

S. HRG. 111-1015

**SAFE PORT ACT REAUTHORIZATION: SECURING
OUR NATION'S CRITICAL INFRASTRUCTURE**

HEARING

BEFORE THE

**COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION
UNITED STATES SENATE**

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

—————
JULY 21, 2010
—————

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



U.S. GOVERNMENT PRINTING OFFICE

67-271 PDF

WASHINGTON : 2011

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) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*

DANIEL K. INOUE, Hawaii	KAY BAILEY HUTCHISON, Texas, <i>Ranking</i>
JOHN F. KERRY, Massachusetts	OLYMPIA J. SNOWE, Maine
BYRON L. DORGAN, North Dakota	JOHN ENSIGN, Nevada
BARBARA BOXER, California	JIM DEMINT, South Carolina
BILL NELSON, Florida	JOHN THUNE, South Dakota
MARIA CANTWELL, Washington	ROGER F. WICKER, Mississippi
FRANK R. LAUTENBERG, New Jersey	GEORGE S. LEMIEUX, Florida
MARK PRYOR, Arkansas	JOHNNY ISAKSON, Georgia
CLAIRE McCASKILL, Missouri	DAVID VITTER, Louisiana
AMY KLOBUCHAR, Minnesota	SAM BROWNBACK, Kansas
TOM UDALL, New Mexico	MIKE JOHANNIS, Nebraska
MARK WARNER, Virginia	
MARK BEGICH, Alaska	

ELLEN L. DONESKI, *Staff Director*

JAMES REID, *Deputy Staff Director*

BRUCE H. ANDREWS, *General Counsel*

ANN BEGEMAN, *Republican Staff Director*

BRIAN M. HENDRICKS, *Republican General Counsel*

NICK ROSSI, *Republican Chief Counsel*

CONTENTS

	Page
Hearing held on July 21, 2010	1
Statement of Senator Rockefeller	1
Statement of Senator Hutchison	3
Prepared statement	4
Statement of Senator Lautenberg	5
Statement of Senator Klobuchar	38
Statement of Senator Cantwell	40
Statement of Senator LeMieux	42

WITNESSES

Admiral Robert J. Papp, Commandant, U.S. Coast Guard, Department of Homeland Security	5
Prepared statement	8
Hon. Alan Bersin, Commissioner, U.S. Customs and Border Protection, De- partment of Homeland Security	15
Prepared statement	17
Stephen L. Caldwell, Director, Homeland Security and Justice Issues, U.S. Government Accountability Office	21
Prepared statement	23

APPENDIX

Response to written questions submitted to Admiral Robert J. Papp by:	
Hon. John D. Rockefeller IV	53
Hon. Frank R. Lautenberg	60
Hon. Barbara Boxer	61
Hon. Maria Cantwell	62
Hon. Kay Bailey Hutchison	64
Hon. David Vitter	69
Response to written questions submitted to Hon. Alan Bersin by:	
Hon. John D. Rockefeller IV	70
Hon. Frank R. Lautenberg	76
Hon. Barbara Boxer	76
Hon. Bill Nelson	78
Hon. Maria Cantwell	79
Hon. Mark Pryor	81
Hon. Kay Bailey Hutchison	82
Response to written questions submitted to Stephen L. Caldwell by:	
Hon. John D. Rockefeller IV	83
Hon. Kay Bailey Hutchison	83
Hon. John D. Rockefeller IV	85
Hon. Kay Bailey Hutchison	94
Hon. Bill Nelson	95
Hon. Frank R. Lautenberg	95
Hon. Amy Klobuchar	97

**SAFE PORT ACT REAUTHORIZATION:
SECURING OUR NATION'S
CRITICAL INFRASTRUCTURE**

WEDNESDAY, JULY 21, 2010

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

The Committee met, pursuant to notice, at 2:40 p.m. in room SR-253, Russell Senate Office Building, Hon. John D. Rockefeller IV, Chairman of the Committee, presiding.

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

The CHAIRMAN. All right, this hearing will come to order. You have the brains of the Committee before you.

[Laughter.]

The CHAIRMAN. Actually, the brains of the Committee is sitting behind us.

[Laughter.]

Senator HUTCHISON. Right, exactly.

The CHAIRMAN. Every day, terrorists are hard at work at hatching new plans to do America harm. As the former Chairman and current member of the Intelligence Committee, I have a very special way of knowing that, and I can tell you, the threats are very real—and, of course, you all know that—and that they continue and they expand and become more malicious.

In the last year alone, we have seen one terrorist try to blow up an airplane on Christmas Day, and we've seen another try to turn his SUV into a bomb near Times Square. No matter how many plots we disrupt, more will replace them, and history has shown us that one of the greatest security challenges we face is securing our free and open transportation system.

Although our aviation security system is the most visible part of our Nation's homeland security system, DHS is working to secure all aspects of our transportation infrastructure. Today, we're going to talk about a huge challenge we have in making our ports more secure. The very size, location, and constant movement at ports makes them vulnerable to a potential terrorist attack. In fact, a fairly easy terrorist attack.

If terrorists were to shut down a major port, the economic disruption to our economy would be incalculable, as it would be to the psyche of Americans. Maritime security is more than just protecting our ports from attack; it's protecting our ships, both mili-

tary and commercial, preventing attacks on our communities, and keeping extremely hazardous materials from being used as weapons.

Welcome, Senator Lautenberg.

Senator LAUTENBERG. Thank you.

The CHAIRMAN. For example, small vessels can carry explosives, as they did in the 2000 USS Cole attack, or smuggle terrorists, as they did in Mumbai, India, in 2008. Preventing terrorists from using our maritime transportation system to smuggle weapons or people into this country is very important to our economic security, and our national psyche.

I think, as a West Virginian—of chemical plants on the Ohio River, right between West Virginia and Ohio—it's called the Ohio River, but we own it, which means we have to pay to build the bridges. That's just a small thing, which is not really a part of this hearing. Anyway, it's lined with chemical plants, and it's lined with powerplants, all the way from Pittsburgh all the way down to Cincinnati. And I think the Coast Guard is only able, at this point, because of funding problems, et cetera, to supply, at the most, three, but, up until recently, only two armed speedboats to patrol that 200 miles. It's like an open, free chance for anybody.

Many people may not know this, but West Virginia is actually home to the seventh-largest port—and that includes San Diego, San Francisco, New York, et cetera—in the country, and it's called Huntington, West Virginia. It connects all the way from the Atlantic to the Gulf, and it's just an unbelievable sight of transference of cargo. Over 77 million tons move through that port annually, 30 of which is petroleum and chemical products. If terrorists attacked a chemical plant adjacent to the Port of Huntington, the resulting toxic plume would be devastating. It can happen any day. It has not, but it could.

Make no mistake, the challenges before us are very great. Two of our witnesses today will discuss the enormously difficult task of balancing the need to protect our maritime transportation system with the efficient flow of commerce.

For example, in 2007, Congress required 100-percent scanning of all oceanborne cargo containers entering the United States. Last year, the Secretary of Homeland Security told this committee that she doubted that DHS could meet that challenge. It will be expensive. Very expensive.

If we cannot meet this mandate, then I believe we need to find a different way to address this threat. I look forward to hearing from you and having a discussion about that. What is possible, what is not; If we stretched, did something different, what difference could we make? As I have discussed already with Admiral Papp, the Coast Guard has too few resources to meet all of its missions, and that is unacceptable. I believe the Coast Guard needs more resources and more support to do its job, period. One can argue about debt, deficits, and all the rest of it, but protecting the American people ought to be, pretty much, preemptive, I would think.

So, just as the Committee has jurisdiction over maritime issues, we also have a primary role of making sure our maritime sector is, itself, secure. So, in the coming days, we're going to introduce legis-

lation that builds on provisions in the Security and Accountability For Every Port Act of 2006, or the SAFE Port Act, and the Maritime Transportation Security Act of 2002, bills this committee passed to strengthen maritime security.

The SAFE Port Act of 2006 furthered the preparedness of our ports by requiring national and regional security plans and mandating Coast Guard-approved incident response plans for all vessels, ports, and facilities on and adjacent to waterways that are engaged in maritime transportation.

This bill that I introduced will do the following: focus resources on critical needs, critical small vessel security—we need to talk about that—especially hazardous cargo, and the security of the global supply chain; reauthorize the Port Security Grant Program to ensure that adequate resources exist to secure our airport facilities; and, most importantly, seek to address key security gaps and lessons learned from the past 4 years.

I look forward to hearing from our witnesses today and as we go to several things: evaluate the current state of port security, reflect on the implementation of previous port security bills, and discuss how we can improve going ahead.

I thank everybody for being here, and I turn now to my extremely distinguished Co-Chair, Kay Bailey Hutchison.

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

Senator HUTCHISON. Well, thank you very much, Mr. Chairman.

And it is such an important part of our responsibility—port security. It has been 4 years since this committee passed the port security legislation, which became the SAFE Port Act of 2006. And, as many of these provisions in the bill begin to expire, we look forward to working together, the Chairman and I and other members, to reauthorize this important legislation.

The maritime transportation system in the United States is a vital asset to our Nation's economy, employing more than 13 million workers. The cargo that passes through our ports and waterways contributes approximately three-quarters of a trillion dollars to the U.S. gross domestic product.

In my home State of Texas—I'm going to brag on my port—the Port of Houston continues to rank first in the country in U.S. imports, first in foreign waterborne tonnage, and is home to one of the largest petrochemical complexes in the world, as well as part of the U.S. Strategic Petroleum Reserve.

The Houston ship-channel businesses account for almost 800,000 jobs and have an economic impact of close to \$120 billion. The Port of Houston is just one of the ports in our Gulf Coast, in Texas. We go from Brownsville all the way up the coast, through Port Arthur, in Beaumont. So, we do have a huge amount of waterborne commerce in my State, and there is no question that this is a security issue, just as any part of our transportation and commerce system is.

The Brookings Institution estimated that a detonated weapon of mass destruction at an American port could cost \$1 trillion to the national economy. So, it is the job of the Department of Homeland Security, with assistance from other entities in the Administra-

tion—certainly the Coast Guard, as well—Congress, State and local governments, and industry stakeholders, to be able to work seamlessly together. It's going to take the contribution of all of these entities to prevent any kind of devastating terrorist activity in our ports.

I am interested to hear what the three of you are going to say, and I hope that you will elaborate on any ideas that you have, going forward, for us to be able to pass a bill that will make a difference in our ports' security. I'm interested in ways that the government agencies, both State, local, as well as the different Federal agencies, can work seamlessly with each other, and cooperatively with the private sector, and efficiently, to make sure that risk management is the best that we can do to secure our Nation's transportation systems.

So, thank you for being here, and thank you, Mr. Chairman, for continuing to focus on this important issue.

[The prepared statement of Senator Hutchison follows:]

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

Mr. Chairman, thank you for holding today's hearing on port security, a critical element of our Nation's national security efforts.

It has been almost 4 years since this committee passed port security legislation, which became the SAFE Port Act of 2006. As many of the provisions in that bill begin to expire, I look forward to working with the Chairman and the other members to reauthorize this important legislation.

The maritime transportation system in the United States is a vital asset to the Nation's economy, employing more than 13 million workers. The cargo that passes through this country's ports and waterways contributes approximately three-quarters of a trillion dollars to the U.S. gross domestic product.

In my home state of Texas, the Port of Houston continues to rank first in the country in U.S. imports, first in foreign waterborne tonnage, and is home to one of the world's largest petrochemical complexes, as well as the U.S. Strategic Petroleum reserve.

The Houston shipping channel businesses account for almost 800,000 jobs and have an economic impact of close to \$120 billion.

Clearly, our Nation's economy and the flow of commerce can be affected significantly by an unforeseen event, which I am concerned we are not adequately prepared. A terrorist incident at a major U.S. port could cause a devastating loss of life and deliver a huge blow to our economy.

For example, the Brookings Institution estimated that a detonated weapon of mass destruction (WMD) at an American port could cost \$1 trillion to the national economy.

And so, it is the job of the Department of Homeland Security, with assistance from other entities within the Administration, as well as Congress, State and Local governments and industry stakeholders, to help put systems in place to prevent these devastating types of events from occurring and disrupting the delicate equilibrium of the flow of commerce and the sanctity of our way of life.

Therefore, I am particularly interested to hear what assessment our witnesses will provide of the state of our Nation's maritime security. In addition, I hope that our witnesses will elaborate on innovative ideas to help better secure our Nation's ports. I am especially interested in ways in which government agencies can work seamlessly with each other, work cooperatively with the private sector, and most importantly, work efficiently, so as not to expend precious financial resources on ineffective projects. Risk management is fundamental to securing our Nation's transportation systems.

Thank you and I look forward to hearing from our witnesses on these very important issues.

The CHAIRMAN. Thank you, Senator Hutchison.
And now to the distinguished Senator Frank Lautenberg.

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

Senator LAUTENBERG. Thanks, Mr. Chairman.

And your reminder that your landlocked State has such an important port is an important focus on what our ports mean to us, and certainly to your State, as you mentioned. My home State of New Jersey is, unfortunately, a prime terrorist target. In fact, the most at-risk area in the entire country for a terrorist attack is the 2-mile stretch from Newark Liberty International Airport to the Port of Newark.

And yesterday, I stood in that port with leaders of the Port Authority and those who labor there to provide for themselves and their family, and I was reminded again why the port is so critical. I'm very familiar with the port there. I was a commissioner of the Port Authority, and I ran a good-sized company in New Jersey, and was aware of the revenue and the energy provided by the port. And that port is so critical and attractive to those who want to hurt us. They know that the lifeblood of not just our region's economy, but our Nation's economy exists there.

The Port of Newark is the largest port on the East Coast, generating \$20 billion a year in economic activity. An attack on this port, or any of the Nation's ports, would be devastating. Billions of tons of domestic, important import and export cargo pass through American ports and waterways each year. And for example, when the Port of Long Beach in California shut down because of a labor dispute in 2001, it cost the economy a billion dollars a day. The Brookings Institution estimated that a detonated weapon of mass destruction at any one of our ports could cost the American economy a trillion dollars. It's a major responsibility of ours—Mr. Chairman, and you wear that mantle well—of ours to make sure our ports remain secure.

The 9/11 Commission underscored that obligation when it noted that opportunities to do harm are as great or greater in maritime and surface transportation than in aviation. When it comes to preventing future terrorist attacks, we dare not leave anything to chance. And that's why we passed the SAFE Port Act in 2006. That law set out a clear roadmap for the Department of Homeland Security to make sure our ports were protected.

Unfortunately, we're not yet at our destination. We've got more work to do. And I'm looking forward to hearing from our witnesses about the progress that has been made to meet the benchmarks set by that law, and the challenges that remain.

I'm delighted to have these witnesses here, Mr. Chairman. I congratulate you for having this hearing.

The CHAIRMAN. Thank you, Senator.

And now I think we should move in the direction of admirals. Admiral Papp, we look forward to hearing from you.

**STATEMENT OF ADMIRAL ROBERT J. PAPP, COMMANDANT,
U.S. COAST GUARD, DEPARTMENT OF HOMELAND SECURITY**

Admiral PAPP. Thank you, Mr. Chairman, good afternoon. And, to Ranking Member Senator Hutchison, good afternoon to you, ma'am, and Senator Lautenberg, our long-time supporter. It's good to see you again, sir.

I'm pleased to appear before you today to discuss this very important topic of maritime, homeland, and port security. I have an extensive written statement that I've submitted for the record, and I would just ask to do a short oral statement to open up.

The CHAIRMAN. All statements are in the record.

Admiral PAPP. Thank you.

I have three issues—three brief issues to address, here. First and foremost, the topic of this hearing, which is port security, of course. And while we've worked successfully with our Federal, State, local, foreign, and international partners to construct a robust maritime homeland and port security architecture, one of the things that concerns me the most, and one of the reasons I'm most grateful for this hearing today, is my concerns about complacency.

One of the things, as the Atlantic Area Commander, that I put up on our operations brief every morning, is the number 3,119. That's the number of days that transpired between the first attack on the World Trade Center, in February 1993, and then the events of September 11, 2001. And each day, we counted the increasing numbers of days that have passed since 9/11. Fortunately, we're up, now, to 3,235, so we've surpassed the period between the first attack and second attack on the Trade Center. But, what that tells me is, as we go longer and longer away from that event, we run the risk of our public becoming complacent.

So, Mr. Chairman, you drawing attention to this very important topic is good for us, and good for the Nation, and I thank you for that.

As I stated, 3,235 days have passed since 9/11. And while we've worked tirelessly to enhance our maritime, homeland, and port security, we must not let our guard down. We need to be looking to undertake initiatives that will tighten the security net in our ports, particularly with respect to the threat posed by small vessels. These initiatives include, amongst others, continuing to strengthen an already robust Federal, State, and local partnerships, working to formalize programs like America's Waterways Watch to incorporate the presence of professional mariners and recreational boaters into a coordinated effort. More vessels on the water can only mean greater security.

Since 9/11, the Coast Guard has exercised its versatile, adaptable ships, boats, and aircraft—and, I would say, versatile and adaptable people, as well—along with our authorities, partnerships, and capabilities, to create a layered security triad consisting of maritime security regimes, maritime domain awareness, and maritime security operations. This maritime triad, as I refer to it, is like a three-legged stool; if you forget one of those legs, you're going to subject yourself to a lack of success. So, we have to concentrate on all three.

The first leg of the "stool," as I refer to it, is the maritime security regimes. Maritime security regimes include domestic and international statutes, regulations, and agreements. Maritime security regimes constitute the framework for coordinating partnerships and establishing enforceable maritime security standards. Examples of that, of course, include the Maritime Transportation Security Act, the international maritime organizations, international ship and port facility code, and, of course, the SAFE Port Act.

The second leg of the “stool,” as I refer to it, is maritime domain awareness. Interagency operation centers, the nationwide automatic identification system, and long-range identification and tracking systems, Blue Force Tracking, and the America’s Waterways Watch Initiative, are also important to maritime domain awareness efforts. These initiatives are the means to collect, fuse, analyze, and disseminate a common operating picture and information, not just to the Coast Guard, but to our partners, as well, and to make us all stronger.

The third leg of this “stool” is the Maritime Security and Response Operations, or MSRO. These elements include coastal and waterway deterrence patrols, high-risk vessel escorts, response to threats, and recovery from attacks that may occur. The MSRO encompasses military outload security, enforcement of fixed security zones, control of port access activity and movement, and also includes waterborne security boardings, airborne use of force, underwater port security, and deliberate contingency and recovery plans and exercises focused on regional surge operations.

Ensuring the availability of the—of our Coast Guard cutters, aircraft, boats, and supporting systems and infrastructure to conduct these activities has become increasingly challenging. As Commandant, I’m committed to aggressively recapitalizing our assets to sustain fleet readiness and ensure future mission success. This is a top priority for me, moving forward.

Of the three concerns I listed, my second concern is my goal of steadying the service. Among other things, consummating our modernization effort and consolidating our command-and-control and mission-support structure within the Coast Guard. To complete this modernization effort, which was started under my predecessor, we, of course, need the authorization act. Your giving focus to this and working with the Coast Guard to continue the authorization act, moving forward, is deeply appreciated, and I look forward to working with you and the Committee to complete this very important initiative so that we can continue and finalize the structure of our Coast Guard.

And my last concern is actually a statement of pride. I want to tell you how absolutely proud I am of the men and women of the Coast Guard. We’re now 3 months into the *Deepwater Horizon* response, and a tremendous number of our Reserve and active-duty personnel, ships, and aircraft, those same versatile and adaptable assets and people I spoke of earlier, are deployed to the Gulf in support of the National Incident Commander. Our most important mission is to continue our all-hands-on-deck effort to protect the Gulf, its people, and their way of life.

As a force provider to the National Incident Commander, it’s my duty, however, to closely monitor the impact of this response on our people and our assets. Our Coast Guard men and women are focused and committed to accomplishing this all-important mission. Coastguardsmen were first on scene, performing search-and-rescue operations when the *Deepwater Horizon* rig exploded, resulting in the tragic loss of life of 11 people. And our versatile and adaptable people and assets transitioned as this incident evolved into the largest and most extensive environmental disaster that our Nation has faced, and we are proud that we are leading, along with the

Department of Homeland Security and across the entire inter-agency, the largest and most comprehensive response. We will be in the Gulf until our mission is completed.

In conclusion, while much has been accomplished, much remains to be done. Opportunities remain to strengthen relationships, improve maritime domain awareness, recapitalize our fleet, enhance public vigilance, and refine collaborative security regimes. The Coast Guard, as a component of the Department of Homeland Security, is committed to working hand-in-hand with our many partners to ensure the safety of American citizens and our ports and waterways.

Again, I look forward to working with this committee to understand the challenges and to earn your support. I thank you for the opportunity to testify today, and I look forward to your questions.

Thank you.

[The prepared statement of Admiral Papp follows:]

PREPARED STATEMENT OF ADMIRAL ROBERT J. PAPP, COMMANDANT,
U.S. COAST GUARD, DEPARTMENT OF HOMELAND SECURITY

Good afternoon, Chairman Rockefeller, Ranking Member Hutchison and distinguished members of the Committee. I am Robert Papp, Commandant of the Coast Guard and I am pleased to be here today to discuss the Coast Guard's critical role in protecting one of our Nation's most important economic and strategic lifelines, our Marine Transportation System (MTS). As the lead Federal agency for U.S. maritime security, the Coast Guard works with its port partners to build resiliency into the U.S. MTS. We have come a long way in protecting this system and its users; however, security challenges remain, and they demand an agile and technologically advanced Coast Guard.

Port Security: Mission and Scope

The Coast Guard's enduring value to the Nation resides in our multi-mission authorities, resources and capabilities. The ability to field versatile assets and personnel with broad authority is perhaps the Federal Government's most important strength in the maritime security environment. While each of the Coast Guard's eleven mission programs primarily supports safety, security or stewardship, all of our missions can serve additional roles. For example, when Coast Guard personnel conduct vessel safety inspections, their activities include verification of immigration documents and validation of crew manifests. The Coast Guard's safety and security authorities are fully integrated, providing a suite of unrivaled capabilities to address security in the maritime and port environment.



