to the Coast Guard for approval." Has the Coast Guard completed review of the remaining facility security plans? If not, how many have yet to submit a facility security plan to the Coast Guard for approval?

Answer. All required facility security plans were approved by the target date of December 31, 2004. After a detailed review for content at the National Facility Security Plan Review Center (NFSPRC), local Coast Guard Captains of the Port (COTPs) approved the plans individually following compliance verification examinations of each applicable facility. In all, approximately 3,200 facility security plans were reviewed and coordinated by the Coast Guard's NFSPRC.

Question 7. What is the status of the Coast Guard's schedule to have Automatic Identification System (AIS) capabilities at each Vessel Traffic Service and when do you think that this long-term goal of nationwide AIS coverage will be completed?

Answer. The Coast Guard has installed the Automatic Identification System (AIS) in all Coast Guard Vessel Traffic Services (VTS) as of November 2004. This capability provides AIS coverage within each VTS' area of responsibility. The Coast Guard has also a chartered Major Systems Acquisition project to establish a nationwide AIS surveillance network to support all Coast Guard missions. Eventually, the entire coastline, the Great Lakes and the Western Rivers will be covered by AIS under this project. The current schedule calls for nationwide AIS coverage to be fully complete in 2010.

Question 8. As you know, ensuring the security of our Maritime domain is a critically important component of our economy. Securing the Maritime domain is an effort that must be orchestrated with each and every one of our Nation's trading partners. We must be assured of the contents and security of shipments as they leave foreign ports destined for the U.S. In your testimony, you state that the Coast Guard continues to assess the effectiveness of antiterrorism measures and implementation of the International Ship and Port Facility Security code requirements. You state that "10 countries are scheduled for visits by June 2005 with the goal of visiting all of our approximately 140 maritime trading partners." Which countries are included in the list of 10 to be visited by June 2005? When does the Coast Guard estimate that an assessment will be conducted on all 140 maritime trading partners?

Answer. As of July 2005 the Coast Guard has visited 29 countries including: Algeria, Argentina, Australia, Bahamas, Chile, Columbia, Dominican Republic, Ecuador, Equatorial Guinea, Gabon, Guatemala, Honduras, Hong Kong, India, Jamaica, Japan, Mexico, New Zealand, Panama, Peru, Philippines, Singapore, South Korea, Thailand, Trinidad and Tobago, Tunisia, Turkey, Uruguay and Venezuela.

The Coast Guard estimates that an assessment will have been conducted on all 140 maritime trading partners by December 2007.

Question 9. As you know, the Transportation Workers Identification Card has played an important role in port security by enhancing identity verification. In your testimony you state that the Coast Guard is working with the Transportation Security Administration (TSA) to develop new credentialing for Merchant Mariners. What is the current status of this effort?

Answer. The Coast Guard continues to update the merchant mariner credentialing statutes, which include provisions that will allow the future harmonization of mariners' credentials and TWIC. The Coast Guard is not developing entirely new credentials for mariners, but will continue to build upon existing security features that have already been incorporated into mariners' credentials until full integration with the TWIC is achieved. The Coast Guard is currently in the final stages of drafting a Legislative Change Proposal (LCP) that will accomplish many of the needed updates to its merchant mariner document statutes and is also working closely with TSA to ensure the efficient and effective integration of the TWIC and mariners' credentials. The two efforts, though related, are progressing under different timelines. The LCP is solely a Coast Guard effort and expected to be published in early 2006. TSA is the lead agency on the TWIC effort, with the Coast Guard providing assistance.

Question 9a. In what capacity is the Coast Guard assisting the TSA to develop a new identification system for merchant mariners?

Answer. The Coast Guard has partnered with TSA to develop and implement the Transportation Worker Identification Credential (TWIC) in the maritime mode, which will satisfy the mandate of 46 U.S.C. 70105, requiring that certain mariners carry a biometrically enhanced "transportation security card." The TWIC will build

upon and integrate with the current mariners credentialing system rather than implement an entirely new identification system. The National Maritime Center (NMC) is fully involved in advising TSA of mariner credentialing requirements and existing Coast Guard processes, and is leading the effort to ensure that the MMD process is integrated into the TWIC process to the fullest appropriate degree.