The Coast Guard primarily addresses MTS security through its Port, Waterways and Coastal Security (PWCS) mission, which is carried out using the Coast Guard's broad authorities and multi-mission assets. PWCS also benefits from other Coast Guard missions, including: Marine Safety, Illegal Drug and Migrant Interdiction, Defense Readiness, and Aids to Navigation missions.

The Coast Guard's holistic approach to port security protects against internal and cross-border threats, builds versatility, and supports the safe flow of lawful travel and commerce. Our efforts are focused on preventing and disrupting terrorist attacks and subversive acts in the maritime domain and the MTS. Should an attack occur, Coast Guard resources and competencies are prepared to contribute to a swift response and recovery.

Critical infrastructure, key resources and large population centers within or near America's ports represent vulnerabilities that terrorists may seek to exploit. As such, our port security efforts leverage the capabilities of the private sector, other Government agencies, including the Maritime Administration, and the public to multiply our defenses.

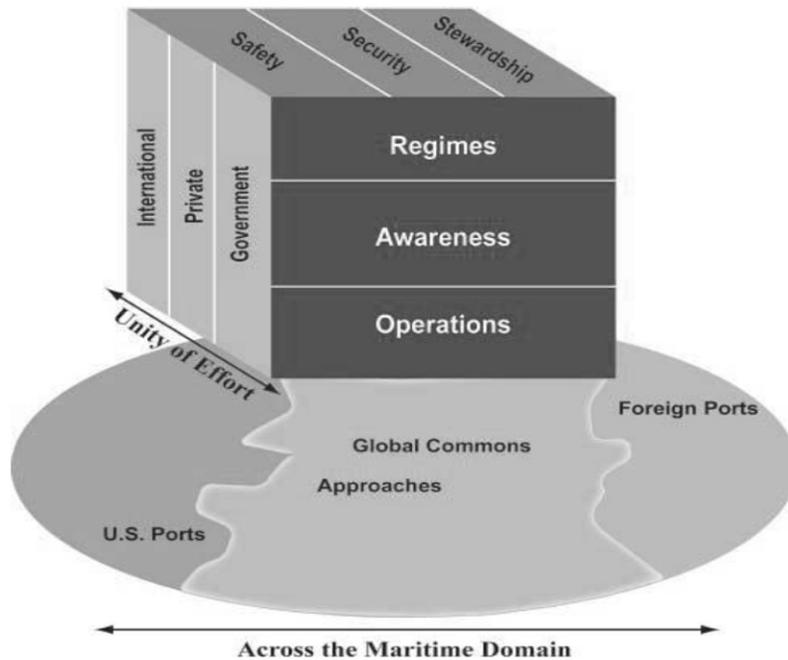
The Coast Guard helps secure over 95,000 miles of coastline, over 300 ports and over 10,000 miles of navigable waterways. Coast Guard and its port partners provide security for myriad landside connections that allow the various transportation modes to move people and goods to, from, and on the water. More than \$958 billion of international commerce, including 1.4 billion tons of cargo, is carried within the MTS. The Coast Guard regulates protection of more than 8 million cruise ship and ferry passengers, accounting for more than 65 million passenger-miles a year. The Coast Guard also regulates waterway security for numerous boaters operating almost 13 million registered recreational vessels. Finally, the Coast Guard protects

the movement of numerous high-value military vessels and maritime cargo in support of ongoing overseas contingency operations.

The demand for maritime escort and security services continues to grow. Over the last few years, for example, Liquefied Natural Gas (LNG) imports have doubled, from 1.5 percent to 3 percent of gas used, and are estimated to rise to more than 15 percent by 2025. This demand has triggered increased applications for facilities and development of new facilities, which, in turn, will likely result in an increased number of LNG vessel transits. Our challenge is to manage risk and deploy our limited assets where they achieve the greatest effect, and to both implement effective security measures while supporting the smooth flow of legitimate commerce. Under the current policies for Coast Guard asset utilization, growth in the maritime industry will increase the demand for Coast Guard capabilities, capacity and partnerships.

Mission Elements

The Coast Guard's role as Lead Federal Agency (LFA) for maritime security is embedded within the overarching system of maritime governance. The Coast Guard's systematic, maritime governance model for port security consists of maritime security regimes, domain awareness, and maritime security and response operations, which are carried out in a unified effort by international, governmental, and private stakeholders. The Coast Guard exercises unique competencies, capabilities, authorities, and partnerships in an attempt to help reduce the risk of terrorism and related nefarious acts. It also engages the private sector through Area Maritime Security Committees, implementation of the *DHS Small Vessel Security Strategy* (SVSS), *America's Waterway Watch* (AWW), and local and regional exercises. The SVSS proactively recognizes that small vessels are a potential means for exploitation by terrorists, smugglers of weapons of mass destruction (WMDs), narcotics, aliens, and other contraband, and other criminals and addresses near-shore security concerns and provides a coherent framework to improve maritime security and safety.

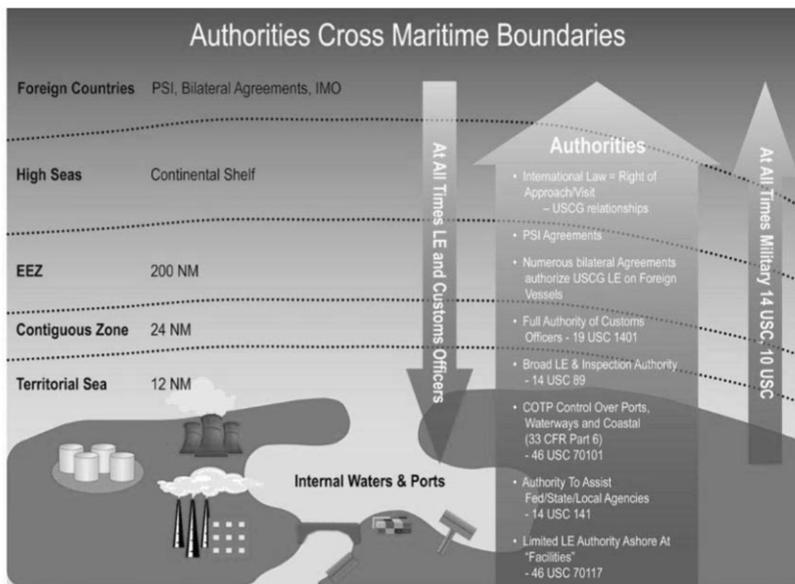


A System of Maritime Governance

The Coast Guard has extensive statutory authority, presence, command and control capability, and experience in maritime safety and security. The Coast Guard employs a holistic layered approach to maritime security that is designed to detect,

deter, and prevent the methods of terror and terrorists as early as possible in the event chain. This approach requires rigorous analysis of the terrorist threat and corresponding risk-reduction strategies and tactics. It facilitates early warning of maritime-related threats originating in other nations by way of offshore regions routing into the U.S. For example, through the 96-hour advanced notice of arrival process, the Coast Guard is able to screen vessels for potential threats far from the Nation's ports. Another example of a "far-from-the-homeland" element of this layered security system is the International Port Security (IPS) Program, which verifies that effective antiterrorism measures have been instituted in foreign ports to help reduce the risk to U.S. ports.

Port Security—A layered system



The three major elements of the Coast Guard's maritime security strategy are Maritime Security Regimes, Maritime Domain Awareness, and Maritime Security and Response Operations.

Maritime Security Regimes

The Maritime Security Regimes element of the Coast Guard's maritime security strategy includes domestic statutes and regulations, and international agreements and codes. It is comprised of the "rules" to coordinate partnerships and establish maritime security standards. Regimes represent the framework that complements efforts to conduct effective MDA activities and maritime operations. All of the regimes associated with all Coast Guard missions also support port security effectiveness.

The 2002 Maritime Transportation Security Act (MTSA) requires that ships and port facilities assess their vulnerabilities and develop measures to reduce them. The MTSA also requires that the Coast Guard periodically assess the effectiveness of antiterrorism measures in both U.S. and foreign ports and take action in cases in which effective anti-terrorism measures are not in place. In accordance with the provisions of the MTSA, the U.S. helped lead the International Maritime Organization in the development of an international code, designated the International Ship and Port Facility Security Code (ISPS). The ISPS Code contains security-related requirements for governments, port authorities and shipping companies, together with a series of guidelines and recommendations for meeting those requirements. The Coast Guard's IPS Program engages with foreign governments and visits foreign ports to assess their compliance with the ISPS Code and to improve security through dialogue.

Additionally, MTSA required the development and implementation of strategic, regional, vessel and facility security plans to enhance maritime transportation security. Area Maritime Security Plans are created by committees established by the Coast Guard and comprised of Federal, state, tribal, and local agencies and industry representatives. The Transportation Workers Identification Credential (TWIC) program, a Transportation Security Administration (TSA) initiative primarily enforced by the Coast Guard that helps to ensure that only properly vetted individuals have access to secure areas at ports, furthers the multilayered approach to the safeguarding of U.S. ports and maritime critical infrastructure and key resources.

Various programs and strategies have been developed to address specific threats and risks. The SVSS helps to reduce the small vessel security threat, and our strategy establishes the rules by which other vessels are identified as having a potential terrorism threat.

Maritime Domain Awareness

Maritime Domain Awareness (MDA), the second major element of the Coast Guard's maritime security strategy, supports the development of maritime regimes and effective Maritime Security and Response Operations. MDA requires that all-source intelligence and broad situational awareness be collected, fused, analyzed, and disseminated, enabling the United States and other nations to understand activities, events, and trends that could threaten their security in the maritime and port environment. MDA consists of what is observable and known as well as what is anticipated or suspected. Improving MDA requires continued development of intelligence capabilities and broader maritime situational awareness that leverages Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) capabilities. MDA provides the key Common Operating Picture (COP) of conditions and activity across the maritime domain. The COP includes information about vessels, cargo, passengers and crew, and shore-side infrastructure. As an example of the need for awareness, the Coast Guard is keenly interested in the real-time location and movements of certain vessels. These include all High Interest Vessels (which may pose a threat), High Value Units (certain military vessels), Certain Dangerous Cargo Vessels, and High Capacity Passenger Vessels. The Maritime Security Risk Analysis Model (MSRAM) is used to analyze and calculate risk to maritime critical infrastructure and key resources using threat factors provided by the intelligence community. MSRAM evaluates the consequence and vulnerability judgments in the field at the local, regional and national levels to enhance security risk analysis by informing the Common Operating Picture (COP) at the tactical, operational and strategic levels.



Interagency Operations Centers, the Nationwide Automatic Identification System, the Long Range Identification and Tracking (LRIT) system, and Blue Force Tracking support the MDA effort. These initiatives provide high-tech means to collect, fuse, analyze, and disseminate COP information and intelligence. Every Coast Guard unit has MDA responsibilities and serves as a sensor to increase awareness and knowledge of the maritime domain. The AWW initiative enlists public support to report suspicious activity on or near ports, docks, marinas, riversides, beaches, waterfront communities, or maritime infrastructure.

Maritime Security and Response Operations (MSRO)

The third major element of the Coast Guard's maritime security strategy is Maritime Security and Response Operations (MSRO). Ground, waterborne, and airborne prevention and response operations are conducted to prevent, disrupt and recover from attacks.

Recognizing that the Coast Guard and its partners cannot be everywhere all of the time, the Coast Guard conducts Maritime Security and Response Operations based on risk-informed decision-making models.

Coast Guard forces are trained and equipped to perform MSRO activities to enhance the Nation's ability to prevent and respond to maritime terrorism events. Specifically, Deployable Operations Group (DOG) forces were created to support operational and tactical commanders, including DOD and other Federal agencies. DOG forces include Maritime Safety and Security Teams, the Maritime Security Response Team, Tactical Law Enforcement Teams, Canine Explosive Detection Teams, and the National Strike Force.



MSRO elements include coastal and waterway deterrence patrols, high-risk vessel escorts, response to threats, and recovery from attacks. MSRO encompasses Military Out-Load security support, enforcement of fixed security zones, and control of port access, activity, and movement. MSRO also includes waterborne security boardings, Airborne Use of Force, underwater port security, deliberate, contingency, and recovery planning and exercises, and focused regional surge operations. A key element of the offshore portion of the MSRO is persistent presence of Coast Guard cutters and aircraft that are regularly engaged in multi-mission operations, such as at-sea interdiction and enforcement. As appropriate, MSRO forces are being equipped to respond to chemical, biological, radiological, nuclear, and high-yield explosive threats. The Area Maritime Security Training and Exercise Program is also an element of MSRO.

FY 2009 Mission Accomplishments

- The Coast Guard conducted 49,276 armed waterborne patrols projecting presence near maritime critical infrastructure or key resources, 18,690 security

boardings of small vessels in and around U.S. ports, waterways, and coastal regions, 4,000 escorts of high-capacity passenger vessels, such as ferries and cruise ships, 1,855 security boardings of High Interest Vessels (designated as posing a greater-than-normal risk to the U.S.), 1,429 escorts of high-value U.S. naval vessels transiting U.S. waterways, and 660 escorts of vessels carrying Certain Dangerous Cargoes (CDCs).

- In support of Overseas Contingency Operations, the Coast Guard provided waterside security and escorts for 192 military outloads throughout the system of 20 predesignated commercial and military strategic U.S. seaports.
- The Coast Guard's MSRAM continued to support risk management decisions in the execution of the PWCS mission. MSRAM helps prioritize security risk from terrorist attacks by assessing the risk between vastly different critical infrastructure facilities and key resources. MSRAM supported port security grant funding decisions by enabling DHS to compare various ports and determine which ports have the highest risk.
- The Coast Guard expanded its global vessel track picture through Long Range Identification and Tracking (LRIT) for vessels greater than 300 gross tons and improved Automatic Identification System (AIS) data. LRIT began operation in 2008 and to date over 750 U.S.-flagged vessels have been certified for carriage. The Coast Guard operates an International Data Exchange (IDE) that routes vessel positioning data among all participating LRIT national and regional data centers, as well as the U.S. national data center. At any given time, the Coast Guard tracks approximately 2,500 foreign flagged LRIT-equipped vessels en route to the U.S. or sailing within 1,000 nautical miles of U.S. territory, as well as U.S. ships around the globe.
- The Coast Guard conducted over 60 international port security visits/evaluations. These visits ensure foreign nation compliance with port and facility protocols to increase the security of commerce bound for the U.S. The Coast Guard also published eight Port Security Advisories (PSAs) to provide guidance to the maritime community on security issues related to piracy.
- The Coast Guard equipped and trained additional air stations around the country to increase its Airborne Use of Force (AUF) capability. AUF-capable helicopters offer a rapid and potent deterrence and response to terrorist threats.
- As of July 15, 2010, the Transportation Security Administration (TSA) has issued nearly 1.5 million Transportation Worker Identification Credential (TWIC). The Coast Guard began full-time enforcement of TWIC regulations nationwide on April 15, 2009. Since then, the Coast Guard inspected TWICs in port facilities throughout the U.S.
- The Coast Guard updated the Nation's 43 Area Maritime Security Plans in coordination with respective Area Maritime Security Committees. The revisions incorporate lessons learned from recent hurricanes to enhance the recovery of the MTS. Per SAFE Port Act requirements, the plans now integrate the DHS Strategy to Enhance International Supply Chain Security and Salvage Response Plans. The new plans align Coast Guard exercises with the Homeland Security Exercise and Evaluation Program.
- Coast Guard FORCECOM training teams conducted PWCS Weapons of Mass Destruction (WMD) equipment training. 3,826 Coast Guard personnel assigned to boarding teams learned how to use detection gear and properly wear and maintain protective clothing.
- At 12 designated, key seaports, the Coast Guard developed Underwater Terrorism Preparedness Plans. The preparation, maintenance and exercising of these plans increases the Coast Guard's ability to deter and respond to the threat of underwater attack.
- Coast Guard Maritime Force Protection Units (MFPU) Bangor, WA, and Kings Bay, GA, each received a new 87-foot cutter and 64-foot escort boat and crews. MFPU's protect Navy ballistic missile submarines from terrorist and other threats.
- Coast Guard conducted over 14,000 inspections on U.S.-flagged vessels.
- Coast Guard conducted 6,900 dockside safety exams on commercial fishing vessels.
- Coast Guard screened over 75,000 foreign vessel arrivals and conducted over 9,500 Safety of Life at Sea (SOLAS) safety compliance exams and over 8,700 ISPS security compliance exams.

- Coast Guard issued 73,168 credentials to qualified merchant mariners, ensuring the safe, secure, and efficient navigation of ships.

Conclusion

Port security and the resiliency of the MTS rely on an integrated approach to safety and security in order to prevent, disrupt or respond to terrorist attacks or major marine incidents. The Coast Guard's operational model is flexible, adaptive, efficient and capable of succeeding in various maritime scenarios to achieve these goals.

While much has been accomplished to protect the MTS, there is also much more to be done. Opportunity remains to strengthen partnerships, improve maritime domain awareness through existing sensor integration and interagency cooperation, enhance public vigilance, and refine collaborative security regimes. The Coast Guard is committed to working hand-in-hand with international partners and domestic stakeholders, including recreational waterway users, commercial maritime interests and law enforcement partners, to ensure a resilient MTS and the safety of American citizens. Thank you for the opportunity to testify today. I welcome your questions.

The CHAIRMAN. Thank you, Admiral, very much.

And now Alan Bersin, who is Commissioner of U.S. Customs and Border Protection, Homeland Security.

**STATEMENT OF HON. ALAN BERSIN, COMMISSIONER,
U.S. CUSTOMS AND BORDER PROTECTION,
DEPARTMENT OF HOMELAND SECURITY**

Mr. BERSIN. Good afternoon, Mr. Chairman, Madam Ranking Member, Senator Lautenberg.

As the Commissioner of Customs and Border Protection, it's a privilege to appear before you as you take on the important—indeed, critical—task of taking a look at the SAFE Port Act of 2006 and preparing for its reauthorization.

We know that the central challenge here is to secure the flow of goods in and out of the United States, and to do so in ports that are safe and secure. It seems to us that there is a central challenge we must confront, and that will take up much of the dialogue we have here this afternoon; which is that we must find a way to both enhance the security of our ports and the flow of our goods at the same time that we provide for an economically prosperous America and an economically competitive America.

From the perspective of Customs and Border Protection, we understand the task to consist of two major dimensions: first, risk management, and understanding and taking risk management and its associated concepts to the next level; and second, building on the partnerships that will be essential between the private sector and the government to ensure the kind of security and facilitation we seek.

Preventing and disrupting terrorist threats, including chemical, radiological, biological, and nuclear attacks, are at the core of the CBP mission. We pursue a comprehensive and global strategy, as part of the DHS family of agencies, to secure containerized cargo. While inspections and operations at our ports are a key component of our strategy, to fully meet our responsibilities, we must identify and stop threats before they arrive at American ports. This requires that we secure the flow of cargo at each stage of the supply chain—at the port of origin, while in transit, and when it arrives in the United States. To accomplish this, CBP pursues a multi-layered approach to security, using a risk management approach

that allows us to apply resources to prioritize enforcement objectives.

At the core of our approach to risk management is the notion that our borders are not merely juridical lines on a map—they're not simply the physical barriers that separate us from foreign nations—but, rather, borders need to be conceptualized as the flow of goods and people, and it is the job of CBP, in the concert with other agencies in the government, to stop dangerous people and dangerous things from approaching the homeland and entering our country, doing harm to our people.

At the same time, we have an important role to play in trade facilitation, in building an economically prosperous America. Although often presented as being in tension or conflict, our security and trade facilitation missions, indeed, are mutually supportive. By utilizing risk-based strategies and applying a multilayered approach, we can focus our time and resources on the small percentage of goods that are high-risk or about which we know the least, which, in turn, allows us to expedite trade that is low-risk or about which we already know a great deal.

Our multilayered approach is based on the following core elements: obtaining information about the cargo, and those involved in moving it, early in the process; using advanced targeting techniques and sophisticated algorithms to assess risk in building a knowledge base about the people and the companies involved in the supply chain; partnering with the private sector to secure that supply chain; collaborating with other Federal agencies and departments, such as the U.S. Coast Guard, the Food and Drug Administration, the Consumer Product Safety Commission, Immigration and Customs Enforcement, and the Department of Agriculture, among 40 other agencies for which CBP serves as the executive agent at our ports of entry—seaports, landports, and airports; working with foreign governments to foster an effective working relationship between and among customs regimes; and maintaining robust inspection regimes, including non-intrusive inspection equipment and radiation detection technologies, at our ports of entry.

As detailed in my written statement, which the Chairman has deemed accepted, we're pursuing a number of different initiatives as part of our approach to secure containerized cargo. Some of the more notable are trusted-shipper programs, the Customs-Trade Partnership Against Terrorism, C-TPAT, and the prescreening programs, Container Security Initiative, and the Secure Freight Initiative.

Frankly, Mr. Chairman, Ranking Member Hutchison, it's time that we look at these programs, brilliantly conceived and supported by the Congress, that need to get to the next generation. We need to get to the next level of Secure Freight Initiative, CSI, and C-TPAT.

We must also leverage the unique capabilities of the National Targeting Center Cargo to proactively analyze advance cargo information using the Automated Targeting System before shipments reach the United States.

As you know, CBP requires advance electronic cargo information for all inbound shipments in all modes of transportation, and then

uses advance targeting to identify potential threats. This is the essence of the risk management process.

We require the electronic transmission of data, as mandated by the SAFE Port Act, through the Importer Security Filing and Additional Carrier Requirements rule, the so-called “10 plus 2,” which went into full effect in January of this year. With 10 additional data elements from the importer and 2 from the carrier regarding the stowage plan, “10 plus 2” allows CBP targeting specialists to identify risk factors earlier in the supply chain and further in time and space from the U.S. homeland.