Question 9b. What role can this Committee play to assist in this endeavor?

Answer. The Committee's oversight will continue to be very important. The task of creating a uniform, biometrically enabled credential that is to be implemented across all transportation modes is a hugely complex endeavor that requires considered, careful planning to effectively implement. While the Coast Guard is involved in implementation of the Transportation Worker Identification Credential (TWIC) within the maritime mode only, almost every mode of transportation other than the airlines, will be impacted to some degree in its rulemaking. To ensure that the rule which results is intelligent and effective, the Coast Guard is careful to rely upon experts in the field who fully understand the intricacies of implementing for the first time this type of technology at the proposed scale. While thoughtful, measured regulations will achieve significant improvements in the security of our ports, a rushed implementation is unlikely to achieve any significant security enhancements, and could potentially wreak havoc with the Nation's economy while placing unfounded burdens upon workers, employers and the Federal Government.

Question 9c. What timeline, if any, has been established for completion of a new identification system for merchant mariners?

Answer. The merchant mariner identification system and supporting statutes were designed in a far different threat environment than today. As such, the Coast Guard is examining the full scope of necessary changes to the identification documents and requirements in order to modernize the system, as well as to put in place appropriate safeguards. Some of these changes will no doubt require legislative proposals. The Coast Guard is in the final stages of examining those needs now and any needed legislative changes will be proposed by the Administration in the course of the 2007 authorization cycle.

Question 10. In your testimony, you state that the Coast Guard is continually looking for ways to improve its ability to respond to suspect activities by increasing Coast Guard operational presence in our maritime domain and improving the Coast Guard's capacities for response and recovery. The Coast Guard's responsibility to defend and secure 26,000 miles of navigable waterways and 361ports is a challenging task. What are some initiatives that the Coast Guard is considering to expand its operation presence and enhance its ability to respond to a terrorist incident?

Answer. Coast Guard efforts to increase operational presence in ports and coastal zones focus not only on adding more people, boats and ships to force structures, but also on making the employment of those resources more effective through the application of technology, information sharing and intelligence support. Since 9/11, we have:

- Established 13 new Maritime Safety and Security Teams,
- Deployed over 100 new small boats and boat crews,
- Provided radiation detection capabilities to many of our boarding teams,
- Deployed field intelligence support teams to better collect and disseminate maritime threat information,
- Acquired fifteen 87-foot Coastal Patrol boats and four 179-foot coastal patrol craft to increase operational presence in our ports.

The FY 2006 budget focuses resources toward increasing both the quantity and quality of Coast Guard operational presence by providing funding for:

- Integrated Deepwater System—Continued investment in 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 or terrorist activity at sea or on the ports, waterways or coast of America.
- Airborne Use of Force (AUF) capability—deploys organic AUF capability to five Coast Guard Air Stations, increasing the ability to respond to maritime security threats.
- Enhanced Cutter Boat Capability—replaces existing obsolete and unstable cutter boats throughout the entire WHEC/WMEC fleet with the more capable Cutter Boat—Over the Horizon and replaces aging, unsafe boat davit systems on 210-foot WMECs.

- Increase Port Presence and Liquefied Natural Gas (LNG) Transport Security—provides additional Response Boat-Smalls and associated crews to increase presence to patrol critical infrastructure areas, enforce security zones, and perform high interest vessel escorts in strategic ports throughout the Nation. Provides additional boat crews and screening personnel at key LNG hubs such as Cove Point, MD and Providence, RI to enhance LNG tanker and waterside security.
- Enhanced Maritime Safety and Security Team (E–MSST)—Reallocates existing Coast Guard resources to immediately fill an existing gap in national maritime Law Enforcement and Counter-Terrorism (LE/CT) capability. Full operation of E–MSST Chesapeake, VA will provide an offensive DHS force able to execute across the full spectrum of LE and CT response in support of homeland security and homeland defense objectives, including CT response capability for scheduled security events out to 50 nautical miles from shore and augments to interagency assets in high visibility venues such as National Special Security Events (NSSEs).