And finally, I know that the 100-percent scanning requirement, as a matter of law, remains of interest to this Congress and to our Department. We have been advancing the screening requirement through pilot projects at five foreign seaports. We’ve learned much from these pilots, but they have also demonstrated a number of significant challenges to the 100-percent requirement. These include limitations with currently available technology, logistical challenges with the design and layout of foreign ports, and the high cost of implementation. As Secretary Napolitano has informed the Congress, the Department will need to seek the time extensions authorized by law as we work with the Congress to a more permanent solution to the issues of security at our ports. The Secretary, as you know, is committed to working with the Congress on this issue.

Mr. Chairman, members of the Committee, thank you again for this opportunity. I look forward to our dialogue and to responding to your questions regarding the terms and conditions of the reauthorization of the SAFE Port Act.

Thank you, sir.

[The prepared statement of Mr. Bersin follows:]

PREPARED STATEMENT OF HON. ALAN BERSIN, COMMISSIONER, U.S. CUSTOMS AND BORDER PROTECTION, DEPARTMENT OF HOMELAND SECURITY

Chairman Rockefeller, Ranking Member Hutchison, esteemed members of the Committee, it is a privilege and an honor to appear before you today to discuss U.S. Customs and Border Protection’s (CBP) work to secure the flow of goods into and out of the United States—preventing smuggling and protecting the country from dangerous shipments while expediting legitimate commerce. CBP pursues a multilayered approach to security, using a risk management approach that allows us to strategically apply resources to prioritized enforcement objectives and threats.

CBP is at the frontline of protecting the Nation from threats, including those posed by containerized cargo. At the core of that mission is preventing chemical, radiological, biological, and nuclear threats, and preventing and disrupting terrorist attacks arising from border crossings. We also stem the illegal flow of drugs, contraband and people, protect our agricultural and economic interests from harmful pests and diseases, protect American businesses from theft of their intellectual property, enforce textile agreements, determine and track import safety violations, regulate and facilitate international trade, collect import duties, facilitate legitimate travel, and enforce U.S. trade laws. In Fiscal Year 2009, CBP screened 100 percent of the maritime containers arrived at our seaports through our multilayered approach—9.8 million in all.

While security is our core mission, CBP also has important trade responsibilities. Our security and trade facilitation missions are mutually supportive: by utilizing risk-based strategies, and applying a multilayered approach, we can focus our time and resources on the small percentage of goods that are high-risk or about which we know the least, which in turn allows us to expedite trade that is low-risk or about which we already know a great deal.

Overview of CBP Approach

We are operating in the age of integrated global supply chains, and our approach to this environment must be equally comprehensive and global. While inspections and operations at our ports are a key component of our strategy, to fully meet our responsibilities, we must identify and stop threats before they arrive at American ports. This requires that we secure the flow of cargo at each stage of the supply chain—at the point of origin, while in transit, and when it arrives in the United States.

Our multilayered security approach involves:

- Obtaining information about cargo and those involved in moving it early in the process;
- Using advanced targeting techniques to assess risk and building a knowledge base about the people and companies involved in the supply chain;
- Fostering partnerships with the private sector and collaborating with other Federal agencies and departments, such as the U.S. Coast Guard, Department of Health and Human Services, the Consumer Product Safety Commission, Immigration and Customs Enforcement, and the Department of Agriculture, and with foreign governments, including through information sharing;
- Expanding enforcement efforts to points earlier in the supply chain than simply our borders; and
- Maintaining robust inspection regimes, including non-intrusive inspection equipment and radiation detection technologies, at our ports of entry.

We have asked the trade community to assume its fair share of the burden as well, to exercise reasonable care in customs matters, to provide information to better understand the parties to a transaction, and to invest in the resources necessary to keep up with current requirements. CBP strives to provide an environment built upon predictability, transparency, and uniformity in the importing process. We weigh the cumulative costs of our decisions on business and, when possible, provide for simplified commercial processing. CBP and the trade community must be partners, leveraging both parties' expertise.

In addition to addressing security concerns, CBP has also been aggressive in addressing other public safety concerns, such as product safety. CBP has established the Commercial Targeting and Analysis Center (CTAC), which is solely dedicated to import safety concerns. The Import Safety CTAC serves as a fusion center for CBP and other government agencies—including the Consumer Product Safety Commission, the Food and Drug Administration and the Food Safety Inspection Service—to combine resources and manpower to protect the American public from harm that could be caused by unsafe imported products. CBP looks forward to the expansion of this targeting center to include the participation of additional agencies.

With that background, I would like to discuss the operational initiatives that help us fulfill the security, trade and public safety missions I have outlined.

Advance Information

CBP requires advanced electronic cargo information, as mandated in the Trade Act of 2002 (24-Hour Rule, through regulations), for all inbound shipments in all modes of transportation. CBP requires the electronic transmission of additional data, as mandated by the SAFE Port Act, through the Importer Security Filing and Additional Carrier Requirements rule (Security Filing "10+2"), which became effective as an Interim Final Rule on January 26, 2009, and went into full effect on January 26, 2010. Under the Security Filing "10+2" rule, importers are responsible for supplying CBP with ten trade data elements 24 hours prior to vessel lading, and ocean carriers are required to provide their vessel stow plans no later than 48 hours after departure and their container status messages no later than 24 hours after creation or receipt. This advance data allows CBP targeting specialists to identify risk factors earlier in the supply chain. Security Filing "10+2" joins the 24 hour rule, and the C-TPAT program and CSI discussed below, in collecting advanced information to improve CBP's targeting efforts.

As part of CBP's layered targeting strategy, the National Targeting Center—Cargo (NTC-C) proactively analyzes advance cargo tactical and strategic information using the Automated Targeting System (ATS) before shipments reach the United States. ATS provides uniform review of cargo shipments for identification of the highest threat shipments, and presents data in a comprehensive, flexible format to address specific intelligence threats and trends. Through targeting rules, the ATS alerts the user to data that meets or exceeds certain predefined criteria. National targeting rule sets have been implemented in ATS to provide threshold targeting for national security risks for all modes of transportation—sea, truck, rail, and air.

ATS is a decision support tool for CBP officers working in the NTC-C and in Advanced Targeting Units at our ports of entry and CSI ports abroad.

Once NTC-C has analyzed the advanced information using ATS and other tools, intelligence briefs are created and disseminated to officers in the field. This information is used by CBP and other agencies to support enforcement actions, such as seizures and arrests.

NTC-C has established partnerships and liaisons with other agencies, both domestically and abroad. Partnerships with Immigration and Customs Enforcement, the Drug Enforcement Administration, the Financial Crimes Enforcement Network, the Department of Commerce, and the Department of Health and Human Services promote information sharing and the exchange of best practices, while collaboration with foreign governments results in seizures and detection of threats at our borders and in foreign ports.

Customs Trade Partnership Against Terrorism (C-TPAT)

CBP works with the trade community through the Customs Trade Partnership Against Terrorism (C-TPAT), a voluntary public-private partnership program wherein some members of the trade community adopt tighter security measures throughout their international supply chain and in return are afforded benefits such as reduced exams, front of line examination privileges to the extent possible and practical, and an assigned Supply Chain Security Specialist who helps them maintain compliance. C-TPAT has enabled CBP to leverage private sector resources to enhance supply chain security.

Prospective C-TPAT members submit basic company information and a security profile through an Internet-based portal system. CBP conducts records checks on the company in its law enforcement and trade databases and ensures the company meets the security criteria for its particular business sector. Members who pass extensive vetting are certified into the program. Using a risk-based approach, CBP Supply Chain Security Specialists conduct on-site visits of foreign and domestic facilities to confirm that the security practices are in place and operational.

C-TPAT has been a success—membership in the program has grown from 7 companies in its first year to 9,897 as of July 8, 2010. C-TPAT's certified partners include 4,416 importers, 2,739 carriers, 843 brokers, 809 consolidators/third-party logistic providers, 59 Marine Port Authority and Terminal Operators, and 1,031 foreign manufacturers. C-TPAT has conducted 15,207 onsite validations of manufacturing and logistics facilities in 90 countries. Of those in the program, 313 C-TPAT importer partners have been granted the highest level of program benefits having qualified for Tier 3 status, which means that these companies have exceeded C-TPAT's security requirements.

Additionally, CBP is working with foreign partners to establish bi-national recognition and enforcement of C-TPAT. CBP currently has signed mutual recognition agreements with New Zealand (2007), Canada (2008), Jordan (2008), Japan (2009), and Korea (2010). We are continuing to work toward similar recognition with the European Union and other countries.

Container Security Initiative

CBP partners with foreign governments through the Container Security Initiative (CSI) to prevent and deter terrorist threats before they reach American ports. CSI enables CBP to identify and inspect high-risk U.S.-bound cargo containers at foreign ports prior to departure. Through CSI, CBP stations multidisciplinary teams of officers to work with host country counterparts to identify and examine containers that are determined to pose a high risk for terrorist activity. CSI, the first program of its kind, was announced in January 2002 and is currently operational in 58 foreign seaports—covering more than 80 percent of the maritime containerized cargo shipped to the United States.

CBP officers stationed at CSI ports, with assistance from CSI targeters at the National Targeting Center-Cargo (NTC-C), review 100 percent of the manifests originating and/or transiting those foreign ports for containers that are destined for the United States. In this way, CBP identifies and examines high risk containerized maritime cargo prior to lading at a foreign port and before shipment to the United States. In FY 2009, CBP officers stationed at CSI ports reviewed over 9 million bills of lading and conducted over 56,000 exams in conjunction with their host country counterparts.

As the CSI program has matured, CBP looked for opportunities to increase efficiencies and reduce costs by shifting functions to the NTC-C. CBP's ability to target high risk containers has progressed to the point that much of the work can be done from CBP's U.S. location rather than through a physical presence overseas. CBP is exploring opportunities to utilize emerging technology in some locations, which will

allow the program to become more efficient and less costly. In January 2009, CBP began to reduce the number of personnel stationed overseas who perform targeting functions, increasingly shifting the targeting of high risk containers to personnel stationed at the NTC-C. This shift in operations reduces costs without diminishing the effectiveness of the CSI program. CBP will remain operational in all 58 locations in Fiscal Year 2011 with sufficient personnel in country to conduct the examinations of high risk shipments with the host government and to maintain relationships with their host-country counterparts.

Secure Freight Initiative

The Secure Freight Initiative (SFI) is an effort to enhance the U.S. government's ability to scan containers for nuclear and radiological materials at seaports worldwide and better assess the risk of inbound containers. This initiative is the culmination of our work with other Federal agencies, foreign governments, the trade community, and vendors of cutting-edge technology. SFI provides carriers of maritime containerized cargo greater confidence in the security of the shipment they are transporting, and increases the likelihood of an uninterrupted and secure flow of commerce.

In advancing the goal of 100 percent scanning, the Secure Freight Initiative (SFI) deploys networks of radiation detection, provided by the Department of Energy, our partner in SFI, and imaging equipment at five overseas pilot ports. This advanced pilot has encountered a number of serious challenges to implementing the 100 percent scanning mandate.

Certain challenges are logistical. Many ports simply do not have one area through which all the cargo passes; there are multiple points of entry, and cargo is "trans-shipped," meaning it is moved immediately from vessel to vessel within the port. These ports are not configured to put in place detection equipment or to provide space for secondary inspections. At these ports, scanning 100 percent of cargo with current systems is currently unworkable without seriously hindering the flow of shipments or redesigning the ports themselves, which would require huge capital investment.

Other challenges are the limitations that are inherent in available technology. DHS currently uses both passive radiation detection and active x-ray scanning to look for radioactive material in cargo. An important obstacle is the absence of x-ray scanning technology which can effectively and automatically detect suspicious anomalies within cargo containers that should trigger additional inspection. Currently, DHS personnel visually inspect screens for possible anomalies, but the scale and the variety of container cargo make this process challenging and time-consuming. In addition, current x-ray systems have limited penetration capability; this can limit their ability to find a device in very dense cargo.

While DHS is pursuing technological solutions to these problems, expanding screening with available technology would slow the flow of commerce and drive up costs to consumers without bringing significant security benefits.

Finally, and on that note, the costs of 100 percent scanning pose a great challenge, particularly in a struggling economy. Deploying SFI-type scanning equipment would cost about \$8 million per lane for the more than 2,100 shipping lanes at more than 700 ports around the world that ship to the United States. On top of these initial costs, operating costs would be very high. These include only DHS expenses, not the huge costs that would have to be borne by foreign governments or industry. It is also important to keep in mind that about 86 percent of the cargo shipped to the United States is sent from only 58 of those more than 700 ports. Installing equipment and placing personnel at all of these ports—even the tiny ones—would strain government resources without a guarantee of results.

Thus, in order to implement the 100 percent scanning requirement by the 2012 deadline, DHS would need significant resources for greater manpower and technology, technologies that do not currently exist, and the redesign of many ports. As Secretary Napolitano has indicated, these are all prohibitive challenges that will require the Department to seek the time extensions authorized by law.

Non Intrusive Inspection/Radiation Detection Technology

The deployment of imaging systems and radiation detection equipment has made a tremendous contribution to CBP's progress in securing the supply chains that bring goods into the United States from around the world against exploitation by terrorist groups. Non-Intrusive Inspection (NII) technology serves as a force multiplier that allows officers to detect possible anomalies between the contents of a container and the manifest. CBP's use of NII allows us to work smarter and more efficiently in recognizing potential threats.

CBP has aggressively deployed NII and RPM technology. Prior to 9/11, not a single Radiation Portal Monitor (RPM), and only 64 large-scale NII systems, were deployed to our country's borders. Today, CBP uses RPMs to scan 99 percent of all cargo arriving in the U.S. by land and sea. CBP, in partnership with the DHS Domestic Nuclear Detection Office (DNDO) and Pacific Northwest National Laboratory (PNNL), has deployed 493 RPMs at northern border land ports of entry; 392 RPMs at southern border land ports of entry; 451 RPMs at seaports; and 52 RPMs at mail facilities. Currently, CBP has 267 large-scale NII systems deployed. Additionally, CBP has deployed over 1,700 Radiation Isotope Identifier Devices (RIIDs) and over 20,000 Personal Radiation Detectors (PRDs). These devices allow CBP to examine 100 percent of all identified high-risk cargo. To date, CBP has used the deployed NII systems to conduct over 42 million examinations, resulting in over 8,300 narcotic seizures, with a total weight of over 2.6 million pounds, and over \$28.6 million in undeclared currency seizures. Since RPM program inception in 2002, CBP has scanned over 438 million conveyances for radiological contraband, resulting in over 2.7 million alarms. CBP's Laboratories and Scientific Services 24/7 Teleforensic Center spectroscopy group at the National Targeting Center has responded to over 23,000 requests from the field for technical assistance in resolving alarms. To date, 100 percent of alarms have been successfully adjudicated as innocent, legitimate trade, legitimate transportation, or non-terrorism related.

Conclusion

Mr. Chairman, Members of the Committee, thank you again for this opportunity to testify about CBP's commitment to enhancing cargo security. We look forward to continuing to work with the Committee on this issue. I will be happy to answer any of your questions.

The CHAIRMAN. Thank you, sir.

And then, finally, we hear from Stephen Caldwell, who is Director, Homeland Security and Justice Issues, working in the U.S. Government Accountability Office, known as the GAO.

STATEMENT OF STEPHEN L. CALDWELL, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. CALDWELL. Thank you very much, Chairman Rockefeller. And nice to be here, Senator Hutchison and Senator Lautenberg.

Let me summarize my written statement, which has four main topics: risk management, the small vessel threat, foreign port security, and container security.

Risk management, as required by the Homeland Security Act, should continue to be the guiding principle, in terms of protecting our ports and the seas beyond. Since GAO's original work looking at risk management used in ports and for other infrastructure, the Coast Guard has made a great deal of progress in developing models and methodologies that can be used, not only to assess risk, but to adjust operations and make resource decisions.

I think the important thing for all of us to remember about risk management is it's about managing risks, not eliminating them. Risk management will still require some level of judgment by our government officials and other maritime stakeholders. We won't be able to prevent all threats at all times. At the Committee's request, we plan to conduct additional work at ports, which, among other things, will look at how the Coast Guard is using MSRAM to adjust risks, and even reduce them.

In terms of the small vessel threat, this continues to be one of the most vexing problems in security in our ports and coastal areas. Our small boats are large in number, anonymous in their movement, and ominous in their capabilities.

Current systems for tracking vessels, in some ways, are geared more for tracking the vessels as targets than they are for tracking the small vessels that might be attacking them. While the Coast Guard has activities in place to provide waterborne escorts to protect cruise ships and hazardous tankers, the Coast Guard does not have the resources to escort all of them. Even in places with robust State and local law enforcement assistance, it would be very difficult to prevent an unexpected attack by a determined terrorist group using small vessels. Some steps to mitigate the risks have already been mentioned, such as expanding America's Waterway Watch Program, and another one would be to expand District 11's "Operation Focused Lens" Program. It has now been 2 years since DHS issued its Small Vessel Security Strategy, so we look forward for the Department to issue the implementation plan to go with it.

Security in our home ports begins at the foreign ports, where crews and cargoes and passengers are loaded on vessels that are bound for the United States. The Coast Guard's program for assessing the security at foreign ports has matured considerably, as they are now in their third round of visits. Despite the progress, there will always be some inherent challenges in this program, related to foreign nation sovereignty as well as their own resource limitations. Coast Guard visits to these nations are always going to be somewhat limited in scope and duration, so they will remain a snapshot of security in place at the ports we visit and when we visit.

As we indicated in our earlier report, this is an area where the Coast Guard could benefit from risk management, concentrating its efforts on nations where perhaps risks are the greatest.

Regarding container security, the statutory requirement to double-scan 100 percent of all inbound containers continues to be a difficult issue, as Mr. Bersin has already noted. While two of the Secure Freight Initiative pilot ports achieved relatively high levels of scanning, the other pilot ports ran into a number of implementation problems.

In its most recent budget, CBP proposed to downgrade three of the SFI ports to the CSI level, and the budget did not have any new funds for the Strategic Trade Corridor, which the Secretary had previously approved as one potential way to advance toward 100-percent scanning.

Our most recent report on SFI made recommendations to CBP to conduct feasibility analysis, improve some of their cost estimates, conduct certain economic analysis, and provide different alternatives to Congress. And this hearing may, in some ways, help advance that last recommendation.

Some of the alternative solutions suggested by CBP to the 100-percent scanning, such as "10 plus 2" and improved technologies, for both containers themselves and for the scanning equipment, are being pursued. We have work underway on all of these efforts, and will complete those reports later this year.

In closing, thank you very much for letting me appear here, and I'm happy to answer any questions about GAO's work on maritime security.

Thank you.

[The prepared statement of Mr. Caldwell follows:]

PREPARED STATEMENT OF STEPHEN L. CALDWELL, 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 port security issues and their related challenges. Ports, waterways, and vessels are part of an economic engine handling more than \$700 billion in merchandise annually, according to the Department of Homeland Security (DHS), and an attack on this system could have a widespread impact on global shipping, international trade, and the global economy. Balancing security concerns with the need to facilitate the free flow of people and commerce remains an ongoing challenge for the public and private sectors alike. Within DHS, component agencies have responsibility for securing the maritime environment. The U.S. Coast Guard is responsible for protecting the public, the environment, and U.S. economic and security interests in any maritime region in which those interests may be at risk, including America's coasts, ports, and inland waterways. U.S. Customs and Border Protection (CBP) is responsible for keeping terrorists and their weapons out of the United States, securing and facilitating trade, and cargo container security.

Various laws have been enacted since the September 11, 2001 terrorist attacks to strengthen port security. The Homeland Security Act of 2002¹ charges DHS with establishing a risk management framework across the Federal Government to protect the Nation's critical infrastructure and key resources. In addition, much of a new port security framework was set in place by the Maritime Transportation Security Act of 2002 (MTSA).² Enacted in November 2002, MTSA was designed, in part, to help protect the Nation's ports and waterways from terrorist attacks by requiring a wide range of security improvements. Among the requirements included in MTSA were: (1) conducting vulnerability assessments for port facilities and vessels; (2) developing security plans to mitigate identified risks for the national maritime system, ports, port facilities, and vessels; and (3) establishing a process to assess foreign ports from which vessels depart on voyages to the United States. The Security and Accountability For Every (SAFE) Port Act of 2006 later directed the Secretary of Homeland Security to, among other things, increase the security of container cargo bound for the United States by requiring CBP to establish a pilot program to test the feasibility of scanning 100 percent of U.S.-bound containers at foreign ports.³ Further, in August 2007, the Implementing Recommendations of the 9/11 Commission Act were enacted and provide, among other things, that by July 2012, a container loaded on a vessel in a foreign port shall not enter the United States unless that container is scanned before it is loaded onto the vessel.⁴

My statement today is based on related GAO reports and testimonies issued from December 2005 through June 2010 addressing risk management and port security, and also includes selected updates—conducted in July 2010—to the information provided in these products and on the actions agencies have taken to address recommendations made in these products that are also discussed in this statement. These products include our assessment of the progress that DHS and its component agencies have made to strengthen port security, the challenges that remain, and recommendations for improvement.⁵ The details on the scope and methodology for those reviews are available in our published products. The selected updates include a review of: (a) the Coast Guard's and CBP's Fiscal Year 2011 Congressional budget justification and (b) CBP's Fiscal Year 2010 Report to Congress on supply chain security. In particular, my statement addresses the extent to which DHS and its component agencies have made progress and face challenges regarding: (1) strengthening risk management, (2) reducing the risk of small-vessel threats,⁶ (3) implementing foreign port assessments, and (4) enhancing supply chain security. We conducted this work in accordance with generally accepted government auditing standards.

¹Pub. L. No. 107-296, § 201, 116 Stat. 2135, 2144 (2002).

²Pub. L. No. 107-295, 116 Stat. 2064 (2002).

³Pub. L. No. 109-347, § 231, 120 Stat. 1884, 1915-16 (2006).

⁴Pub. L. No. 110-53, § 1701(a), 121 Stat. 266, 489-90 (2007). The law defines scanning to be an examination with both nonintrusive imaging equipment and radiation detection equipment. In addition, while the law states that cargo containers are not to enter the United States unless they were scanned at a foreign port, actual participation in the program by sovereign foreign governments and ports is voluntary.

⁵See the list of related GAO products at the end of this statement.

⁶According to DHS's *Small Vessel Security Strategy*, "small vessels" are characterized as any watercraft—regardless of method of propulsion—less than 300 gross tons, and used for recreational or commercial purposes.

In summary, DHS and its component agencies—the Coast Guard and CBP—have taken various actions to implement port security legislation and enhance port security. These efforts include: (1) the Coast Guard’s development of a risk assessment model to help prioritize limited resources; (2) DHS and the Coast Guard’s development of a strategy and programs to reduce the risks associated with small vessels, such as a community outreach program, vessel tracking systems, and security operations; (3) the Coast Guard’s implementation of the International Port Security Program to assess security measures in foreign ports; and (4) CBP’s efforts to scan U.S.-bound cargo containers. Although these initiatives have helped to improve port security, challenges remain, including resource constraints; the lack of technology to track and identify small vessels; sovereignty concerns over the Coast’s Guard’s visits to foreign ports; and a variety of political, logistical, and technological barriers to scanning all cargo containers. We have made recommendations to DHS in prior reports to help address these challenges, and DHS generally concurred with our recommendations in these reports.

The Coast Guard Has Made Progress in Improving Its Risk Management

In December 2005, we reported that risk management, a strategy for helping policymakers make decisions about assessing risks, allocating resources, and taking actions under conditions of uncertainty, had been endorsed by Congress and the President as a way to strengthen the Nation against possible terrorist attacks against ports and other infrastructure.⁷ Risk management has long been used in such areas as insurance and finance, but at the time its application to domestic terrorism had no precedent. We noted that unlike storms and accidents, terrorism involves an adversary with deliberate intent to destroy, and the probabilities and consequences of a terrorist act are poorly understood and difficult to predict. The size and complexity of homeland security activities and the number of organizations involved—both public and private—add another degree of difficulty to the task.

We have examined Coast Guard efforts to implement risk management for a number of years, noting how the Coast Guard’s risk management framework developed and evolved. In 2005, we reported that of the three components GAO reviewed—the Coast Guard, the Office for Domestic Preparedness (this office’s function is now within the Federal Emergency Management Agency), and the Information Analysis and Infrastructure Protection Directorate (now the National Protection and Preparedness Directorate)—the Coast Guard had made the most progress in establishing a foundation for using a risk management approach. While the Coast Guard had made progress in all five risk management phases,⁸ its greatest progress had been made in conducting risk assessments—that is, evaluating individual threats, the degree of vulnerability in maritime facilities, and the consequences of a successful attack.⁹ However, we reported that those assessments were limited because they could not compare and prioritize relative risks of various infrastructures across ports. At the time the Coast Guard had actions under way to address the challenges it faced in each risk management phase and we did not make recommendations in those areas where the Coast Guard had actions well under way. Several of these actions were based, in part, on briefings GAO held with agency officials. Our recommendations were designed to spotlight those areas in which additional steps were most needed to implement a risk management approach to Coast Guard port security activities. We recommended that the Coast Guard take action to:

- establish a stronger linkage between local and national risk assessment efforts—an action that could involve, for example, strengthening the ties between local assessment efforts, such as area maritime security plans, and national risk assessment activities; and

⁷ GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005).

⁸ The five phases of the risk management framework developed by GAO are: (1) setting strategic goals and objectives, and determining constraints; (2) assessing the risks; (3) evaluating alternatives for addressing these risks; (4) selecting the appropriate alternatives; and (5) implementing the alternatives and monitoring the progress made and results achieved.

⁹ Risk assessment is a function of: (1) threat—the likelihood that a particular asset, system, or network will suffer an attack or an incident; (2) vulnerability—the likelihood that a characteristic of, or flaw in, an asset’s, system’s, or network’s design, location, security posture, process, or operation renders it susceptible to destruction, incapacitation, or exploitation by terrorist or other intentional acts, mechanical failures, and natural hazards; and (3) consequence—the negative effects on public health and safety, the economy, public confidence in institutions, and the functioning of government, both direct and indirect, that can be expected if an asset, system, or network is damaged, destroyed, or disrupted by a terrorist attack, natural disaster, or other incident.

- ensure that procedures for evaluating alternatives and making management decisions consider the most efficient use of resources—actions that could entail, for example, refining the degree to which risk management information is integrated into the annual cycle of program and budget review.

Since we made those recommendations, both DHS and the Coast Guard have made progress implementing a risk management approach toward critical infrastructure protection. In 2006, DHS issued the National Infrastructure Protection Plan (NIPP), which is DHS's base plan that guides how DHS and other relevant stakeholders should use risk management principles to prioritize protection activities within and across each critical infrastructure sector in an integrated and coordinated fashion.¹⁰ In 2009, DHS updated the NIPP to, among other things, increase its emphasis on risk management, including an expanded discussion of risk management methodologies and discussion of a common risk assessment approach that provided core criteria for these analyses.¹¹ For its part, the Coast Guard has made progress assessing risks and integrating the results of its risk management efforts into resource allocation decisions. Regarding risk assessments, the Coast Guard transitioned its risk assessment model from the Port Security Risk Assessment Tool (PS-RAT) to the Maritime Security Risk Assessment Model (MSRAM). In 2005 we reported that the PS-RAT was designed to allow ports to prioritize resource allocations within, not between, ports to address risk most efficiently. However, the new MSRAM can assess risk across ports and is used by every Coast Guard unit and assesses the risk—threats, vulnerabilities, and consequences—of a terrorist attack based on different scenarios; that is, it combines potential targets with different means of attack, as recommended by the NIPP. The Coast Guard uses the model to help implement its strategy and concentrate maritime security activities when and where relative risk is believed to be the greatest. According to the Coast Guard, the model's underlying methodology is designed to capture the security risk facing different types of targets, allowing comparison between different targets and geographic areas at the local, regional, and national levels. We have also reported that the Federal Emergency Management Agency has included MSRAM results in its Port Security Grant Program guidelines as one of the data elements included in determining grant awards to assist in directing grants to the ports of greatest concern or at highest risk.

With regard to the integration of risk management results into the consideration of risk mitigation alternatives and the management selection process, Coast Guard officials stated that the Coast Guard uses MSRAM to inform allocation decisions, such as the deployment of local resources and grants. We have also reported that at the national level, the Coast Guard uses MSRAM results for: (1) long-term strategic resource planning, (2) identifying capabilities needed to combat future terrorist threats, and (3) identifying the highest-risk scenarios and targets in the maritime domain. For example, Coast Guard officials reported that results are used to refine the Coast Guard's requirements for the number of required vessel escorts and patrols of port facilities. At the local level, the Captain of the Port¹² can use MSRAM as a tactical planning tool. The model can help identify the highest risk scenarios, allowing the Captain of the Port to prioritize needs and better deploy security assets.¹³ The 2011 Congressional Budget Justification showed that the Coast Guard uses risk or relative risk to direct resources to the mitigation of the highest risk. For example, the use of risk management in the allocation of resources that is specific to port security concerns the Ports, Waterways, and Coastal Security program. This program has a performance goal to manage terror-related risk in the U.S. Mar-

¹⁰Critical infrastructure are systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. Homeland Security Presidential Directive 7 divided up the critical infrastructure in the United States into 17 industry sectors, such as transportation, energy, and communications, among others. In 2008, DHS established an 18th sector—Critical Manufacturing.

¹¹The framework for the updated NIPP includes six components: (1) set goals and objectives; (2) identify assets, systems, and networks; (3) assess risks; (4) prioritize; (5) implement programs; and (6) measure effectiveness. See GAO, *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*, GAO-10-296 (Washington, D.C.: Mar. 5, 2010).

¹²The Captain of the Port is the Coast Guard officer designated by the Commandant of the Coast Guard to enforce within his or her respective areas port safety and security and marine environmental protection regulations, including, without limitation, regulations for the protection and security of vessels, harbors, and waterfront facilities.

¹³For more information on the use of MSRAM see GAO, *Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain*, GAO-10-400 (Washington, D.C.: Apr. 9, 2010).

itime Domain to an acceptable level. The Coast Guard uses a program measure to direct resources to the programs that reduce risk the most based on the amount invested. Based on the development of the MSRAM assessment process and the use of risk management analysis results in its allocation of resources, we believe that the Coast Guard has addressed the recommendations discussed earlier concerning risk management.¹⁴

DHS and the Coast Guard Have Taken Several Actions to Address the Small-Vessel Threat but Challenges Remain in Mitigating the Risk

In recent years, we reported that concerns had arisen about the security risks posed by small vessels. In its April 2008 Small Vessel Security Strategy, DHS identified the four gravest risk scenarios involving the use of small vessels for terrorist attacks, which include the use of a small vessel as: (1) a waterborne improvised explosive device, (2) a means of smuggling weapons into the United States, (3) a means of smuggling humans into the United States, and (4) a platform for conducting a standoff attack—an attack that uses a rocket or other weapon launched at a sufficient distance to allow the attackers to evade defensive fire.¹⁵ According to the Commandant of the Coast Guard, small vessels pose a greater threat than shipping containers for nuclear smuggling.¹⁶ Some of these risks have been shown to be real through attacks conducted outside U.S. waters, but—as we reported in December 2009—no small-vessel attacks have taken place in the United States. Many vessels frequently travel among small vessels that operate with little scrutiny or notice, and some have suffered waterborne attacks overseas by terrorist or pirates who operated from small vessels. For example, at least three cruise ships have been attacked by pirates on small boats while armed with automatic weapons and rocket propelled grenades, although the three vessels were able to evade the pirates by either maneuvering or fighting back.¹⁷ Oil tankers have also been attacked. For example, in October 2002, a small vessel filled with explosives rammed the side of an oil tanker off the coast of Yemen.¹⁸ The concern about small-vessel attacks is exacerbated by the fact that some vessels, such as cruise ships, sail according to precise schedules and preplanned itineraries that could provide valuable information to terrorists in preparing for and carrying out an attack against a vessel.

DHS and the Coast Guard have developed a strategy and programs to reduce the risks associated with small vessels; however, they face ongoing challenges related to some of these efforts. The following discusses some of our key findings with regard to reducing the risks associated with small vessels:

- *Small Vessel Security Strategy.* DHS released its Small Vessel Security Strategy in April 2008, as part of its effort to mitigate the vulnerability of vessels to waterside attacks from small vessels, and the implementation plan for the strategy is under review. According to the strategy, its intent is to reduce potential security and safety risks posed by small vessels through operations that balance fundamental freedoms, adequate security, and continued economic stability.¹⁹ After review by DHS, the Coast Guard, and CBP, the draft implementation plan was forwarded to the Office of Management and Budget in April 2010, but the release of the plan has not been approved by the Office of Management and Budget.
- *Community Outreach.* Consistent with the Small Vessel Security Strategy's goal to develop and leverage strong partnerships with the small-vessel community, the Coast Guard, as well as other agencies—such as the New Jersey State Police, have several outreach efforts to encourage the boating community to share threat information; however, the Coast Guard program faces resource limita-

¹⁴ We have work planned for this committee to address a request concerning port security planning that will include a more detailed examination of MSRAM.

¹⁵ Department of Homeland Security, *Small Vessel Security Strategy* (Washington, D.C., April 2008).

¹⁶ From testimony delivered by Vice Admiral Thad Allen, Chief of Staff, United States Coast Guard, during a hearing on the Coast Guard role in border and maritime security, before the Committee on Appropriations, Subcommittee on Homeland Security, U.S. Senate (Apr. 6, 2006).

¹⁷ For more information on cruise ship security, see GAO-10-400.

¹⁸ GAO, *Maritime Security: Federal Efforts Needed to Address Challenges in Preventing and Responding to Terrorist Attacks on Energy Commodity Tankers*, GAO-08-141 (Washington, D.C.: December 10, 2007).

¹⁹ The goals of the Small Vessel Security Strategy are to: (1) develop and leverage a strong partnership with the small-vessel community and public and private sectors; (2) enhance maritime security and safety; (3) leverage technology to enhance the ability to detect, determine intent, and when necessary, interdict small vessels; and (4) enhance coordination, cooperation, and communications between Federal, state, local, and tribal stakeholders, the private sector, and international partners.

tions. For example, the Coast Guard's program to conduct outreach to the boating community for their help in detecting suspicious activity, America's Waterway Watch, lost the funding it received through a Department of Defense readiness training program for military reservists in Fiscal Year 2008. Now it must depend on the activities of the Coast Guard Auxiliary, a voluntary organization, for most of its outreach efforts. In addition to America's Waterway Watch, the Coast Guard piloted a regional initiative—Operation Focused Lens—to increase public awareness of suspicious activity in and around U.S. ports, and direct additional resources toward gathering information about the most likely points of origin for an attack, such as marinas, landings, and boat ramps. According to Coast Guard officials, the agency views Operation Focused Lens to be a best practice, and the agency is considering plans to expand the program or integrate it into other existing programs.

- *Vessel Tracking.* In December 2009, we reported that the Coast Guard was implementing two major unclassified systems to track a broad spectrum of vessels; however, these systems generally could not track small vessels.²⁰ The Coast Guard and other agencies have other technology systems, though—including cameras and radars—that can track small vessels within ports, but these systems were not installed at all ports or did not always work in bad weather or at night. Even with systems in place to track small vessels, there was widespread agreement among maritime stakeholders that it is very difficult to detect threatening activity by small vessels without prior knowledge of a planned attack.
- *Nuclear Material Detection Efforts.* DHS has developed and tested equipment for detecting nuclear material on small vessels; however, efforts to use this equipment in a port area have been limited to pilot programs. DHS is currently conducting 3-year pilot programs to design, field test, and evaluate equipment and is working with CBP, the Coast Guard, state, local, tribal officials, and others as they develop procedures for screening. These pilot programs are scheduled to end in 2010, when DHS intends to decide the future path of screening of small vessels for nuclear and radiological materials. According to DHS officials, initial feedback from Federal, state, and local officials involved in the pilot programs has been positive. DHS hopes to sustain the capabilities created through the pilot programs through Federal grants to state and local authorities through the port security grant program.²¹
- *Security Activities.* The Coast Guard also conducts various activities to provide waterside security including boarding vessels, escorting vessels into ports, and enforcing fixed security zones, although they are not always able to meet standards related to these activities. Through its Operation Neptune Shield, the Coast Guard sets the standards for local Coast Guard units to meet for some of these security activities. Although the Coast Guard units may receive some assistance from other law enforcement agencies in carrying out these security activities, Coast Guard data indicates that some units are not able to meet these standards due to resource constraints. However, the Coast Guard's guidance allows the Captain of the Port the latitude to shift resources to other priorities when deemed necessary, for example when resources are not available to fulfill all missions simultaneously. The planned decommissioning of five Maritime Safety and Security Teams—a domestic force for mitigating and responding to terrorist threats or incidents—may continue to strain Coast Guard resources in meeting security requirements. Although remaining teams are to maintain readiness to respond to emerging events and are to continue performing routine security activities, such as vessel escorts, their ability to support local units in meeting operational activity goals may be diminished.

The Coast Guard Has a Program in Place to Assess the Security of Foreign Ports, but Challenges Remain in Implementing the Program

The security of domestic ports also depends upon security at foreign ports where cargoes bound for the United States originate. To help secure the overseas supply chain, MTSA required the Coast Guard to assess security measures in foreign ports from which vessels depart on voyages to the United States and, among other things, recommend steps necessary to improve security measures in those ports. In re-

²⁰ For more information on vessel tracking systems, see GAO, *Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed*, GAO-09-337 (Washington, D.C.: Mar. 17, 2009).

²¹ For more information, see GAO, *Combating Nuclear Smuggling: DHS Has Made Some Progress but Not Yet Completed a Strategic Plan for Its Global Nuclear Detection Efforts or Closed Identified Gaps*, GAO-10-883T (Washington, D.C.: June 30, 2010).

response, the Coast Guard established a program, called the International Port Security Program, in April 2004. Under this program, the Coast Guard and host nations review the implementation of security measures in the host nations' ports against established security standards, such as the International Maritime Organization's International Ship and Port Facility Security (ISPS) Code.²² Coast Guard teams have been established to conduct country visits, discuss security measures implemented, and collect and share best practices to help ensure a comprehensive and consistent approach to maritime security in ports worldwide. Subsequently, in October 2006, the SAFE Port Act required the Coast Guard to reassess security measures at such foreign ports at least once every 3 years.

As we reported in October 2007, Coast Guard officials told us that challenges exist in implementing the International Port Security Program.²³ Reluctance by some countries to allow the Coast Guard to visit their ports due to concerns over sovereignty was a challenge cited by program officials in completing their first round of port visits. According to these officials, before permitting Coast Guard officials to visit their ports, some countries insisted on visiting and assessing a sample of U.S. ports. The Coast Guard was able to accommodate their request through the program's reciprocal visit feature in which the Coast Guard hosts foreign delegations to visit U.S. ports and observe ISPS Code implementation in the United States. This subsequently helped gain the cooperation of the countries in hosting a Coast Guard visit to their own ports. However, as Coast Guard program officials stated, sovereignty concerns may still be an issue, as some countries may be reluctant to host a comprehensive country visit on a recurring basis because they believe the frequency is too high.

Another challenge program officials cited is having limited ability to help countries build on or enhance their capacity to implement the ISPS Code requirements. Program officials stated that while their visits provide opportunities for them to identify potential areas to improve or help sustain the security measures put in place, other than sharing best practices or providing presentations on security practices, the program does not currently have the resources to directly assist countries, particularly those that are poor, with more in-depth training or technical assistance. To overcome this, program officials have worked with other agencies (*e.g.*, the Departments of Defense and State) and international organizations (*e.g.*, the Organization of American States) to secure funding for training and assistance to countries where port security conferences have been held (*e.g.*, the Dominican Republic and the Bahamas).

CBP Has Established a Program to Scan U.S.-Bound Cargo Containers, but Challenges to Expanding the Program Remain

Another key concern in maritime security is the effort to secure the supply chain to prevent terrorists from shipping weapons of mass destruction (WMD) in one of the millions of cargo containers that arrive at U.S. ports each year. CBP has developed a layered security strategy to mitigate the risk of an attack using cargo containers. CBP's strategy is based on a layered approach of related programs that attempt to focus resources on potentially risky cargo shipped in containers while allowing other cargo containers to proceed without unduly disrupting commerce into the United States. The strategy is based on obtaining advanced cargo information to identify high-risk containers, utilizing technology to examine the content of containers, and partnerships with foreign governments and the trade industry. One of the programs in this layered security strategy is the Secure Freight Initiative (SFI). In December 2006, in response to SAFE Port Act requirements, DHS, and the Department of Energy (DOE) jointly announced the formation of the SFI pilot program to test the feasibility of scanning 100 percent of U.S.-bound container cargo at three foreign ports (Puerto Cortes, Honduras; Qasim, Pakistan; and Southampton, United Kingdom). According to CBP officials, while initiating the SFI program at these ports satisfied the SAFE Port Act requirement, CBP also selected the ports of Busan, South Korea; Hong Kong; Salalah, Oman; and Singapore to more fully demonstrate the capability of the integrated scanning system at larger, more complex ports. As of April 2010, SFI has been operational at five of these seven seaports.

²²The International Port Security Program uses the ISPS Code as the benchmark by which it measures the effectiveness of a country's antiterrorism measures in a port. The code was developed after the September 11 attacks and established measures to enhance the security of ships and port facilities with a standardized and consistent security framework. The ISPS Code requires facilities to conduct an assessment to identify threats and vulnerabilities and then develop security plans based on the assessment. The requirements of this code are performance-based; therefore compliance can be achieved through a variety of security measures.

²³GAO, *Maritime Security. The SAFE Port Act. Status and Implementation One Year Later*, GAO-08-126T (Washington, D.C.: Oct. 30, 2007).

In October 2009, we reported that CBP has made some progress in working with the SFI ports to scan U.S.-bound cargo containers; but because of challenges to expanding scanning operations, the feasibility of scanning 100 percent of U.S.-bound cargo containers at over 600 foreign seaports remains largely unproven.²⁴ CBP and DOE have been successful in integrating images of scanned containers onto a single computer screen that can be reviewed remotely from the United States. They have also been able to use these initial ports as a test bed for new applications of existing technology, such as mobile radiation scanners. However, the SFI ports' level of participation, in some cases, has been limited in terms of duration (*e.g.*, the Port of Hong Kong participated in the program for approximately 16 months) or scope (*e.g.*, the Port of Busan, Korea, allowed scanning in one of its eight terminals). In addition, the Port of Singapore withdrew its agreement to participate in the SFI program and, as of April 2010, the Port of Oman had not begun scanning operations. Furthermore, since the inception of the SFI program in October 2007, no participating port has been able to achieve 100 percent scanning. While 54 to 86 percent of the U.S.-bound cargo containers were scanned at three comparatively low-volume ports that are responsible for less than 3 percent of container shipments to the United States, sustained scanning rates above 5 percent have not been achieved at two comparatively larger ports—the type of ports that ship most containers to the United States. Scanning operations at the SFI ports have encountered a number of challenges—including safety concerns, logistical problems with containers transferred from rail or other vessels, scanning equipment breakdowns, and poor-quality scan images. Both we and CBP had previously identified many of these challenges, and CBP officials are concerned that they and the participating ports cannot overcome them.²⁵ In October 2009, we recommended that DHS conduct a feasibility analysis of implementing the 100 percent scanning requirement in light of the challenges faced.²⁶ DHS concurred with our recommendation.