Question 10a. Has Congress provided the Coast Guard with the resources it needs to meet its current mandates, including those set forth in the MTSA?

Answer. The FY 2005 Budget provided approximately $101 million and 791 personnel to support the implementation of MTSA. This support has been instrumental to executing the implementation of MTSA requirements and sustaining its ongoing enforcement. Much has been done to enhance port security and while more clearly remains to be done, the Coast Guard will continue to work with the Administration and Congress to pursue additional resources as needed to mitigate the highest maritime risks.

Question 10b. What additional resources can Congress provide that are necessary to allow for the enhancements that you reference?

Answer. The FY 2006 budget request, now before the Congress, represents the highest priority needs of the Coast Guard. Fully supporting the President's request for FY 2006 will make significant enhancements to Coast Guard capability and readiness. As for additional resources, the next highest unfunded priorities are represented in our FY 2006 Unfunded Priorities list that was provided to Congress on February 25, 2005, and a copy of which is attached.

Question 11. As you state in your testimony. "Cargo security encompasses the process of ensuring that all cargo bound for the U.S. is legitimate and was properly supervised from the point of origin, through its sea transit, and during its arrival at the final destination in the U.S." However, it is clear that the supervision and checking of cargo arriving at U.S. ports is woefully inadequate. I understand that as little as 5 percent of cargo arriving at our ports is checked. While the Coast Guard works with Customs and Border Protection (CBP) to provide oversight and check cargo arriving at our ports, can you provide this Committee an update on the varying levels of screening being conducted to ensure the safety of these cargos as well as an update on current efforts to increase screening of cargo?

Answer. CBP meets its goal of inspecting 100 percent of high-risk people and cargo, while allowing legitimate commerce and passengers to proceed unimpeded, through effective risk management and its Cargo Security Strategy. Approximately 10 million sea containers and 11 million trucks arrive in the United States annually; inspection of every vehicle would likely damage the U.S. economy and would be counterproductive to CBP's dual mission of securing the borders while facilitating trade. Because the vast majority of shipments are low-risk, CBP must use risk management techniques to identify and screen the relatively few high-risk shipments.

Rather than simply increasing the percentage of random inspections, CBP employs a layered cargo security strategy that is built on five interrelated initiatives. First, under the 24-Hour Rule, all containers bound for the U.S. are required to submit manifest data to CBP 24 hours before lading at the foreign port. Next, the National Targeting Center (NTC) provides CBP with tactical targeting capability for all oceangoing cargo and cargo shipped by all other transportation modes 24 hours a day, seven days a week. The NTC uses manifest information provided by the 24-Hour Rule and will eventually include data from Advanced Container Security Devices to perform its targeting functions. Additionally, screening with Non-Intrusive Inspection (NII) technology, including some physical exams, is required for all high-risk sea containers and other cargo conveyances arriving in the U.S. NII technology is a critical component of CBP's Cargo Security Strategy aimed at preventing terrorist groups from smuggling a Weapon of Mass Effect or its components into the United States. Under the Container Security Initiative (CSI), cargo security is pushed beyond the borders of the United States. Currently, there are 38 operational CSI ports that are staffed with specially trained CBP targeting teams. CSI ports utilize NII and radiation detection technology to facilitate examinations performed on

high-risk containers. While examinations are conducted by CBP's host nation counterparts, the CBP teams have the ability to observe these exams.

Additionally, Automated Targeting Systems (ATS) at CSI ports are linked to the NTC to immediately identify any high-risk containers bound for the United States. Finally, under the Customs-Trade Partnership Against Terrorism (C–TPAT), CBP has established partnerships with the private sector to implement minimum standardized security requirements and concepts throughout the entire supply chain, back to and including the foreign manufacturer's loading docks.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO REAR ADMIRAL HERETH

Question 1. In the Coast Guard's report to the Commerce Committee on implementation of Joint Operation Command Centers, you failed to discuss any common standards, best practices or lessons learned from any of the existing command centers and how those standards can be used to develop additional units throughout the country in strategic ports. Rather, the report discussed the Coast Guard's current development of Sector Command Centers that are part of the Departmental directive to co-locate the regulatory and operational assets into one location for all of the Coast Guard's missions with the capability to expand and work with other agencies should an incident occur. I would contest approaching port security from a reactionary perspective is not in the best interests of national security. And further, in meetings I have had with the Commandant. he has described a very different vision than what is contained in this report. What does the Coast Guard hope to achieve with the further development of Joint Operation Command Centers?