CBP and DOE spent approximately \$100 million through June 2009 on implementing and operating the SFI program, but CBP has not developed a comprehensive estimate for future U.S. program costs, or conducted a cost-benefit analysis that compares the costs and benefits of the 100 percent scanning requirement with other alternatives. The SAFE Port Act requires CBP to report on costs for implementing the SFI program at foreign ports, but CBP has not yet estimated total U.S. program costs because of both the lack of a decision by DHS on a clear path forward and the unique set of challenges that each foreign port presents. While uncertainties exist regarding a path forward for the program, a credible cost estimate consistent with cost estimating best practices could better aid DHS and CBP in determining the most effective way forward for SFI and communicating the magnitude of the costs to Congress for use in annual appropriations. To address this, in October 2009, we recommended that CBP develop comprehensive and credible estimates of total U.S. program costs.²⁷ DHS concurred with our recommendation.

CBP and DOE have paid the majority of SFI costs for operating the SFI program. The SAFE Port and 9/11 Commission Acts do not address the issue of who is expected to pay the cost of developing, maintaining, and using the infrastructure, equipment, and people needed for the 100 percent scanning requirement, but implementing the requirement would entail costs beyond U.S. Government program costs, including those incurred by foreign governments and private terminal operators, and could result in higher prices for American consumers. CBP has not estimated these additional economic costs, though they are relevant in assessing the balance between improving security and maintaining trade capacity and the flow of cargo. To address this, in October 2009, we recommended that DHS conduct a cost-benefit analysis to evaluate the costs and benefits of achieving 100 percent scanning as well as other alternatives for enhancing container security.²⁸ Such an analysis could provide important information to CBP and to Congress to determine the most effective way forward to enhance container security. DHS agreed in part with our recommendation that it develop a cost-benefit analysis of 100 percent scanning, acknowledging that the recommended analyses would better inform Congress, but stated the recommendations should be directed to the Congressional Budget Office. While the Congressional Budget Office does prepare cost estimates for pending leg-

²⁴ GAO, *Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers*, GAO-10-12 (Washington, D.C.: Oct. 30, 2009).

²⁵ GAO, *Supply Chain Security: Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers*, GAO-08-533T (Washington, D.C.: June 12, 2008).

²⁶ GAO-10-12.

²⁷ GAO-10-12.

²⁸ GAO-10-12.

isolation, we think the recommendation is appropriately directed to CBP. Given its daily interaction with foreign customs services and its direct knowledge of port operations, CBP is in a better position to conduct any cost-benefit analysis and bring results to Congress for consideration.

Senior DHS and CBP officials acknowledge that most, if not all foreign ports, will not be able to meet the July 2012 target date for scanning all U.S.-bound cargo. Recognizing the challenges to meeting the legislative requirement, DHS expects to grant a blanket extension to all foreign ports pursuant to the statute, thus extending the target date for compliance with this requirement by 2 years, to July 2014. In addition, the Secretary of Homeland Security approved the “strategic trade corridor strategy,” an initiative to scan 100 percent of U.S.-bound containers at selected foreign ports where CBP believes it will mitigate the greatest risk of WMD entering the United States. According to CBP, the data gathered from SFI operations will help to inform future deployments to strategic locations. CBP plans to evaluate the usefulness of these deployments and consider whether the continuation of scanning operations adds value in each of these locations, and potential additional locations that would strategically enhance CBP efforts. While the strategic trade corridor strategy may improve container security, it does not achieve the legislative requirement to scan 100 percent of U.S.-bound containers. According to CBP, it does not have a plan for full-scale implementation of the statutory requirement by July 2012 because challenges encountered thus far in implementing the SFI program indicate that implementation of 100 percent scanning worldwide by the 2012 deadline will be difficult to achieve. However, CBP has not performed a feasibility analysis of expanding 100 percent scanning, as required by the SAFE Port Act. To address this, in October 2009, we recommended that CBP conduct a feasibility analysis of implementing 100 percent scanning and provide the results, as well as alternatives to Congress, in order to determine the best path forward to strengthen container security.²⁹ DHS concurred with our recommendation.

In DHS’s Congressional Budget Justification FY 2011, CBP requested to decrease the SFI program’s \$19.9 million budget by \$16.6 million. According to the budget justification, in Fiscal Year 2011, SFI operations will be discontinued at three SFI ports—Puerto Cortes, Honduras; Southampton, United Kingdom; Busan, South Korea—and the SFI program will be established at the Port of Karachi, Pakistan. Furthermore, CBP’s budget justification did not request any funds to implement the strategic trade corridor strategy.

Mr. Chairman, this completes my prepared statement. I would be happy to respond to any questions you or other Members of the Committee may have at this time.

Related GAO Products

Combating Nuclear Smuggling: DHS Has Made Some Progress but Not Yet Completed a Strategic Plan for Its Global Nuclear Detection Efforts or Closed Identified Gaps. GAO-10-883T. Washington, D.C.: June 30, 2010.

Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain. GAO-10-400. Washington, D.C.: April 9, 2010.

Coast Guard: Deployable Operations Group Achieving Organizational Benefits, but Challenges Remain. GAO-10-433R. Washington, D.C.: April 7, 2010.

Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience. GAO-10-296. Washington, D.C.: March 5, 2010.

Coast Guard: Observations on the Requested Fiscal Year 2011 Budget, Past Performance, and Current Challenges. GAO-10-411T. Washington, D.C.: February 25, 2010.

Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers. GAO-10-12. Washington, D.C.: October 30, 2009.

Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation. GAO-09-492. Washington, D.C.: March 27, 2009.

Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed. GAO-09-337. Washington, D.C.: March 17, 2009.

Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security. GAO-08-904T. Washington, D.C.: June 25, 2008.

Supply Chain Security: Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers. GAO-08-533T. Washington, D.C., June 12, 2008.

²⁹ GAO-10-12.

Highlights of a Forum: Strengthening the Use of Risk Management Principles in Homeland Security. GAO-08-627SP. Washington, D.C.: April 15, 2008.

Maritime Security: Federal Efforts Needed to Address Challenges in Preventing and Responding to Terrorist Attacks on Energy Commodity Tankers. GAO-08-141. Washington, D.C.: December 10, 2007.

Maritime Security: The SAFE Port Act: Status and Implementation One Year Later. GAO-08-126T.T Washington, D.C.: October 30, 2007.

Maritime Security: The SAFE Port Act and Efforts to Secure Our Nation's Ports. GAO-08-86T. Washington, D.C.: October 4, 2007.

Information on Port Security in the Caribbean Basin. GAO-07-804R. Washington, D.C.: June 29, 2007.

Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure. GAO-06-91. Washington, D.C.: December 15, 2005.

The CHAIRMAN. Thank you, Mr. Caldwell.

I'll start the questioning with, actually, one of the last questions I was going to ask. Admiral, I'm going to ask this to you.

It's interesting, in aviation—and Kay Bailey Hutchison and I have been working on an aviation bill for a long time, and we hope to get it done—and one of the interesting things there are, there are so many more general aviation—I'm making a small-boat comparison, okay?—general aviation planes that are in the air at any given moment than there are commercial flights, but they only pay a very small percentage of keeping up the air traffic control system. In fact, it used to be as little as 8 percent. I think it's now something like 14 percent.

What is my point? I'm talking, basically, about larger jets. But, you have a real problem in small vessels. There are more than 17 million small watercraft operating in U.S. waters, and that is one extraordinary security threat. It wasn't that long ago that a one-engine airplane flew into a building in New York, and it didn't get a whole lot of attention. New York City. And it was just a pilot who fell asleep, or something. But, I happen to care about that one, because it happened, and second, my son was living in that building. And he is okay, and the building's okay, because it was a small, one-engine plane. But, it says what the possibility of small numbers of ships or craft on the water can mean.

So, my question to you is, To what extent is this a problem, from a monitoring point of view, from a national security point of view? I mean, it's my understanding that you can have a small aircraft or a small boat carry a very heavily loaded series of briefcases into port, and nobody's going to notice. So, how do you monitor? How do you do that? Or is it, in fact, financially entirely out of your scope?

Admiral PAPP. Mr. Chairman, it's certainly a problem that has concerned me—

The CHAIRMAN. I don't mean your scope, but your ability to do something about it, because of resources.

Admiral PAPP. Well, I think there's something we can do about it. And what I would do is go back through my own experience. Shortly after 9/11, I was the 9th District Commander, up in the Great Lakes. And I have to think that, when I looked out my window across Lake Erie and saw all those small boats out there, that half of those 17 million might be just on Lake Erie. The fact of the matter was, there are about 7 million boats up in the Great Lakes,

and then you throw in another, maybe, 3 million from the Canadian side and international waters, it's quite a challenge.

And I think, as I went up there and started confronting the problem after 9/11, I looked at those small boats as the enemy. In other words, every one of them's a threat. The truth of the matter is, the vast majority of them are our friends, and can be used as sensors, and can enable us to provide us better maritime domain awareness.

So, a great example of making effective use of this, at very small cost, is the America's Waterways Watch Program, where we go out, we engage the boating community. We make them part of the system, instead of having them the enemy, and they will help us, they will inform us and become a part of our system of maritime domain awareness.

So, I think continuing those sorts of efforts—outreach, making sure that the boating community doesn't get—share the same complacency that I was talking about, informing them that there is the potential for threats out there and we need them to help us in doing our job, I think goes a long ways toward doing that.

I visited, up the Gulf of Maine, with Senator Snowe, back a few months ago, and just from my own personal experience sailing in the waters off New England, most of those lobstermen up there, or the fishermen on Georges Banks, they know who are supposed to be out there, they know each other, they sometimes even fight each other out—trying to protect their own special areas. They know strangers when they come in there, they know behavior that is not normal, and if they have an avenue to be able to report this to the Coast Guard, it helps us in our situational awareness. We can share that, and investigate it.

So, I think there are ways of using that large group of small vessels, that were, in the past, perceived as a threat, to help enable us to take care of what might be a threat out there.

The CHAIRMAN. Two very quick questions. When you say you're making outreach to those people so that we look upon them as the enemy, but you're looking to make outreach and to get them to be alert and not be complacent, and the rest of it, which, by definition, means that you are talking to, or being responded to, by those who want to cooperate with you. That doesn't talk about those who actually might have, or circumstantially might have, explosive devices put upon their small craft, and not even know it. So, I'm comforted by the lobstermen knowing, you know, who the friendlies and the unfriendlies are, the strangers are, but, outside of the fishing community—17 million—that's a very large number.

Admiral PAPP. Sure.

The CHAIRMAN. And my understanding is that you and Homeland Security—that the Coast Guard and Homeland Security are preparing a new strategy as to how to approach small vessels, in terms of security. And I'm interested to know, how is that coming along? Are we going to be able to get that, and see it?

Admiral PAPP. Yes, Mr. Chairman. That's in the final stages of review by the Secretary right now. And I don't know what their timeline is, in terms of approval by the Secretary, but, across components, we've been working on that. It has to be a layered response. There is outreach to the boating community. And in that

regard, the adaptability, the multimission structure of the Coast Guard, our continuing involvement in boating safety over the years, our Coast Guard auxiliaries that number over 30,000 people across the country, help enable us to reach out to those people, to inform them of the program, and to get them to help us out.

But, it really boils down to the—its other aspects, as well. Good intelligence is clearly essential to the small-boat problem. And the Coast Guard, as a member of the intelligence community, is constantly looking out for trends, for activities, for other things that might indicate a challenge or a potential threat within the country. When we know that, or when we have events, that's when we don't rely just upon other people in the area; we have Captain of the Port authorities that can set up security zones. We can do escorts. We can put resources out there, and not just Coast Guard resources, but CBP resources or local, State, and—or other Federal agencies, to help us, in the event of a—

The CHAIRMAN. Admiral, I thank you. I just, in turning to Senator Hutchison, would need to comment that it seems to me you're talking about the reach out being kind of like driver education, "You've got to be safe, you've got to do this, you've got to do that." People who don't want to be safe, who want to do this, can be incredibly safe, but very destructive. And that's kind of the problem that I'm getting at. How do you reach those people? And, I guess, in this document, I'm going to learn something about that.

In any event, thank you.

And I turn now to Senator Hutchison.

Senator HUTCHISON. Well, thank you very much.

I would just like to ask the three of you—in the issue of port security, obviously we have foreign ships coming in, containers coming in, and we've increased our capabilities with containers, and put seals on them after they've been inspected in a foreign port. But, my question is, What have you found that we can do that would be more and better coordinated with all of the different entities that can contribute to security to make our ports as secure as possible, with all of the foreign tonnage coming in?

I'll just start with you and just go down the way.

Admiral PAPP. Senator, I think, first and foremost, it's pushing it as far offshore as possible. And, in that regard, our International Port Security Program—I've been really pleased, over the last couple of years, in the advances that we've made. As the Atlantic Area Commander for the Coast Guard, all the international port—or, all the international port security liaison officers were working under the Atlantic Area staff. We programmed them, we scheduled them. We've made visits to 150 of 154 countries to validate their security regimes within their ports. That's really the first step, is making sure that they are complying with the same security standards that are required throughout the world, and trying to normalize that so that we can trust the ports in which the cargo is loaded.

With that, the experts on cargo security—or "the" expert—is sitting right next to me.

But, the Coast Guard will assure the standards of security within the port. The handling of cargo is taken care of by my partner's organization.

Mr. BERSIN. Precisely so. In addition to the security dimensions of the port, Senator, we see it as an issue of risk management. And the segmentation of traffic between those cargoes and containers about which we know something adverse, and distinguish those from which we know may present a lower risk. Unless we can actually separate out those containers as far away in time and space from the American homeland, we have a difficult time to move lawful traffic in the way in which we need for an economically competitive America.

Senator HUTCHISON. Are you talking about specific types of cargo, or the ports from which they came being a different risk assessment, or the companies that are transporting being a different risk assessment? Is that a—

Mr. BERSIN. All of—

Senator HUTCHISON.—part of your—

Mr. BERSIN.—the above. I mean, in terms of being able to distinguish containers that we need to look at more carefully from those in which we can expedite—in effect, looking for that needle in a haystack, both by having intelligence about the ones we need—where we might pluck out the needle that would cause us harm, but also reducing the size of the haystack. So, this is about increasing the information about the container, the importer, the shipper, the freight consolidator, every part of the supply chain, so that we can actually do this segmentation of traffic—

Senator HUTCHISON. And do you think we effectively do that?

Mr. BERSIN. We are in a position, compared to 2006, with much more information, a more effective way of managing that information. I believe a more—

Senator HUTCHISON. With the capability to do the transfers away from the ports?

Mr. BERSIN. In terms of, for example, having more information before a container arrives at the American port, yes. The “10 plus 2,” the importer filing—safety filing, security filing—has permitted us to gather much more information than we did before that, so that we can do the risk management and the assessment while the containerized cargo is coming toward the American port.

So, the answer to that is yes. And we also have more sophisticated targeting rules, which incorporate threat streams so that we can actually both separate out that cargo that presents low risk from that cargo that is either high risk or about which we know very little.

Senator HUTCHISON. Thank you.

From the GAO?

Mr. CALDWELL. Thank you, Senator Hutchison.

While GAO is probably not in the position to be able to come up with the path forward and “Where do we go from here?” Our work has found that there is a fairly robust and layered regime of programs for port security out there. And the details of these programs are already in the statements of the two gentlemen here.

I think where we come in, our contribution, is to look at the execution and the implementation of those programs, and a lot of times we have found weaknesses in those areas. But, I have to say that both Coast Guard and CBP have generally been very responsive to our recommendations. It’s not always an easy fix, the things

that we're asking them to improve, but they have generally been responsive to the recommendations that we've made.

So, while I agree with the Commandant that complacency is one of the issues, I think these programs need to continue to mature—the programs in place while the programs that we're discussing—or even “10 plus 2” is relative new, in terms of that program being fully implemented. One of the bigger issues we see right now is, obviously, the 100-percent scanning requirement. We're at a little bit of an impasse here between what the statute actually says and, I think, what can actually be accomplished by the Department. Our Department's pretty much made that clear, and I think that foreign governments and companies have as well. It's something that would be very difficult to implement because the technology is just not there right now.

Another question has arisen from that is, How does that fit into the layered strategy? Aspects of that requirement may detract from some of the existing programs out there. Countries may be less willing to participate in CSI if everything's going to be scanned, anyway. Companies may be less willing to participate in C-TPAT, and foreign governments that have AEO programs, may be less willing to have them if their containers are going to get scanned anyway.

It is a question of trying to balance across these different programs. And, hopefully, these programs will continue to mature and improve.

Senator HUTCHISON. Mr. Chairman, thank you. And my time is up, but I do have another couple of questions for a second—

The CHAIRMAN. Well, go ahead.

Senator HUTCHISON.—round.

The CHAIRMAN. Look, we can—

Senator HUTCHISON. No—

The CHAIRMAN.—be a little informal here—

Senator HUTCHISON. No, no, there are other members here. I'd—

The CHAIRMAN.—right? You want more time?

Senator HUTCHISON.—prefer—

The CHAIRMAN. Seven minutes?

Senator HUTCHISON. No. I'd prefer—

The CHAIRMAN. No?

Senator HUTCHISON.—to let—

The CHAIRMAN. OK.

Senator HUTCHISON.—them go, but I would like a second round.

Senator LAUTENBERG. We have great respect and admiration for Senator Hutchison, and part of the admiration is her grace and her willingness—

The CHAIRMAN. To yield to the Senator—

Senator HUTCHISON. To let Mr. Lautenberg—

The CHAIRMAN.—from New Jersey.

Senator HUTCHISON.—speak.

[Laughter.]

The CHAIRMAN. Senator Lautenberg.

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

And when we look at the witness table here, and we see the responsibilities that are covered by these three people, they're enor-

mous. And Admiral Papp just mentioned in his remarks—that I'm a strong supporter, as I know both of you are—each of you is, as well—with the Coast Guard. And when we look at the assignments they have, it needs a constant reminder about the fact that they cover so many bases, and that they continue to respond positively, bravely, and courageously to new assignments without always getting—without almost ever getting the resources that accompany the additional responsibilities.

And right now, with the attention that's given to the Coast Guard—and I congratulate you, Admiral Papp, for your ascending to the leadership of the Coast Guard; you've earned it. It's a wonderful organization and they're lucky to have you as their leader. We all feel that way. But, I want to just take a moment to say that, in the bill that I now have in my chairmanship on the Appropriations Committee—and that is the DHS bill—we increased the Coast Guard budget by \$221 million from last year. We were happy to do it, and know how vital it was that you get the additional support that you need as your responsibilities in your organization contains.

Mr. Bersin, also, you know, people often forget how broad the responsibility of your organization is. And when we look at Customs, we think about people that we see more often at the airport and the most visible places. But, you've got an array of things, going from agriculture interests and have a—intellectual property theft, preventing and disrupting terrorist attacks, a lot going on there.

One of the things that you mentioned, and has been on our mind and our screen, was that—you mentioned this—the screening that's supposed to have taken place. Three years ago, Congress acted to require 100-percent scanning of all containers coming to the country. However, last year the GAO found out that we were only scanning less than 5 percent of all U.S.-bound containers, and that 100-percent screening has not been achieved at even a single port.

Now, what has the Department done to improve this leap ahead from the 5-percent scanning rate? Where is it?

Mr. BERSIN. Senator, first, to distinguish between the scanning for the RPMs, the radiological scanning is taking place with regard to maritime cargo. With regard to the gamma-ray or X-ray scanning, you're correct that we have not instituted a 100-percent scanning. As I indicated in my statement, and as the Secretary has indicated to the Congress, while we have completed the pilot project at the five ports designated in the SAFE Port Act of several years ago, the lessons we've learned there suggest that we need to continue to do work with regard to developing a security regime that takes into account the problems that I indicated in the statement.

Senator LAUTENBERG. How many ports—or, how many containers—percentage of containers do we cover, in terms of your responsibility?

Mr. BERSIN. The—there are approximately, last year, just under 10 million containers, and we are—

Senator LAUTENBERG. That's out of how many?

Mr. BERSIN. Ten million containers that are coming to the United States, and we are scanning 4 to 5 percent of those, sir.

Senator LAUTENBERG. Four to 5 percent, OK. I got the number—I jumped ahead of you on the numbers.

Mr. BERSIN. And—

Senator LAUTENBERG. So, we're still far behind the objectives that we set for ourself at this point in time.

Mr. BERSIN. Measured by the 100-percent standard, yes, sir.

Senator LAUTENBERG. Yes. We have a deadline, 2012, for 100-percent scanning of all incoming shipping containers. But, we're a long way from that point. And when I look ahead to a year and a half, or two, at the most—do you think we can possibly meet that standard?

Mr. BERSIN. As you know, and as the Secretary has advised Congress, Senator Lautenberg, the Department is working on a proposal that, first, would actually provide the documentation, as the GAO has requested, that would indicate what it would take to do the scanning, in terms of cost and logistical outlay.

Senator LAUTENBERG. What's your estimate Mr. Bersin? What do you think? When do you think, if we can possibly, at all, reach that goal that we set for 2012?

Mr. BERSIN. Frankly, Senator, I think that we're going to need to develop an alternative approach that provides us with the security that is sought by the 100-percent scanning, but to do so in a way that incorporates risk management and recognizes the difficulties—

Senator LAUTENBERG. Right.

Mr. BERSIN.—of trying to do it all—

Senator LAUTENBERG. But—

Mr. BERSIN.—at once.

Senator LAUTENBERG.—we're a long way away, and—I don't want to cut you off, but—I come from a position that says, okay, here's A, there's B; What's the difference between A and B? And the difference here is that we're significantly behind the goal that we'd like to have. And I think it's important that we recognize this, Mr. Chairman, in this committee.

Admiral Papp, the SAFE Port Act required that the Coast Guard establish an Interagency Operation Command Center at all the high-priority ports, and that was to be done by last October. Unfortunately, the Coast Guard has not yet begun to construct a center for the Port of New York/New Jersey, the largest port on the East Coast. Why hasn't an IOCC been established for the New York/New Jersey region? And when might the Coast Guard move forward on this project?

Admiral PAPP. Well, you're absolutely right, Senator, there is nothing that is called the IOC, or Interagency Operations Center, in the Port of New York, but we have been working, across the country, in 35 critical ports to develop IOCs. There are probably three components of that. First of all, is getting the software to be able to consolidate the sensors, and then to set up the structure within which to work, which we think we can do, based upon the work we do in our Area Maritime Security Committees. And then, third, and probably the thing that has probably confounded us the most is having a facility where you gather.

But, we've been focused on things like the buildings we've put up in Seattle or the buildings that we've—that we're now building in New Orleans, and focusing on them as Interagency Operations

Centers. It's tough to come up with the resources to be able to construct buildings.

So, what we've been working on is virtual—virtually bringing people together. We have implemented a piece of software called Watchkeeper, which brings various sensors and other databases together, which we can share with the interagency in each one of those ports. We've fielded that in Charleston, and we expect to have all 35 of the ports, basically our sector command centers, using Watchkeeper within the next year.

The next step is to share that with the other interagency partners across the port. And then, the third step would be to provide the facilities, either virtual or physical facilities, to bring all the interagency together within those command centers.

I will tell you, though, in our Area Maritime Security Committees, in terms of developing plans, the Coast Guard has constantly been involved in outreach across the interagency. In the Port of New York, at Sector New York, they have room within their command center, where, in times of operations, we bring in Commissioner Kelly's people or Ports Authority people or the interagency, and we work together.

So, while we may not be able to reach out and identify a building as an Interagency Operations Center, we've certainly been working within the spirit to bring the interagency together so that we can have greater synergies in providing security in the ports.

Senator LAUTENBERG. Mr. Chairman, I wind up with an observation, if I might, to you, sir, and that is that we have these responsibilities, and there are serious people here, with strong staff and strong commitment, but yet have not come close to the goals that we've set out. And some of this is a division of resources. And we have to recognize that defending ourselves at home from terrorism is not really less important than defending ourselves in far distant places for our security, that security at home, here, whether it's in the ports or in the airports, that we have to have resources to do it with. And we spend \$650 billion each and every year on defense, and it's appropriate that we have to have something at least comparable to honestly present our people with the resources they need.

I thank you very much.

The CHAIRMAN. Thank you, Senator Lautenberg.

And now Senator Klobuchar.

**STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA**

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

Thank you, to all of you.

Admiral Papp, the SAFE Port Act strengthened the Maritime Transportation Security Act by adding a requirement that the Coast Guard conduct two inspections annually and one being unannounced. Have those unannounced inspections helped? Have they been effective in improving compliance?

Admiral PAPP. Yes, ma'am, I believe they have. And I'm—in the interest of transparency, I'm trying to search my mind for our success rate in terms of those. We've devoted an awful lot of resources and inspectors toward completing those inspections and unan-

nounced visits, and conducting exercises. And as we have reviewed all the plans—and we go through 3,200 security plans across the country—and I'm sure you're talking about the domestic security plans—

Senator KLOBUCHAR. Yes.

Admiral PAPP.—that's a large task to take on, but we're very proud of the fact that we have completed those, and we have updated them, in accordance with the Act. And I think that it is a success story for us.

Senator KLOBUCHAR. Very good. And maybe you can follow up when you can get some of the data and things in writing, but I appreciate that.

Commissioner Bersin, as part of CBP's layering targeting strategy, you discussed the role of a National Targeting Center in sharing local officers, the information and intelligence that you gather on incoming cargo. And I'm a former prosecutor, so I'm always concerned that local law enforcement be properly looped in on issues. And I know this has sometimes been an issue in the past. Could you talk about your efforts in that regard?

Mr. BERSIN. As a former prosecutor myself, I appreciate the value added by State and local authorities. And I know, with regard to CBP, there are numerous instances in which CBP field officers in our seaports and airports, and our Border Patrol Agents on the northern and southern borders, are in constant communication with the State, local, and tribal law enforcement authorities.

With regard to the cargo, containerized cargo security, that information ordinarily would not be directed to local law enforcement. That is to say, we don't have, usually, the local or county interest in inspecting containerized cargo that would come to the ports. But, there are numerous instances in which incidents take place at our ports, in which CBP relies upon the partnerships that exist, whether they're the JTTF, the Joint Terrorism Task Forces, or more conventional law enforcement alliances.

Senator KLOBUCHAR. Speaking of cargo, you also mentioned in your testimony about the work you've done with the Consumer Product Safety Commission and the FDA and the Food Safety Inspection Service to prevent unsafe products from entering our country. I've been active on a lot of those product issues, as have other people on this committee. Could you talk about how you're working with other agencies at the border to weed out dangerous products?

Mr. BERSIN. Yes. Earlier this spring, Senator, CBP, Customs and Border Protection, entered into a memorandum agreement, a working agreement, with the Consumer Product Safety Commission, in which we opened up, formally, the Commercial Targeting and Analysis Center, which is a trade version of our national security targeting system. The database of the—uses the same database information as our national security targeting, but it's focused on issues such as import safety, food and drug safety, intellectual property rights protection, and other trade enforcement issues. FDA is a member of that group, and we expect to hold a conference, in the fall, in which we will be inviting our major other government agency partners to participate as full members of the CTAC and also of the—to build on the so-called International Trade Data System

group, which are the government agencies involved at the ports of entry.

Senator KLOBUCHAR. Thank you. I think that's going to be very important as we see some of these products coming in.

I'm also interested—my last question—in your discussion of the Customs-Trade Partnership Against Terrorism, the public-private partnership program that allows participating trade groups to receive expedited service at ports, in exchange for maintaining a higher level of personal security. So, you're working in partnership, acknowledging that some businesses and trade groups are going to do a better job of having higher security. And you mentioned that CBP is working with foreign partners to establish binational recognition and enforcement. Could you elaborate on that?

Mr. BERSIN. We cannot do our job, Senator, without segmenting the traffic between, as I indicated in my statement, traffic we know something about from traffic we know nothing about or about which we have derogatory information. The C-TPAT Program, the Trusted Shipper Program, the Trusted Broker Program, the Trusted Freight Consolidator Program, is essential—an essential public-public partnership that actually offers some assurance of supply chain security so that we can offer benefits of expediting trade to the members of that partnership.

In the same way as you suggest, our partnerships with foreign governments in which they have the so-called AEO or trust—AEO programs, or trusted programs—when we can do a mutual recognition with those countries, we actually multiply our presence. So far, we have five agreements of mutual recognition, with Japan, Korea, Canada, Jordan, and—I always forget the fifth one—

Senator KLOBUCHAR. You can supplement the record.

Mr. BERSIN.—and I always forget the—

Senator KLOBUCHAR. Oh, they're so quietly advising you back there, I didn't notice.

Mr. BERSIN. And I always forget New Zealand, the first one, as I'm reminded, and the one on which we rely for so much of our commodity import. But, of those five countries, we actually have a mutual-recognition regime.

Just recently at the World Customs Organization, we negotiated, with the European Union, a process by which we trust, over the course of a year, we will have mutual recognition between the United States and the 27 nations of the European Union.

Senator KLOBUCHAR. Very good. And I can put my question in writing for you, Director Caldwell, about some of the issues with some of the foreign ports and the recent Coast Guard estimate about 15 countries not maintaining their effective antiterrorism measures. But, I think I'm out of time, and I'll just put that in writing. All right? Thank you.

Thank you, to all of you.

The CHAIRMAN. Senator Cantwell.

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

Senator CANTWELL. Thank you, Mr. Chairman, and thanks for holding this important hearing.

Admiral Papp, good to see you. I'm looking at the FY-2011 budget for the Coast Guard, and I see that there's a 3.3 proposed decrease, about \$75 million. And do you have any idea what that means, as far as how you're going to realize those budget cuts? And I know, also, that there's a GAO report that the FY-2011 budget cites decreases in port funding in waterways and coastal security, and has a cut of about 6 percent. So, I'm just trying to understand how we're going to make these cuts and how we're going to keep our ports safe in the process.

Admiral PAPP. Yes, ma'am. Obviously, some very difficult decisions were made when putting together the 2011 budget. There were tradeoffs made to continue the recapitalization of our infrastructure, the—those versatile and adaptable aircraft, boats, and ships that I talked about earlier, and to sustain some short-term reductions in other activities in order to pay for that.

Where it manifests itself, probably most visibly for this particular hearing, are the five Maritime Safety and Security Teams that were reduced in that budget. I've done a lot of talking about the versatile and adaptable resources that we have. For instance, one of the MSSTs that was to be reduced is in the Port of New York. We have increased Station New York and Sector New York general-purpose forces, almost double over the last 8 years or so. For—as an example, Station New York used to have 45 people, they have 90 people there right now that can do daily missions within the Port of New York; whereas, the MSST, as a single-focus security force—I love having them, but their utility, in terms of providing day-to-day security was not as much as the stations that were there. So, when confronted with the choices of, "How do we balance our forces to provide the services to our country?" we stuck with the versatile, adaptable general forces, to sustain them as much as we could, while recapitalizing some of those ships, boats, and planes that we so desperately need, as well.

Senator CANTWELL. I'm not sure I followed all of that, but I also want to ask you, because in this line of making ends meet, obviously ports are a key part of our security regime. I had asked Secretary Napolitano about the semisubmersible vessels and what we were doing to repair—and I know that there has been, recently—a submersible vessel that was recently discovered in Ecuador, so this whole issue of their involvement in drug trafficking—so, what are the plans to fully combat these submersibles?

Admiral PAPP. Well, ma'am, the first thing is good intelligence. We need to cooperate with the countries of South and Central America, particularly our friends in Colombia, who have really done a complete turnaround down there and have assisted us and really been strong partners in this drug war.

We work the intelligence side very hard, through many methods, so that we can detect these semisubmersibles as they're leaving. If we don't know when they're leaving, then it makes the equation even much more difficult, because of their profile. With the vast expanses in both the eastern Pacific and in the Caribbean, they're very difficult to detect. We have marine aviation patrols out there. We work with the Navy, and we work with other Central and South American countries, as well, to try and detect them. And then, of course, we have our own patrol vessels down there.

Senator CANTWELL. And what about small-vessel threats that—I know there was a pilot program that both Seattle and San Diego participated in, as it related to nuclear detection for small vessels—is that—I think the Coast Guard was involved in that—and do you think that we need to expand that program? Are we going to expand that program—

Admiral PAPP. The—

Senator CANTWELL.—into—you know, into major port areas?

Admiral PAPP. We—as mentioned earlier, the small-vessel threat is one that deeply concerns me, just based upon the magnitude, the sheer numbers, of recreational boaters and fishing boats that are out there. As I talked about before, we perceived all of them as a threat, at one time, and what we've done now is actually saw them as a—see them as a force multiplier. So, outreach through education, some of the programs that we've had out in the 13th Coast Guard District, and our America Waterways Watch Program, have been very beneficial to us, in terms of bringing that recreational and fishing-boat public in to act as additional sensors for us on the water to provide us maritime domain awareness.

Senator CANTWELL. So, do you think the program's going to expand?

Admiral PAPP. Well, it's certainly one that I want to sustain. Right now, it's a very low-cost project for us, the America's Waterways Watch Program. It's slightly in excess of a million dollars, which is basically to provide and conduct outreach, both through Active Duty Coast Guard people and our Coast Guard Auxiliary. That's certainly a program that we could expand upon. And then, we're also—we have our small vessel security—

Senator CANTWELL. That's more what—

Admiral PAPP.—strategy that is on its way, that's—

Senator CANTWELL. That—

Admiral PAPP.—currently under review by the Secretary.

Senator CANTWELL. OK, that's more what I was referring to, so I'll—

Admiral PAPP. Yes, ma'am.

Senator CANTWELL.—look forward to seeing that plan and what you're going to do about small vessel detection.

Admiral PAPP. Yes, ma'am.

Senator CANTWELL. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Cantwell.

Senator LeMieux.

**STATEMENT OF HON. GEORGE S. LEMIEUX,
U.S. SENATOR FROM FLORIDA**

Senator LEMIEUX. Thank you, Mr. Chairman.

Thanks all of you, for your service.

Commandant, it's great to have you here, and congratulations on your new position. I had a chance to visit before you officially came on, and very pleased that you're leading the Coast Guard. And we had a great discussion about what the Coast Guard means to Florida. So, I am proud of you, proud of the work that all the Coast Guard folks have done in the Gulf. This has been an extremely difficult and trying time, and I know your folks are working very long

hours. And I just wanted to let you know, and please pass along, how much we appreciate the good work they've done.

Admiral PAPP. Oh, thank you, sir, they'll appreciate that.

Senator LEMIEUX. I want to talk about port security, and I want to talk about two areas. I want to follow on what Senator Lautenberg said about this container issue. Five percent's not acceptable. And if the law says 100 percent, then we have to get toward 100 percent. And although that may be a very difficult task, frankly and respectfully, it's your job to get there. If you can't get there and that is an unreasonable requirement, then we need to change the law. But, if the law is that you're at 100 percent, we need to try to get to 100 percent, and 5 percent is very far from 100 percent.

We've got, as you know, 14 deepwater ports in Florida. The ports are our lifeblood. They are where the cruise ships come in, and they are where we do our trade. So, I have been concerned for a long time, even prior to my time here in the Senate, when I worked in the attorney general's office in Florida, about port security. I'm concerned about it because of what may come in on a ship, but I'm also concerned about it because, like many cities, our port—most of our ports are embedded in our downtown areas, and they are—you know, as a place of entry, they are so close to our civilian populations and our city centers. So, I worry, as I know you do, about worst-case scenarios and what could come in on a ship. And I'm very pleased to see that you're doing, what, nearly 100 percent on the screening for radioactive materials, and I commend you for that. But, the screening that has to happen on the rest of these containers—there are a lot of things that could come in on them, and it's not just the dangers everyone thinks about it. In Florida, it can be exotic plants and animals that come in and get in our waterways and cause tremendous environmental damage. So, there are a lot of things that can come in on a container, and a lot of containers come through Florida, as you know, not just for Florida's use, but for the entire eastern part of our country.

But, specifically on ports, I wanted to ask you if—what focus you're having on trying to secure the ports, not on the container side, but just on the physical property of the ports. And I'll tell you what worries me. I'm from Fort Lauderdale, and we have Port Everglades there. And Port Everglades is our fuel port. They do cruise ships and other things, too. But, we have these huge fuel containers, that store gasoline and oil, that are basically right in our downtown. And you can see them, and you can drive by them on Federal Highway. And I've always been worried about what someone with bad intentions could do to something like that. And there are other places in Florida, as well—in Tampa, in other places, where the port is right near the city center.

So, if you could address that for me a little, sir, and then we can talk a little bit more about containers.

Mr. BERSIN. Let me start with the containers, because—

Senator LEMIEUX. Whatever your preference.

Mr. BERSIN.—if I might. The—because I don't like being in the position, because I do appreciate, and I know the Secretary appreciates, the threat, and also the fact that 100-percent scanning is the law, and that, in fact, being at 5 percent, there is a huge gap there, and it has been, actually, an issue that has been delayed and

deferred each year, as the legislation permits. So, I think, in fact, we need to come to grips with that, and I suggest to you, Senator, and commit to you, that that process is underway, which is to take the very significant challenges that we face, in terms of cost and logistics of a 100-percent scanning regime.

And it's our obligation, I think, to do two things. One is to provide a complete statement of what it would take, in cost, to meet the law, and in terms of the arrangements, and whether or not we could do that, all things being equal, which oftentimes they're not. And if we cannot do that, then we come up with a regime, in consultation and concert with Congress, that gets us a level of security that is satisfactory to the American people.

So, I understand the Senator's concern. I share it. And I know that the Secretary is committed to the Congress to work through a series of proposals if, in fact, the 100-percent cannot be met.

Senator LEMIEUX. OK.

Mr. BERSIN. With regard to port security, let me lay the scenario up, because this is something that would be in a partnership with the Coast Guard—in some cases, the Navy—and mostly, actually, with the Port Authorities that control the ports, such as the one, Fort Lauderdale, that you refer to. These are county or State authorities that actually have the bonding authority and do the construction. Usually, with regard to CBP, CBP would be consulted as to the specifications for the necessary customs inspection facilities, but the port security layout is ordinarily an issue, frankly, that we would not have control over. We would be consulted, as I believe the Coast Guard would, but ultimately it's a local decision as to how, in fact, to construct the facility.

I will say, in the wake of 2001, and certainly even the Port—the SAFE Port Act, there are much more—there's much more consultation. Before coming into this job, I was the Chairman of a Regional Airport Authority, which is comparable to the authority you suggest that runs the ports at Fort Lauderdale and elsewhere in Florida. And we certainly consulted with our Federal partners. But, at the end of the day, it was a decision of the Airport Authority as to what steps would we take and where the construction would take place. So, I'm not avoiding the responsibility; it's just not within our authority, although we are always willing to consult, as I know the Coast Guard is.

Senator LEMIEUX. I mean, I know there's a shared governance issue. But, as you know, these ports were built a long time ago, most of them, and they were built in a pre-9/11 environment. And I've been appreciative of the heightened security requirements. When you go into these ports now, there's usually a checkpoint and there are other things that you have to do so that there's some monitoring of people who are going in and out. But, I worry about their proximity to city centers. I worry most about the ones that have fuel. And I don't know what the answer is, but I wanted to raise the topic, because I wanted you all to be focused on it.

Mr. BERSIN. I appreciate that, sir.

Senator LEMIEUX. Admiral, you want to speak to that point?

Admiral PAPP. Oh, yes, Senator, surely.

This is where the versatility and the authorities the Coast Guard has really comes into play, in earnest. We have Area Maritime Se-

curity Committees, which brings together the Federal, State, and municipal authorities, the interagency, all under the authority of the Captain of the Port. And our Captain of the Ports are now the area maritime security coordinators under MTSA. Every one of those facilities has to have a facility security plan reviewed, approved, drilled, and exercised, and inspected by the Coast Guard. So, none of these things are done in isolation or unilaterally, they're all done under cooperation and with a multilayered review when they are put in.

And I know, down in Fort Lauderdale, we have extensive Coast Guard oversight down there, we work in partnership with the local communities, and are continually reviewing it.

Senator LEMIEUX. Appreciate that.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator LeMieux.

I guess I'm a little bit frustrated, because there's a lot of, kind of, intelligence-speak, security-speak, government-speak going on here. And the basic—the base—I sort of come back to the boats, the little boats. And Senator LeMieux was referring to that, and others were.

The 100-percent—you've got to get to 100 percent. That's very much in the minds of people, very much in the minds of Congress. If that's not doable, we need to know about that, and we need to change the law, as just has been suggested. But, to hold out a promise—see, in the world of coal mining, where you have disasters on a fairly regular basis, we have—and that's very complex in—it's a sort of hidden secret world, et cetera, deep in—you know, a mile underground, all this kind of thing—we have a mantra, that all accidents are preventable. A little bit, I get the feeling that “We're doing the best we can” from you. That totally makes sense, just as you could say “All accidents are preventable” can't be true, since accidents can occur in various ways and—but, you know, I think that the mantra of “All accidents are preventable” is the one that we have to have, because that's what drives us toward speaking rationally and realistically to each other.

I mean, the *Washington Post* is carrying, I think, a fascinating article—and I'm, you know, on the Intelligence Committee—about the world of intelligence, how it has gone up by enormous numbers, and enormous numbers of dollars, and it's sort of horrifying as you look at all the charts and the way everything is spread, and DHS has, you know, tons and tons of things, and—Is DHS really working properly? And can it work? Was it put together properly?

I think we're going into an era where we have to deal with a new toughness about budget. I know that the Republicans are talking very much about a very severe attitude toward budget deficits, reducing it dramatically, reducing resources available in very, very important programs. The whole concept of the military getting the amount of money that it gets, I think, is beginning to wear on the American people just a bit, because it's—in the President's budget cut, it was exempted—it was exempted—as, in fact, was intelligence. Well, that's good, because we're still in a post-9/11 way of thinking—and we are, very much so—that we've got to stop everything. And therefore, you have to grow, grow, grow.

But, at some point, you also have to make what you are doing work. And so, I come back to the little boats. Secretary Napolitano was here some time ago, and she's got this—you all have this test-radiation-detection-equipment thing going on to find out radiation devices, containers, whatever, that are found in relatively small pleasure boats or commercial boats. Now, you can't, sort of, board each one of these things, because they'd tip over. So, you have, sort of, drive-by or motor-by detection devices, trying to figure out, Are these enemies, or not? You don't really care whether they like America or not, but you care very much about whether they have onboard something which is—could go off in a port, anywhere. And Senator Lautenberg was describing, and Senator LeMieux, how close these ports are to hundreds of thousands, millions of people.

So, I just want to press you on this question, Admiral Papp, of the—you know, what do you know about these little boats? That's something that can be done. I'm not interested in, Do they like us? I'm not interested in outreach, sort of driver education, "Drive—do it safely," all that. I'm interested in your response to matters relating to terrorism and destruction in America.

And to you, Mr. Bersin, these are paramount.

So, now, your world is going to be one—and you have a lot of helicopter problems, you have a lot of helicopter crashes. You didn't used to, but you've got old equipment. Your ice cutters are 45 years old now, right? No money to fix them up. Your Merchant Marine Academy needs a lot of repair. It takes money. I'm not sure the money is going to be there in the future. I'm not sure of that.

So, what—how do you take all of these things that you have to keep your mind on, in terms of being secure—you each have intelligence agencies—I don't think the GAO does, but I may be wrong—but you have intelligence agencies. I don't know how much you share with other intelligence agencies, or whether they share it with you, or whether there's any attempt to make all of that going on. But, we've got to find efficient ways of protecting people. And, in the case—I'm just using small boats sort of symbolically—but that's something we ought to be able to do. It's like—

Why am I offended that I can get on a general aviation aircraft without going through one inch of security, and the pilots can do exactly the same? And I can carry anything I want onto a general aviation plane, and nobody pays any attention. I just go out to Dulles, get on a general aviation plane—don't do it very often, but I can do it and nobody pays any attention. That is not acceptable, in terms of national security. That is unacceptable. There are agencies that allow that, agencies that could stop that.