Answer. Our primary goal is to enable our federal, state and local forces to be more proactive. The limited sensor and coordination capability present in most ports must be improved to make that happen.

We will greatly enhance the ability to be proactive by:

- Developing a robust Common Operational Picture that will be fed by sensors (cameras, radars, etc.) placed according to a risk-based methodology that ensures surveillance of critical infrastructure and waterways.
- Sharing the Common Operational Picture with port partners by providing them a view via a web client service or, if they wish, by including their personnel as a permanent or ad hoc part of the command center staff.
- Coordinating federal, state and local enforcement efforts by developing and implementing technologies to track all assets, providing 7×24 monitored maritime communications capability and leading regular, collaborative planning and execution efforts.

Question 2. MTSA required the Coast Guard to develop a National Maritime Transportation Security Plan (46 U.S.C. 70103) to assign duties and responsibilities among federal agencies, establish procedures to prevent an incident from occurring, and plan for ensuring the flow of commerce is resumed as quickly as possible in the event of an attack. When will the National Plan be completed and made available for comment for our maritime stakeholders?

Answer. The review draft of the National Plan is being edited to prepare for distribution for initial review by federal agency stakeholders, which is expected to begin in mid-August. The Commandant intends to use the National Maritime Security Advisory Committee as one of the primary forums for comment on the plan by stakeholders in the maritime industry. The schedule of availability for other maritime stakeholders must be established in consultation with cognizant authorities in the office of the Secretary of Homeland Security.

Question 2a. Will this serve as the basis for the President's National Maritime Security Strategy requirement in HSPD 13, due to be released in June of this year?

Answer. No, but the National Plan has linkages to certain plans developed under HSPD–13.

In accordance with the MTSA, the National Plan is focused on ensuring the security of assets and infrastructure in the Maritime Homeland domain of the United States. In addition to fulfilling the requirements of MTSA, the National Plan will also serve as the sub-sector plan for national maritime transportation security, within the family of 17 sector security plans established under HSPD–7, including the Transportation Sector Security Plan (TSSP).

In contrast to the MTSA and HSPD–7, HSPD–13 is universal in scope, extending completely across both the international and homeland maritime domains. The National Plan under MTSA has natural linkages and relationships with certain plans

developed under the President's National Maritime Security Strategy requirement in HSPD 13, such as the Maritime Infrastructure recovery Plan (MIRP).

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO ROBERT JACKSTA

Question 1. What are the "minimum-security standards" the bureau has put into place for the C–TPAT program?

Answer. The minimum-security criteria for C–TPAT Importers, promulgated in March 2005 is based on a program assessment of the processes, procedures and best practices extrapolated from CBP's review of security profile submissions and C–TPAT validation visits. The security criteria provide an effective benchmark for C–TPAT companies to continue to build upon their security processes and procedures and focus on foreign manufacturers and container point of stuffing, through the CBP clearance process. The security criteria provide a meaningful expectation of what is required to enroll in the C–TPAT program.

Question 2. How many RPM's have been deployed at seaports?

Answer. As of July 27, 2005, CBP has deployed 88 radiation portal monitors to our Nation's seaports.

Question 3. I understand you are proposing regulations on cargo locks and seals this summer to satisfy the requirements of MTSA. What requirements are you proposing in your regulations for the domestic and international verification of cargo seals?

Answer. At the request of the Department of Homeland Security, the Departmental Advisory Committee on Commercial Operations of Customs and Border Protection and Related Activities (COAC) established a subcommittee to provide advice on this issue. Specifically, DHS requested recommendation in three areas: standards for physical security for inter-modal containers; secure system of transportation; and quantitative performance metrics to measure the success of specific DHS cargo security programs and to guide future efforts. In response to this request, COAC recommended a regulatory requirement for the sealing of loaded containers.