We could do the same with small boats. I'm not saying small boats are the whole issue, but it is an issue, and it's the one that I'm picking on.

So, what about these motor-by radiation detector things? I don't think they're working very well. I could be wrong. And if you've got 17 million, where do you start? Do you start in Houston? Do you start in Newark? Do you start in Fort Lauderdale? You know, it isn't just a question of—you know, coming to hearings must be awful for you. You must hate doing it. But, we have to get a sense of how money is being spent, and what the results we are getting from that money are.

I'm a huge fan of the Coast Guard—you ask Admiral Allen—huge fan of the Coast Guard. But, the Coast Guard has to perform. It doesn't matter whether I like them or don't like them; they have to perform. And you can't come up here and say, "Well, we're doing the best we can. And yes, there's a long distance between 5 percent and 100 percent." And if we can't do 100 percent, or you don't—we could, but—if you had the money, but you don't have the money, then you do need to tell us that so we do change the law, which is at least being square with the American people.

Now, you understand what I'm saying, and I don't have to ramble on, here. But, I feel very strongly about this, that we—we talk to each other in acronyms, we talk to each other in, sort of, statements of certainty, of effort, of aspirations, and yet, when it gets down to, what are the results, really, and what are the reasons those results can't be better? Is it a matter of money? Is it a matter of personnel?

And then again, you run into budget problems in the future. I think we're going to have substantial budget problems in the future. In fact, I guarantee you we're going to have substantial budget problems in the future.

So, just taking what I've said, and picking out whatever little morsel you want, please respond.

Admiral PAPP. Yes, sir. Thank you, Mr. Chairman.

You know, you're absolutely right. It is a tremendously vexing and challenging problem. Seventeen million boaters. But, you know, it's analogous to—I don't know how many cars are in this country. I would venture to say—well, I won't even venture to say. There are many, many more, by magnitudes—cars, trucks. And we know that people have used car bombs and/or truck bombs. You only have to look back as far as Oklahoma City to see that that method has been used. Can we keep people off the streets? Can we prevent another car bomb from happening? I think that's quite a challenge. And I think it's an—analogue to what we're trying to do.

Now, we have authorities. We can shut down—our Captain of the Ports have authorities to shut down waterways, take all the boats off. Now, we do that from time to time. If there's a major security event, whether it's an inauguration, whether it's a Super Bowl game that's alongside the Detroit River, we will shut down waterways because of the increased threat and potential for something to happen.

The CHAIRMAN. But, you know what? I don't count that. I'm not going to let you get away with that, because—

Admiral PAPP. OK.

The CHAIRMAN.—those are predictably dangerous situations; and so, of course everybody, you know, goes around with Uzis and AK-47s and although—I mean, sure, we load up, we have absolute protection, and we shut the waterways down. But, there are the under—the other 364 days a year, where there aren't large events, and there are small ports or large ports and millions of people, and 17 million boats. Didn't mean to interrupt you, but I did.

Admiral PAPP. No, sir. And you're absolutely right. We put in an awful lot of effort on those events. And what I call them is low-probability/high-consequence events, with the amount of structure

we put around them, it's unlikely that an event is going to occur, because we have strengthened and fortified that particular event.

The CHAIRMAN. But, don't you understand—

Admiral PAPP. What concerns me is—

The CHAIRMAN. That's why I don't like your—

Admiral PAPP. Yes, sir.

The CHAIRMAN.—answer, because that's a special situation.

Admiral PAPP. Yes, sir.

The CHAIRMAN. I'm talking about the other 364 days, because that's when something's going to happen.

Admiral PAPP. Well, the vast majority of those 17 million boaters are law-abiding citizens of the United States who, by our nature, are resistant to discipline, structure, and regimes that prevent them from enjoying what they perceive as their right to enjoy the waterway. And therein lies the problem. What sort of strictures, what structure, what discipline, what laws do we put into place that might penalize those—the vast majority of that 17 million while we're trying to find someone who, we don't know for sure is out there?

And that's why I keep on going back to strengthening our intelligence regimes. We have discovered much more through intelligence, where we can track people, where we look at what's being purchased, whether it has the makings for a bomb, whether it's somebody that perhaps has not used the water before, someone becomes suspicious because they buy a large boat, with capacity for carrying things, and they may exhibit behaviors that would indicate that they're not mariners, but might have some nefarious purpose. That's where I see us. Unless we want to have a Coast Guard that is, I don't know, 100,000 people, so that we can have every waterway picketed with our boats out there, I don't know that the country can afford that.

So, given what I have, in terms of resources, I employ them to the best effect that I can, which is leveraging intelligence, strengthening partnerships with—through our Area Maritime Security Committees, and doing the best we can with the resources that we have. And sometimes, yes, sir, knocking on wood, keeping my fingers crossed that there's nothing out there that we haven't detected or that we're not going to be able to get to.

So, I understand, and I fully comprehend—you know, sometimes when I speak to groups, they say, "You're just being—that's just paranoia." For me, is it paranoia or is it possible? And if you come down on the side it's possible, then who is responsible for it, and who is doing something about it?

The CHAIRMAN. OK. I—

Admiral PAPP. It's my responsibility—

The CHAIRMAN.—hear you, and my time is—

Admiral PAPP. Yes, sir.

The CHAIRMAN.—like 3 days over.

Admiral PAPP. Yes, sir.

The CHAIRMAN. But, my approach would be—if I were you, I would take some of those—in Fort Lauderdale or Houston, I would take some of those ships, and those commercial pleasure craft, and I'd stop them, and they'd be furious at you, and you wouldn't care, because you have a job to do, which is far greater than the pleasure

which they're experiencing. You're worried about destruction. I'd stop them, and I'd go through them, and you don't have to do it everywhere, you don't have the personnel to do it everywhere, but the word gets around. The word gets around. And that helps. Rather than saying, "The vast majority of Americans are good, law-abiding citizens." That doesn't do much for my conscience.

Admiral PAPP. Yes, sir. Well, I'm sorry, if I haven't been informative enough. When I talk about maritime security operations, that's where these versatile adaptable forces come in. We are doing boardings constantly. We do random boardings.

The CHAIRMAN. You just said, "But, we don't want to interrupt people in their pleasure."

Admiral PAPP. Well, not the vast majority, but we do random. And that is part of our Operation Neptune Shield philosophy, is to do random and scheduled patrols and boardings throughout our areas of responsibility. That's ongoing, every day. We have thousands of boardings that go on, to inspect vessels for safety, but, once we have people onboard, and we're inspecting for safety, if there is some indication of other activity, whether it's drinking or use of drugs, we carry that inspection further.

The truth of the matter is, in the years since 9/11, we have not lost one single person due to terrorism out on the waters of the United States, but every year we lose about 1,000 people for not wearing life jackets and drunk boating.

The CHAIRMAN. That is right.

Admiral PAPP. Yes, sir.

The CHAIRMAN. But, that's also a way that you avoid answering a question, in Washington-speak. "Nothing has happened." Well, the fact of the matter, a great deal has been attempted, and has been interdicted, which you can't talk about. But, you know, if somebody hadn't been there—I'm just—I'm going to stop talking. OK? Because I want to let these others, if they have other questions, to ask them. But, I just want you to read me.

Admiral PAPP. Yes, sir, absolutely.

Senator HUTCHISON. Well, thank you, Mr. Chairman.

I want to ask you something, because I have been concerned, as I think many people know, because I introduced a bill in response to the administration not waiving the Jones Act immediately after the oil spill. And my question is, Do you believe that it would have been more expeditious if we could have gotten the help from the foreign skimmers into the 3-mile limit more quickly? And, if no, why not? And maybe you'll say "no," but why wasn't it done immediately, on an expedited basis, rather than the processes that you have to go through, that the Coast Guard has the control over, to waive the Jones Act on a piecemeal basis?

Admiral PAPP. Well, thanks, Senator, for that question, because, quite frankly, I've just not understood why people have been concerned about this, because it hasn't delayed anything from getting there. The Jones Act did not even come into play—the spill location being that far offshore, there was no implications to the Jones Act. We had foreign skimmers and ships that came in. They weren't involved in trade between ports in the United States, so as long as they stayed that distance offshore, there was no need to provide a waiver, because the Jones Act just did not apply.

Senator HUTCHISON. But, why—

Admiral PAPP. Now, there was the potential—

Senator HUTCHISON.—once the oil was going into the 3-mile limit, then it was going to be going on the shore. So, why wouldn't you want the full capability that those well-equipped foreign skimmers could have given and were offered?

Admiral PAPP. Well, most of the skimmers that were ordered were ocean skimmer—or, offered—were ocean skimmers. That's where we needed them, out close to the source. We needed to collect as much oil as we could out at the source, at the well. And we've been very successful at doing that. And there was never any delay in getting any of those foreign skimmers because of any Jones Act considerations. And, in fact, they've been helping us out greatly.

Now, to bring in smaller in-shore skimmers, we've just—we have had, between the skimmers we have, organically, in the United States, the thousands of vessels of opportunity that we had step forward in the Gulf, that were employed in the skimming operations, there was just no need for any additional—to my knowledge; now, this is one of the details the National Incident Commander could get into—but, to my recollection, there was no need for smaller, in-shore foreign skimmers to come in, which would not—if they did, it would require a waiver. I know Secretary Napolitano was ready and willing to provide a waiver, if needed, but there just was no need for it.

Senator HUTCHISON. And you feel that there were sufficient numbers—it's sort of a disconnect, from what was being reported and what you're saying, about the numbers of skimmers within the 3-mile limit being sufficient. Do you feel that you had the sufficient number within the 3-mile limit?

Admiral PAPP. In terms of the breakdown in responsibilities—and I have to go back to Senator Rockefeller, because I feel badly, because this is the first time I've ever been accused of Washington-speak in my career, so I'm trying to be as clear and frank as possible—I—the—Admiral Allen is the National Incident Commander. It's my role, as the Commandant of the Coast Guard, to support him with Coast Guard people and forces. So, to that extent, we have given 100-percent support to Admiral Allen in that effort, using Coast Guard forces, Coast Guard people. I've been involved, peripherally, because I've sent some of my admirals, my flag officers, down there to work within the National Incident Command process, so I get some feedback, and my feedback is that we've had sufficient resources down there, that the National Incident Commander, Admiral Allen, has received everything that he has asked for. And so, I have not seen the problem.

Senator HUTCHISON. Well, you are getting into Washington-speak, because I understand what Admiral Allen's role is. There is a disconnect between what we read and see, versus seeming like we're not making the maximum use, in the most efficient way, of the offers that were given.

Let me ask a final question, and that is, the Houston Ship Channel Security District has put in place a fee structure that would allow port tenants and also the Federal dollars to be able to be pooled for port security to be done on a portwide basis. Is this

unique among the other ports, this model? And are others doing it? What's good about it? And is it being implemented in a positive way, which we think is the case, but—is it unique?

Admiral PAPP. I think my friend, the Commissioner, is itching to answer, here, but I have learned about it recently, and I'm encouraged by it. I think it's a great way—and actually, it works within our Area Maritime Secure Committee, that effort—the Coast Guard Captain of the Port in Houston works with the district. And I've received some very encouraging reports. It's exactly what we're looking for, in terms of not just Federal forces providing for security, but the community, the port, and the State all coming together so that—none of us can do it fully on our own; all together, we can do a much better job.

Senator HUTCHISON. Is it a value added, Mr. Bersin?

Mr. BERSIN. If I might—absolutely. In the—it's not unique. What makes the Houston Ship Channel so—makes it one-of-a-kind are the number of jurisdictions that are around the particular area. But, in fact, multi-jurisdictional participation in joint harbor commands or the kinds of interagency and intergovernmental bodies that the Admiral spoke about before, I think, is the way in which we get the greatest leverage out of every—all the governmental authorities. So, that particular model is not unique, but it's very effective.

And I know, on the CBP side, all of the Federal agencies are gathering together to work with the many jurisdictions on the channel to build a common security plan, and then to have the financing to see that it's implemented effectively.

Senator HUTCHISON. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much, Senator Hutchison.

I thank all three of you very much. This has been a very informative hearing. And I'm sorry more members didn't come out, but these are strange days in the Senate.

And this hearing is adjourned.

[Whereupon, at 4:20 p.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV
TO ADMIRAL ROBERT J. PAPP

Question 1. In spite of the recent economic downturn, the rate of global commerce is forecasted to increase over the next few years. As trade and the economy improve, a significant portion—more than 80 percent by some accounts—of goods entering the United States will come through our domestic ports. Given the economic importance of ports, vessels, and waterways, their security is absolutely critical. Where do you see the greatest port security risks? What are you doing to mitigate those risks? How do you believe S. 3639 addresses these concerns?

Answer. The tremendous amount of CIKR and population within or near America's waterways provides terrorists potential opportunities to conduct physical and psychological damage. The Coast Guard makes a determined effort to provide security for about 95,000 miles of coastline. It is responsible for protecting over 300 ports and over 10,000 miles of navigable waterways. It provides security for a myriad of landside connections which allow the various transportation modes to move people and goods to, from, under, and on the water. More than \$958 billion of international commerce, including 1.4 billion tons of cargo, is transported within the MTS. Most cargo is carried by foreign vessels and crews that the Coast Guard cannot as easily scrutinize for security threats as it can U.S. flag vessels. The Coast Guard is challenged to protect more than 8 million cruise ship and ferry passengers as part of a transportation segment that logs more than 65 million passenger-miles a year (a 21 percent increase above the average just 6 years earlier). The Coast Guard secures waterways for numerous boaters operating almost 13 million registered recreational vessels. Additionally, the Coast Guard protects the domestic movement of numerous high value military vessels and maritime cargo for national defense and national security. The vast and complex CIKR and MTS of this Nation and its citizenry is exposed to an extremely unpredictable and diverse set of terrorist and other security threats.

U.S. Marine Transportation System components (*i.e.*, ports, waterways, maritime critical infrastructure and key resources (CIKR), and vessels) are potentially vulnerable to a myriad of maritime and shore-based attack methods (*e.g.*, underwater swimmers, mines, stand-off weapons, small vessel¹ attacks, vehicle and waterborne improvised explosive devices (VBIED/WBIED), etc.).

The Intelligence Community reports no credible indications exist that terrorists are planning to use small vessels in an attack on the United States. However, among the viable maritime attack methods, the direct and indirect use of small vessels generates the greatest concern.

The Coast Guard and other law enforcement agencies face the challenge of distinguishing between the vast number of legitimate vessel operators and the relatively few individuals engaged in illicit and potential terrorist activities. The challenge is immense, as it involves nearly 13 million registered U.S. recreational vessels, 82,000 fishing vessels, and 100,000 other small commercial vessels. On any given day, a considerable number of these boats share waterways with commercial deep draft and military vessel traffic, operating in hundreds of U.S. ports and in the immediate vicinity of maritime critical infrastructure and key resources.

Overall, S. 3639, if enacted, could facilitate or assist the fulfillment of some of maritime security by increasing the transparency associated with owners and operators of recreational vessels, enhancing maritime domain awareness, mitigating small vessel security risk and increasing cooperation and coordination amongst stakeholders.

¹Small vessels are characterized as any watercraft, regardless of method of propulsion, less than 300 gross tons. Small vessels can include commercial fishing vessels, recreational boats and yachts, towing vessels, uninspected passenger vessels, or any other commercial vessels involved in foreign or U.S. voyages.

Question 2. As the U.S. Coast Guard's responsibilities and role in safety and security issues continues to broaden, questions have surfaced about whether the Coast Guard has sufficient resources to adequately execute its missions. Do you believe that we should look to assessing a port security user fee to help manage the growing cost associated with port security? Should the cargo and shipping industries along with other users be required to pay a similar fee?

Answer. A fee-based structure could be appropriate to fund security services that benefit specific users of port facilities. A review of existing fees would be an important first step in making that determination.

Question 3. The Coast Guard is currently examining technologies to test radiation detection equipment, but thus far it appears the results indicate that the technology has operational issues (*i.e.*, is not operating at high speed or far distances). Is this the case and are you confident that the technology works? What alternative technologies are you considering? Will the U.S. Coast Guard commit to coordinating with DOE going forward? Please provide a summary of findings to-date on the tests, the determination of the viability of the technology, and what plans Coast Guard has formulated to address the deficiencies.

Answer. The Coast Guard is not leading any efforts to examine technologies to test radiation detection equipment. The current radiation detection/identification equipment deployed by the Coast Guard is adequate and meets or exceeds Coast Guard Maritime Radiation Detection Program mission requirements. The Coast Guard currently uses human portable systems which typically require boarding team and inspectors to physically board a vessel. Future goals of the Coast Guard Maritime Radiation and Nuclear Detection Program are to minimize the need to board each vessel through the use of stand-off detection and identification technologies. However, based on a review of the results from recently completed testing by the DHS Domestic Nuclear Detection Office (DNDO), stand-off detection/identification is in the embryonic stage of development and the technology does not currently exist to resolve this problem in the short-term.

DHS Domestic Nuclear Detection Office (DNDO) has the lead for the research, development, testing, evaluation, and acquisition of radiological/nuclear detection and identification equipment to ensure that it is fully aligned with their Global Nuclear Detection Architecture (GNDA). USCG has worked with DNDO on the development of requirements for next-generation detectors to ensure that they meet USCG maritime domain requirements. As the lead in detection architecture development, DNDO would be in a much better position to provide a summary of findings to-date concerning tests and technology viability.

The Coast Guard has a long-standing relationship with the Department of Energy (DOE) and the National Nuclear Security Agency (NNSA) and will continue to coordinate our maritime radiation detection program efforts with DOE for technical support. In the event that Coast Guard detects and/or identifies a potential or actual radiological material threat, Coast Guard operational protocol provides mechanisms for requesting the technical services of the DOE/NNSA Radiological Assistance Program (RAP) Teams or the Nuclear/Radiological Advisory Team (NRAT).

Question 4. The Coast Guard is required to perform 2 inspections at MTSA-regulated facilities each year, with one of these being an unannounced inspection. Is an unannounced spot check a sufficient gauge of facility compliance with MTSA? How does it differ from an announced inspection? Is the Coast Guard finding greater non-compliance during unannounced inspections? Coast Guard staff who conduct facility inspections are often assigned multiple duties while they are responsible for facilities that are growing in size and number.

Answer. Yes, unannounced spot checks, as part of a compliance program, are an effective port security tool. During the spot check, Coast Guard personnel are able to carry out inspections until they are satisfied that the facility has met the Maritime Transportation Safety Act (MTSA) requirements.

Typically, announced inspections are MTSA Annual Compliance Exams. These exams may take days to complete, will involve the Facility Security Officer (FSO) as well as other facility personnel, and cover the entire Facility Security Plan in detail. The Coast Guard traditionally schedules MTSA Annual Compliance Exams with the FSO to ensure that the necessary facility personnel are present for the examination and have set aside the requisite amount of time from their daily responsibilities. If a facility has not met the level of security required by MTSA the Captain of the Port (COTP) may conduct additional unannounced MTSA annual compliance examinations.

Between January 1, 2010 and August 4, 2010, there have been 1,358 announced MTSA Annual Compliance Exams conducted. Out of those exams, 18 facilities, or approximately 1.3 percent, did not meet inspection compliance, of the 1,789 unan-

nounced security spot checks there were 6 facilities, or approximately 0.3 percent, which did not meet compliance.

Question 5. Has the Coast Guard conducted any analysis of their inspection requirements to ensure that staffing needs are met and inspections meet their stated goals?

Answer. The Coast Guard has developed and continues to refine a Sector Staffing Model (SSM) to examine several critical factors such as mission hours and activity levels as well as personnel, skill sets, qualifications, experience level, etc., in determining the appropriate number of personnel in key facility inspection positions for various mission areas. The Coast Guard's Marine Safety Improvement Plan is the Service's multi-year plan to enhance performance of the Marine Safety mission through various initiatives including increasing the number of marine inspectors.

Question 6. Coast Guard port security procedures establish specific activity goals, known as Operation Neptune Shield (ONS)—in support of the agency's strategic plan for ports, waterways and coastal security. There are well documented shortages of resources, including GAO reports noting that Coast Guard's inability to meet its own standards. Does the Coast Guard have sufficient resources to handle elevated threat levels?

Answer. The Coast Guard employs risk-based decisionmaking to allocate resources. Using the Maritime Security Risk Analysis Model (MSRAM), the Coast Guard identifies the highest risk vessels, maritime critical infrastructure and key resources (CIKR) within the threatened region, port(s), or National Infrastructure Protection Plan Sector(s). These risk-based results help guide the Coast Guard operational commanders' application of their resources to mitigate the highest maritime risk.

In response to elevated maritime threat levels, the Department of Homeland Security (DHS) may elevate the Homeland Security Advisory System (HSAS) Threat Condition. The Coast Guard Commandant in coordination with the Secretary of DHS, may set elevated MARSEC Levels 2 or 3 nationwide, regionally, by port(s), or by National Infrastructure Protection Plan (NIPP) Sector(s), (e.g., Transportation Systems, Energy, Chemical, etc.). DHS and the Coast Guard endeavor to apply the HSAS Threat Condition and MARSEC Levels in a targeted manner to balance the need for additional security measures against the impacts of those security measures upon the U.S. Marine Transportation System, maritime commerce, and recreational activities in ports and on waterways.

To meet the MARSEC Level 2 and MARSEC Level 3 performance standards, Area Commanders may relocate existing resources from outside of the affected areas and may surge resources from other missions. The ONS OPORD contains provisions to mitigate the impact of surging resources on the Coast Guard's other missions. The ONS OPORD authorizes Area Commanders to adjust the other mission's performance standards.

Sustained MARSEC Level 2 or MARSEC Level 3 operations may justify the recall of Coast Guard Reserve forces under the Secretary of DHS's authority found in 14 U.S.C. 712. Reservists recalled under Title 14 may be issued orders for up to 60 days. Since 2008, the Coast Guard has annually obtained pre-approval from the Secretary of DHS for the Commandant to involuntarily recall up to a pre-designated number of Coast Guard Reservists under Title 14 to ". . . aid in prevention or response to an imminent catastrophe, act of terrorism, or transportation security incident. . . .", thus enhancing our mobilization readiness and the Coast Guard's ability to respond with minimum delay. The use of Coast Guard Reserve forces is subject to certain limitations, particularly the "dwell time" required between periods of active duty.