DHS has reviewed the COAC recommendations and agreed that there is a need for a seal regulation. CBP has drafted the Notice of Proposed Rule Making (NPRM) which will require the sealing of loaded containers being transported by vessel to the United States. At a minimum ISO-compliant high security seals (ISO/PAS 17712) must be affixed to the container at the last point where the container is loaded. Electronically readable mechanical seals and seals that perform other functions, such as electronic seals (e-seals), may also be used if they meet or exceed the high security specifications in ISO/PAS 17712 or are accompanied by a mechanical seal meeting or exceeding the ISO/PAS 17712 high security seal specifications. Verification of this sealing requirement must be performed by the carrier or their agent prior to lading on a vessel departing for the United States. The Department is currently reviewing the draft NPRM.

Question 3a. Aren't you aware that Coast Guard regulations require facilities to routinely check seals for evidence of tampering? (CFR 105.265) How is this being enforced?

Answer. Coast Guard enforces 33 CFR 105.265 during periodic and random cargo facility exams. As noted, 33 CFR 105.265(b)(1) requires facilities to routinely check cargo, cargo transport units and cargo storage areas within the facility prior to, and during, cargo handling operations for evidence of tampering. 33 CFR 105.265(b)(4) requires facilities to check seals and other methods used to prevent tampering of cargo entering the facility and during storage within the facility.

Operational MTSA facilities are required to hold Coast Guard approved Facility Security Plans. Each facility's plan explains the measures and procedures that the company uses to comply with the specific MTSA regulations. In general, facilities check cargo, transport units and loaded containers with a combination of random visual and physical examinations, employment of scanning/detection equipment, mechanical devices and dogs. Per the regulations, the security measures are scalable, and they must increase in frequency and intensity when the Maritime Security (MARSEC) Condition is raised.

Coast Guard facility inspectors verify that each facility is conducting the security measures as specified in its Facility Security Plan. This is especially important when the MARSEC Condition is raised, and Coast Guard inspectors perform spot-checks to verify the enhanced measures are in place.

Question 4. What percentage of entry data is received 24 hours prior to loading in a foreign port for evaluation and screening by the Automated Targeting System?

Answer. Currently, CBP receives trade data via manifest and entry filings. This data is essential for basic risk management and trade facilitation. However, a significant amount of additional information can be gathered during other phases of supply chain operations. New sources and types of data can be used to enhance and strengthen the effectiveness of CBP screening and targeting efforts. Some of these points in supply chain operations where data can be gathered include the purchase order process, staging and shipment, and cargo transportation. By collecting more and different information throughout the supply chain, greater visibility and transparency can be achieved and true risk better understood within the international supply chain.

The CBP Advance Trade Data Initiative (ATDI) is currently a prototype program researching and analyzing data available in today's global supply chains. ATDI seeks to enhance CBP's risk management practices through earlier collection and analysis of business-to-business information used by commercial supply chain participants. This information is available in advance of and in addition to the manifest and entry data currently collected by CBP. ATDI is a fact-finding prototype that seeks to gain greater visibility into supply-chain-security.

The ATDI prototype has been developed with significant participation from members of the trade community. A supply-chain-security committee has been set up within the Trade Support Network as a forum that works with the trade community to identify and leverage advance information early in the supply chain. This advance information will build upon existing CBP security measures to add value to ongoing targeting initiatives in order to secure our Nations borders, as well as our efforts to facilitate legitimate trade. The committee's goal is to identify, discuss, document, and submit the trade communities' supply-chain-security requirement recommendations for CBP's Automated Commercial Environment—ACE, which in partnership with CBP should result in an information requirement plan for the best dataset available to CBP.

Through partnering with the carriers, portals, importers, shippers and terminal operators, CBP is gathering supply chain data, studying what it means, discovering where it can be most effectively obtained in the supply chain, who has it, how the pieces fit together and determining how it can improve our targeting programs. All of this data will assist us to zero in on suspect movements and perform any necessary security inspections at the earliest point possible in the supply chain.

Question 5. Is the Bureau in the process of working with the Department of State on developing human resources that are trained, not only on cargo handling and inspection processes, but that are language and culturally proficient in the host country? If not, how are you addressing the shortfalls in your human capitol for managing existing programs?

Answer. CBP coordinates with Department of State and other applicable parties to train CBP officers who are detailed to overseas locations in support of The Container Security Initiative. These officers assist host countries in the examination of containerized cargo. As part of their training officers are instructed in cultural awareness, security awareness, living overseas, pre-deployment and continued, post-deployment foreign language training, and specific job-related skills.

Question 6. How do ocean-going carriers fit into the C–TPAT program?

Answer. Under the C–TPAT program, ocean-going carriers must not only analyze and increase security practices in their own operations, but also verify the security of their service providers and business partners. Because ocean carriers transport high volumes of ocean going containerized cargo, C–TPAT plays a vital role in ensuring the effective implementation of security during the ocean transportation phase. In fact, C–TPAT ocean-going carriers transport approximately 95 percent of all the U.S.-bound maritime container carrier traffic. While CBP has had partnerships with ocean-going carriers since 1984 through the Carrier Initiative Program, C–TPAT has enabled ocean-going carriers to significantly impact and improve their security practices.

Question 7. GAO's statement refers to two programs to improve supply-chain-security, the Container Security Initiative (CSI) and Customs-Trade Partnership Against Terrorism (C–TPAT). GAO's July 2003 report said that these start-up programs were not designed with a longer term strategic focus and recommended that both programs needed to have strategic plans, human capital plans, and performance measures. CBP agreed to implement these recommendations. Since GAO's July 2003 report, what progress has been made in implementing GAO's recommendations related to strategic plans, human capital plans, and performance measures?

Answer. CSI has developed a series of strategic and human capital plans to measure the Initiative's outcome, information and efficiency. Outcome is evaluated by the percent of worldwide U.S. destined containers processed through CSI ports and the

number of foreign mitigated examinations. Information is measured by the number of: intelligence reports based on CSI foreign sources; operational CSI ports; positive findings; and investigative cases initiated due to CSI activity. Finally, efficiency is appraised by the average cost per CSI port to achieve operational status.

The C–TPAT Strategic Plan was completed and distributed in December 2004 and the Human Capital Plan was developed in February 2005. CBP has recognized the need for outside assistance in the development of performance measures beyond general workload measures and has contracted with an outside firm to assist in the collection and development of performance measures. The development of these performance measures is expected to be completed in 8 to 10 months.

Question 7a. Whether these recommendations have been implemented or not, what other problems or challenges is CBP facing with the CSI and C–TPAT efforts to improve the supply chain?

Answer. As the C–TPAT program has grown, CBP has taken steps to more clearly define minimum security criteria, or baseline security standards, for membership in this voluntary, incentives based program. Additional personnel resources have been added so that members can be more timely validated against these security criteria. Validations are routinely taking place in countries throughout the world, with the exception of China, which has not allowed CBP C–TPAT Supply-Chain-Security Specialists entry into the country. CSI has not been confronted with any problems or challenges in implementing the GAO recommendations.

U.S. DEPARTMENT OF HOMELAND SECURITY, U.S. COAST GUARD
Washington, DC, February 25, 2005

Hon. Harold Rogers,
Chairman,
House Subcommittee on Homeland Security,
Committee on Appropriations,
Washington, DC.

Dear Mr. Chairman:

Pursuant to your request, attached is the Coast Guard's Unfunded Priorities List (UPL). The Fiscal Year 2006 budget currently before Congress represents my highest priorities.

As mentioned in the President's signing statement on H.R. 4567, the Department of Homeland Security Appropriations Act, 2005, to the extent that provisions of the Act (Public Law 108–334), including section 514, call for submission of legislative recommendations to the Congress, the executive branch shall construe such provisions in a manner consistent with the President's constitutional authority to supervise the unitary executive branch and to recommend for the consideration of the Congress such measures as the President shall judge necessary and expedient. However, I am providing this list to you as a matter of comity.

The Coast Guard is extremely grateful for and has benefited from the increased resources provided by the President and Congress over the past several years. Since September 11, 2001, the Coast Guard has enjoyed a substantial increase in funding. Specifically, the Coast Guard's FY 2006 discretionary budget would provide nearly $3.2 billion more than the comparable FY 2001 level, growing the Coast Guard's annual appropriation by 85 percent since the attacks of September 11, 2001. These additional resources have enabled the Coast Guard to establish 13 Maritime Safety and Security Teams across the Nation, deploy over 80 new small boats and accompanying crews, expand our intelligence capabilities. and implement the 2002 Maritime Transportation Security Act (MTSA). Each of these initiatives, among many others, have been critical to allowing the Coast Guard to meet post 9/11 mission demands, while ensuring no degradation in other performance areas.

The President's FY 2006 budget request also represents an 11 percent increase over the comparable FY 2005 discretionary funding levels, and demonstrates extremely strong commitment by the Administration to ensure the Coast Guard is adequately funded. The resources contained in the budget continue to implement the core elements of the Department's *Maritime Strategy for Homeland Security*. For example, robust implementation of organic Airborne Use of Force (AUF) capability and additional Response Boat-Small allowances will greatly *increase operational presence and response posture.* The President's budget also includes several *Maritime Domain Awareness* (MDA) initiatives; such as implementing the Coast Guard Common Operational Picture (COP), continuing the nationwide Automatic Identification System (AIS), and augmenting maritime patrol aircraft. These capabilities are of foremost importance to early detection, identification. and interception of

threats; and reducing America's homeland security risk, including terrorist attacks, migrant smuggling, or drug trafficking.

An identical letter has been sent to Chairman Cochran. Senator Byrd, and Representative Sabo.

Thank you for your interest in the Coast Guard. I am happy to answer any further question you may have, or your staff may contact my House Liaison Office at (202) 225–4775.

Sincerely,

THOMAS H. COLLINS,
Admiral, U.S. Coast Guard

U.S. Coast Guard FY06 Unfunded Priorities List

Priority	Program/Project	Approp	Amount ($K)	FTP	Recurring	Requirement
1	Deepwater	AC&I	637,300	—	No	Funding required to complete design/production of the first FRC, production of first WMSM, six MPA, continued recap of HH–60 radar/FLIR systems and HC–130 avionics and radar systems, and continued development of the COP and C4ISR upgrades.
	FRC Design and Development	AC&I	57,500	—	No	
	Maritime Security Cutter-Medium (formerly OPC)	AC&I	217,000	—	No	
	Maritime Patrol Aircraft	AC&I	225,000	—	No	
	HH–60 & HC–130 Legacy Sustainment	AC&I	47,500	—	No	
	C4ISR Upgrades	AC&I	70,300	—	No	
	Systems Engineering and Government Program Mgmt	AC&I	20,000	—	No	
2	Cutter and Aircraft Legacy Sustainment	AC&I	62,669	—	No	USCG operational requirement as identified in the Coast Guard's Integrated Near Term Support Strategy.
	110′/123′ WPB Mission Effectiveness Project (MEP)	AC&I	35,417	—	No	
	378′ Mission Effectiveness Project (MEP)	AC&I	9,452	—	No	
	HH–65 Sliding Cabin Door Replacement	AC&I	5,800	—	No	
	HH–65 Landing Gear Replacement	AC&I	2,884	—	No	
	HH–65 Tail Rotor Blade/Tail Gearbox Replacement	AC&I	2,936	—	No	
	HH–60J T700 Engine Upgrade	AC&I	6,180	—	No	
3	Additional Maritime Patrol Aircraft (MPA) Hours	OE	4,000	8	Yes	Reduces USIC MPA program flight hour gap consistent with National Strategy for Homeland Security, National Security Strategy, National Drug Control Strategy, and HSPD 7—Critical Infrastructure Protection. Provides 500 C–130H flight hours, which will primarily be used in support of Joint Interagency Task Force South/West operations.

4	Airborne Use of Force	AC&I	8,600	—	No	Capability required to implement guiding security strategies including the National Strategy for Homeland Security, National Security Strategy and HSPD 7—Critical Infrastructure Protection. Outfits approximately 12 aircraft @ up to three air stations for AUF in addition to the capabilities already provided in the FY 2006 budget for approximately 34 aircraft at 5 air stations.
5	Maritime Domain Awareness (MDA)	OE/AC&I	31,000	11	Partial—See Below	Further implements MDA consistent with National Strategy for Homeland Security, National Security Strategy, and Maritime Strategy for Homeland Security. Specific system requirements provided below.
	Ports & Waterways Safety System (PAWSS)	AC&I	17,000	—	No	Completes recap of Vessel Traffic Services in San Francisco, CA and Puget Sound, WA consistent with the Coast Guard's statutory responsibility under the Ports and Waterways Safety Act of 1972 (PWSA), Title 33 U.S.C. §1221 to ensure the safety and environmental protection of U.S. ports and waterways.
	High Frequency Communications System Recap	AC&I	10,500	—	No	Completes HF recapitalization faster than proposed in the FY 2006 budget. Operation of the HF comms system is required to meet International Safety of Life at Sea (SOLAS) treaty requirements.
	Inland Rivers Vessel Movement Center (IRVMC)	OE	3,500	11	Yes	Permanently establishes IRVMC—improving the ability to track Certain Dangerous Cargoes per 33 CFR Part 165.
6	Enhanced Maritime Safety and Security Team (E–MSST)	OE/AC&I	70,000	245	Yes	E–MSST Chesapeake on call capability.

U.S. Coast Guard FY06 Unfunded Priorities List—Continued

Priority	Program/Project	Approp	Amount ($K)	FTP	Recurring	Requirement
7	Merchant Mariner Licensing and Documentation Centralization	OE	26,700	118	Yes	Improves merchant mariner credentialing consistent with Sections 102 (Chapter 70105) and 324 of the Maritime Transportation Security Act of 2002 (Pub. L. 107-295) through centralization screening/evaluation of applicants, production of credentials and records.
8	Sector North Carolina	AC&I	4,000	—	No	Beach erosion forcing re-location of Group Cape Hatteras. Funds re-location.
9	Shore Facility Recapitalization	AC&I	59,370	—	No	Coast Guard shore facility readiness requirements.
	Group Seattle—Construct Admin/Ops Sector Building	AC&I	3,000	—	No	
	Station Galveston—Rebuild Waterfront	AC&I	6,600	—	No	
	Sector San Francisco—Establish Command Center	AC&I	12,200	—	No	
	AIRSTA Elizabeth City—Recap Aquatics Training Facility	AC&I	8,700	—	No	
	AIRSTA Elizabeth City—Consolidate Facilities	AC&I	5,300	—	No	
	Group Port Angeles—Construct Supply Building	AC&I	1,400	—	No	
	Station Coos Bay—Renovate Covered Mooring	AC&I	1,400	—	No	
	Station Fire Island—Rehab Waterfront	AC&I	1,400	—	No	
	TISCOM—Construct Building Addition	AC&I	1,450	—	No	
	Station Cordova—Replace Housing	AC&I	15,000	—	No	
	Base San Juan—Renovate Support Building	AC&I	1,450	—	No	
	Station Ocracoke—Replace Station Facilities	AC&I	750	—	No	
	ISC Alameda—Construct New WPB Mooring	AC&I	720	—	No	

10	Towing Vessel Inspection Program	OE	13,750	203	Yes	Section 415 of The Coast Guard and Maritime Transportation Act of 2004 (Pub. L. 108-617) authorizes the Secretary of DHS to implement mandatory inspection requirements and a safety management system for towing vessels to reduce casualties/mishaps. This line item reflects the annual resource requirement to implement this program.
11	Response Plan for Non-Tank Vessels	OE	1,845	4	Yes	Section 701 of The Coast Guard and Maritime Transportation Act of 2004 (Pub. L. 108-617) requires owners and operators of non-tank vessels to submit spill response plans to the Coast Guard for review. This line-item reflects the annual resources required to establish this program.
	Total Unfunded Priorities		919,234	589		

100

○