Question 7. The number of vessel arriving into U.S. ports has generally increased over the past few years and this trend is expected to continue in the near future. What challenges does this increased workload pose to the Coast Guard in terms of its ability to carry out its mission to board and inspect foreign vessels, especially those deemed high-risk?

Answer. The Coast Guard uses a risk-based approach to mitigate resource gaps, and identify and inspect high risk vessels. As a result of a 2007 comprehensive Marine Safety program review, the Coast Guard identified opportunities to improve capacity and competency through development of the Marine Safety and Improvement Plan. Through development of this Plan, the Coast Guard established a roadmap to improve the effectiveness, consistency, and responsiveness of the program to promote safe, secure, and environmentally sound marine transportation. This roadmap includes reinvigorating industry partnerships, improving technical competencies, increasing the number of inspectors, engineers and investigators, and expanding rule-

making capability to ensure the Coast Guard meets current and future program needs.

Question 8. What steps has the Coast Guard taken to ensure it has the capability and resources to fully carry out its port state control and security boarding responsibilities even as the potential number of vessels needing to be examined or boarded continues to increase?

Answer. The Coast Guard has taken several steps to effectively manage capability and resources to carry out Port State Control (PSC) and security boarding responsibilities. Examples include:

- 2006—New PSC targeting matrix for better targeting of high risk vessels and reduced targeting of low risk vessels;
- 2007—New PSC Training Regime with new courses and improved qualification standards;
- 2008—New High Interest Vessel (security) targeting matrix refined targeting of high risk vessels, reduced targeting of low or no risk vessels; and
- 2010—Maritime Enforcement Specialist (ME) Rating established, and the ME school and qualification procedures established.

Additionally, through the development of the Marine Safety Improvement Plan (MSIP), provided to Congress in October 2007, the Coast Guard developed a multi-year plan to increase the core capabilities of the marine safety program to support and infuse the needed resources to address the growth of responsibilities for the boarding and examination of foreign vessels arriving and operating in U.S. waters.

The Coast Guard is in the process of implementing this multi-year plan. The MSIP provides a roadmap to improve the effectiveness, consistency, and responsiveness of the program to promote safe, secure, and environmentally sound marine transportation. This roadmap includes reinvigorating industry partnerships, improving technical competencies, increasing the number of inspectors, engineers and investigators, and expanding rulemaking capability to ensure the Coast Guard meets current and future program needs.

Question 9. The Coast Guard has formal MOUs or other agreements with state and local law enforcement authorities in some ports for sharing security resources in an elevated MARSEC situation. To what extent have these agreements been formalized to leverage other stakeholder's resources for ensuring port security?

Answer. The legal framework for providing maritime security consists of the overarching Security and Accountability for Every (SAFE) Port and Maritime Transportation Security (MTSA) Acts supported by three statutory pillars: The Magnuson Act (50 U.S.C. 191 et seq.), the Ports and Waterways Safety Act (PWSA) of 1972 (33 USC 1221 et seq.), and Coast Guard operating authorities contained in Title 14, U.S. Code. Collectively and through the implementation of scalable requirements driven by Maritime Security (MARSEC) Levels, this architecture establishes risk-based maritime security burden sharing for federally-regulated waterfront facilities and vessels among Federal, State, and local government entities and industry. Layered security is a manifestation of this shared maritime security responsibility. The initial responsibility for State and local government entities is to resource the activities that they are executing for their portion of the layered security. State and local government may share resources with and provide assistance to the Coast Guard.

Pursuant to requirements within the MTSA as amended by the Security and Accountability for Every Port (SAFE Port) Act of 2006, Coast Guard Captains of the Port (COTP) serving as Federal Maritime Security Coordinators (FMSC) worked in conjunction with their port partners to establish and convene Area Maritime Security (AMS) Committees, conduct AMS Assessments, and to develop required formal AMS Plans. These very comprehensive AMS Plans serve as Coast Guard-coordinated, port community-oriented maritime antiterrorism preplanning of joint deterrence efforts for transportation security incidents (TSI). The AMS Plans provide a strategy for coordinated and scalable actions to detect, deter, and prevent threats at varying threat levels throughout the respective COTP zones.

In August 2009, the Coast Guard completed the first formal five-year update of the Nation's 43 AMS Plans in coordination with respective AMS Committees, as required by MTSA. The FMSCs and AMS Committees use the Coast Guard's Maritime Security Risk Analysis Model to conduct AMS Assessments as required by MTSA implementing regulations in 33 CFR 103.400 to 103.410. The FMSCs/AMS Committees use the results of the AMS Assessments to identify the top three types of Transportation Security Incidents (TSI) most likely to occur in their port areas. All the AMS Plans include procedures and steps to be taken for prevention, protection, security response, and recovery from the identified TSI planning scenarios should such an attack be threatened or actually occur (elevated threat levels). As

stated in the Navigation and Vessel Inspection Circular No. 09–02, Change 3 (Guidelines for Development of Area Maritime Security Committees and Area Maritime Security Plans Required for U.S. Ports), “. . . these Plans may be viewed as unofficial Memorandums of Agreement (MOAs) within the port to ensure key players understand what activities each agency will take, and what resources each will bring for the given scenario.”

The AMS Plans are required to be exercised annually, as part of the Coast Guard’s Area Maritime Security Training Exercise Program (AMSTEP). The AMS Plans and the required AMSTEP exercises are critical elements of the Nation’s maritime security preparedness and enable, at minimum, an annual opportunity for Coast Guard, Federal, state and local law enforcement, tribal and industry representatives, and other governmental agencies to validate the AMS Plans and resource sufficiency and stakeholder responsibilities in light of on-going risk analysis.

In addition numerous Coast Guard operational commanders and State and local government entities have found it beneficial to enter into memoranda of agreement (MOAs) or memoranda of understanding (MOUs). MOAs and MOUs are detailed and have a narrower focus than AMS Plans. They vary in content, based on local resources and needs. They often address tactical specifics such as use of force policy, communications, training, reporting, etc. Several of the existing MOAs and MOUs specifically address elevated Maritime Security (MARSEC) Levels. With respect to the actual sharing of resources, these MOAs and MOUs are considered non-binding on the signatory parties. The State and local government entities may decline requests for resource support from the Coast Guard on the basis of risk-based decisions made to mitigate their share of the maritime security risk or to mitigate higher priority, non-maritime security risks. When elevated Homeland Security Advisory System Threat Conditions or MARSEC Levels are set, it is highly likely that State and local government entity resources may already be fully engaged and therefore unavailable to the Coast Guard. Within an Incident Commander or Area Commander command structure established to manage the incident or event prompting the elevated MARSEC Level, particularly MARSEC Level 3, State and local resources will likely be applied per the approved Incident Action Plan.

Question 10. The Coast Guard—through its International Port Security Program—has completed several rounds of visits to foreign countries to make sure that they meet established port security standards. What standards does the Coast Guard use to make these assessments? How do these standards compare to those used in assessments of domestic U.S. ports?

Answer. The Coast Guard uses a country’s implementation of the mandatory provisions of an international security standard, the International Ship and Port Facility Security (ISPS) Code, as the primary indicator of whether effective anti-terrorism measures are in place. We also consider intelligence information to validate our observations and to ascertain the terrorist threat posed by the country. Regulations issued pursuant to the Maritime Transportation and Security Act (MTSA), 33 CFR Parts 101 through 106, are the standard used to inspect domestic ports. These regulations were developed in conjunction with and are representative of the standards set forth in the ISPS Code. MTSA regulations, however, are more comprehensive, specific, and detailed than the minimum requirements established in the ISPS Code.

Question 11. Every 2–3 years the Coast Guard must inspect facilities in approximately 150 countries participating in the International Port Security Program. How does the Coast Guard determine which ports and facilities it should assess in each country? Does the Coast Guard have the necessary resources to carry out these inspections?

Answer. The Coast Guard uses a risk based approach to determine the port facilities it will visit. The greater the risk the country poses, the more facilities in that country the Coast Guard visits. In general, the Coast Guard seeks to visit a representative sample of large, medium, and small International Ship and Port Facility Security Code regulated facilities that reflect the trading patterns of the country with the U.S. Emphasis is placed on visiting those facilities that have direct trade with the U.S., port facilities that have not yet been visited, and facilities previously visited at which the Coast Guard identified security deficiencies.

The Coast Guard has sufficient resources to visit an adequate sampling of facilities in all countries that conduct maritime trade with the U.S.

Question 12. What has Coast Guard determined will be the impact of rotation length for International Port Security Program personnel, given the training and experience needed for effective observations of facility security during country visits?

Answer. The Coast Guard has determined that its rotation policy has no significant impact on the ability of the International Port Security Program (IPS) to con-

duct its mission. IPS Program personnel receive specific training upon being assigned to the program and continue to advance their skills through on-the-job training with more experienced program personnel. In addition, the program has a cadre of civilian personnel that provide continuity.

Question 13. The Coast Guard continues its visits to the ports of foreign maritime trading partners to assess the effectiveness of antiterrorism measures in those countries' ports. Recognizing that some countries may not be receptive to an expectation that they provide the Coast Guard with periodic access to their ports every few years for a visit, what steps is the Coast Guard taking to address the concerns of those countries and gain their cooperation? Does S. 3639 provide sufficient authority to assist countries in meeting this requirement?

Answer. Due to sovereignty concerns, it is becoming increasingly difficult to gain access to countries for re-assessments. The Coast Guard offers what it calls "reciprocal visits" in which the Coast Guard hosts representatives from the Designated Authority of foreign countries to observe how the Coast Guard implements the international security standard, the International Ship and Port Facility Security Code.

While there is a requirement for the Coast Guard to assess countries, there is no requirement for those countries to be assessed. The Coast Guard is dependent on the country granting access to allow the observation of the security conditions. As noted above, this is becoming increasingly difficult. S. 3639 would clarify and strengthen the Coast Guard's ability to make a finding that effective anti-terrorism measures are not in place in such cases where countries refuse to grant us access. Where possible, the Coast Guard works with other agencies, such as the State Department, to provide capacity building assistance in order to overcome security deficits when a country is having difficulty implementing the international security standard.

Question 14. To carry out the security boardings of high interest vessels, some field units rely on the Maritime Safety and Security Teams (MSSTs) and their related assets. However, these teams and their assets may become unavailable to carry out these boardings if they are deployed to respond to a natural disaster or national security threat that may require them to conduct security activities other than security boardings. Under such circumstances, to what extent will these Coast Guard units be able to conduct security boardings? What actions does the Coast Guard plan to take to ensure that those field units can carry out their required boardings or otherwise mitigate the potential risks?

Answer. The Maritime Transportation Security Act of 2002 directed the creation of Maritime Safety and Security Teams (MSSTs) to enhance the domestic maritime security capability of the United States. MSSTs are deployable specialized forces that are not dedicated to a specific port, and routinely deploy in support of a designated national security event or in response to a natural disaster. When not deployed, MSSTs do augment local forces by conducting some operational activities under Operation Neptune Shield (ONS), such as escorts of high capacity passenger vessels. However, MSSTs perform a relatively small percentage of the high interest vessel security boardings in their respective homeports. Coast Guard Sectors will continue to be the backbone of Coast Guard security efforts in a port, including security boardings of high interest vessels. Therefore, deployment of MSSTs will not have a significant impact on a Sector Commander's ability to conduct security boardings.

Question 15. In November 2009, a group of terrorists in small vessels arrived in Mumbai, India and attacked multiple targets, killing more than 100 people. With regards to the United States, are we just as vulnerable to foreign terrorists in small vessels, perhaps arriving from the Caribbean, attacking our cities or maritime infrastructure? Does DHS have any programs that would be able to track and prevent such small vessels from carrying out such an attack?

Answer. While the Intelligence Community reports no credible indications exist that terrorists are planning to use small vessels in an attack on the United States, their use overseas (such as in Mumbai, India in November 2009) is a clear indicator of a capability.

The Department of Homeland Security (DHS) is concerned about security risks associated with small vessels and has taken steps to mitigate such risk.

The DHS Small Vessel Security Strategy (SVSS) was developed in an effort to mitigate potential risks associated with small vessels. Numerous activities supporting the Strategy are already being implemented or have been completed. For example:

- Maritime Domain Awareness initiatives:

- The Citizen Action Network (CAN), which has long served the Puget Sound area, and Focused Lens (FL), developed in California ports to systematically increase maritime patrol presence and effectiveness, have begun working with the America's Waterway Watch (AWW) program to develop a model for upgraded suspicious activity information collection. This coordinated set of programs was tested with Canadian partners during the 2010 Winter Olympics and plans are being formulated to roll it out nationally.
- Under the combined leadership of the United States, the United Kingdom, and Japan, the International Maritime Organization (IMO) developed and issued Non-Mandatory Guidelines on Security Aspects of the Operation of Vessels Which Do Not Fall within the Scope of SOLAS Chapter XI-2 and the International Ship and Port Facility Security (ISPS) Code. These guidelines are being included in the National Association of State Boating Law Administrators' standards of training for boat operators, and in the U.S. Power Squadrons' training materials.
- Our primary system to track vessels today is the Nationwide Automatic Identification System (NAIS). Currently, as per national and international regulations, AIS is required to be carried on commercial vessels greater than 300 gross tons. However, a Notice of Proposed Rulemaking (December 2008) proposed to mandate AIS carriage on smaller commercial vessels, fulfilling the requirements of the Maritime Transportation Security Act of 2002 (MTSA) and addressing a considerable number of small craft.
- Our Vessel Traffic Services track vessels by radar, AIS, and in some cases by camera, in several major commercial ports, and by various sensors employed by U.S. Coast Guard (USCG) Sector or Interagency Operations Centers.
- We have expanded upon the requirements of the MTSA directed Area Maritime Security Plans (AMSP), Vessel Security Plans, and Facility Security Plans to require planners specifically address potential small vessel risks, with plan revisions completed at the appropriate 5 year revision cycle (in most cases, in 2009).

A key function of our tactical methods to address small vessel threats are addressed through Maritime Security and Response Operations programs, under the Coast Guard's Operation Neptune Shield. This is a tiered system, which aligns with and supports DHS' Homeland Security Advisory System (HSAS) and represents a diverse set of operational activities, many of which directly relate to small vessel security risks:

- Waterborne, airborne, and shoreside patrols and visits to critical infrastructure.
- Security boardings of small vessels—Operation Neptune Shield has a specific requirement for each Sector Commander to conduct a minimum number of security boardings of small vessels (<300 GT) each month.
- Vessel escorts of:
 - High Value military ships;
 - Vessels carrying high consequence cargoes; and
 - A percentage of high capacity passenger vessels (*e.g.*, cruise ships, ferries)

Taken as a whole, these awareness programs, regimes, and operational measures are intended to provide layered security against small vessel and other security risks in the maritime domain.

Question 16. In April 2008 DHS issued its Small Vessel Security Strategy and is now developing a more detailed implementation plan. When will that detailed implementation plan be completed and approved? Will DHS be seeking more authorities or resources to implement the plan? If not, how will the strategy and plan have any impact on the potential threat of small vessel attacks?

Answer. As described in the response to Question 12, numerous activities supporting the Strategy are already being implemented or have been completed. While there is no formal implementation plan, DHS has prepared a security-sensitive internal document (referred to as an implementation plan) to help guide small vessel security investments by Department and its components. Additionally, DHS will soon finalize a document for release to the public that provides examples of planned and ongoing activities, especially those that depend on cooperative efforts and public engagement.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO
ADMIRAL ROBERT J. PAPP

Question 1. The SAFE Port Act required that the Coast Guard establish Interagency Operation Command Centers at all high priority ports by October 2009. Why hasn't an IOCC been established in the New York/New Jersey region and when will the Coast Guard move forward?

Answer. The WatchKeeper information management software will be deployed to Sector New York in Fiscal Year 2011. Interagency Operations Centers (IOCs) are being established in 35 high priority ports nationwide with one IOC centrally located within the geographic area of responsibility in each of the Coast Guard's 35 Sectors. For each location to officially achieve designation as an IOC, at a minimum, the following must be in place:

1. A regular schedule of coordination meetings with Federal, state, and local port partners, as appropriate.
2. Shared awareness of the operational schedules of maritime assets between IOC member agencies.
3. IOC member agencies have direct access to WatchKeeper information sharing capabilities.
4. Joint awareness and coordination between Coast Guard and U.S. Customs and Border Protection of planned vessel inspection activities.
5. The IOC operates under a Unified Command structure and members adhere to best practices.

To support these IOCs, the Coast Guard established the IOC Acquisition Project to provide the means for collaboration and consensus-building needed to enhance unity of effort among maritime stakeholders.

Question 2. Last September, the DHS Inspector General issued a highly critical report on the Department's efforts to address small vessel security. The IG stated that the Department has not provided a comprehensive strategy for addressing threats from small vessels, such as those used in the USS Cole and Mumbai attacks. Since this report was issued, what additional steps has the Coast Guard taken to address small vessel security?

Answer. The Coast Guard played a critical role in the Department of Homeland Security's (DHS's) development of the Small Vessel Security Strategy (SVSS). The Coast Guard has already implemented and expanded a number of measures to address security threats posed by small vessels. For example:

- Maritime Domain Awareness initiatives:
 - America's Waterways Watch;
 - Citizens' Action Network
 - Automatic Identification System (AIS) carriage requirements; and
 - Robust intelligence gathering and analysis, including Field Intelligence Support Teams at each Coast Guard Sector.
- Security Regimes:
 - Area Maritime Security Plans (AMSP), which conform to the Maritime Transportation Security Act (MTSA), include actions to mitigate small vessel attacks;
 - Coast Guard approved security plans are required for MTSA regulated vessels and facilities; and
 - Coast Guard Captains of the Port (COTPs) possess broad authorities to control port access, movement, and activity.
- Maritime Security and Response Operations:
 - The Coast Guard utilizes a tiered risk-based system, which aligns with and supports DHS' Homeland Security Advisory System;
 - A diverse set of operational activities, including:
 - Waterborne, airborne, and shoreside patrols and visits to critical infrastructure; and
 - Security boardings of small vessels.
- Vessel escorts of:
 - High Value military ships;

- Vessels carrying high consequence cargoes; and
- High capacity passenger vessels (*e.g.*, cruise ships, ferries).

Question 3. The Port Authority of New York and New Jersey is unable to move forward on a number of projects to improve the security of the port because of the twenty-five percent cost share requirement for port security grants. It is my understanding that waiving this requirement is a long, arduous process that is rarely successful. What should be done about this cost-share requirement so that it does not impede the security of our ports?

Answer. The cost-share requirement is a statutory requirement mandated under 46 U.S.C. § 70107 (c). The Secretary of Homeland Security does have the authority (again, pursuant to statute) to reduce the cost-share requirement for Port Security Grant Program (PSGP) projects.

FEMA issued Information Bulletin No. 322 on July 15, 2009 to define the process grantees should follow to submit requests for cost-share waivers for FY 2007, 2008, and 2009 PSGP grants. Cost-share waiver requests are evaluated on a project-by-project basis and generally not granted for an entire award. Each waiver request must contain a strong justification from the prime recipient, proof of written notice to the local Captain of the Port and Area Maritime Security Committee (AMSC), assurance that granting the waiver will not change the security compliance requirements the grantee is required to operate under within their approved security plan, and a revised budget.

All cost-share waiver requests are considered by FEMA, USCG, and DHS leadership. All requests for waivers under this process that have been presented to the Secretary for consideration have been approved thus far.

Question 4. Over a million maritime workers have gone through background checks and obtained TWIC cards, to gain access to secure areas of our ports. The Port Authority of New York/New Jersey is one of the sites testing these TWIC cards. However, this technology has been fraught with challenges and has not been working as intended. How do the challenges with the TWIC program affect the security of our ports?

Answer. The Transportation Worker Identification Credentials (TWIC) program is an additional layer of security that builds upon the sound security regime currently in place under the Maritime Transportation Security Act (MTSA). The Security and Accountability For Every (SAFE) Port Act of 2006 requires the Department of Homeland Security (DHS) to conduct a TWIC pilot program in at least five distinct geographic locations to test the business processes, technology, and operational impacts required to deploy transportation security card readers. Currently, there are 24 TWIC pilot program participants in 10 different geographic locations representing a broad sampling of MTSA regulated facility and vessel operations. The Port Authority of New York/New Jersey is one of the pilot participants.

As of September 27, 2010, TWICs have been successfully issued to over 1.5 million individuals who have gone through an extensive Security Threat Assessment (STA). All personnel requiring unescorted access to secure areas of MTSA regulated facilities and vessels, and all mariners holding Coast Guard issued credentials have been vetted and determined not to pose a security risk to the maritime transportation system. Although the use of readers for checking TWICs has not yet been instituted by regulation, TWICs are required to be used as a visual identification card. Based on the STA and visual inspection of the TWIC, the TWIC program has strengthened DHS' multilayered approach to the safeguarding of our Nation's ports and critical maritime infrastructure.

TSA is working closely with TWIC pilot program participants, the Coast Guard, NIST and industry on technological challenges related to the TWIC reader pilot. Specifically with the Port Authority of New York/New Jersey, there are site visits and weekly calls to assist them troubleshoot issues, some of which are related to requirements they have for their specific implementation of the TWIC.

Verification of the TWIC through the use of readers is the ultimate end state for the TWIC program; it is an additional layer which will build upon a very sound security regime currently in place under MTSA.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BARBARA BOXER TO
ADMIRAL ROBERT J. PAPP

Question 1. The security of our Nation's ports is a major priority for me. Forty percent of our Nation's goods go through the Ports of Los Angeles and Long Beach. California ports from West Sacramento to Oakland and San Diego are economic engines in my state, generating billions of dollars of revenue for our localities. With difficulties and delays in implementing the 100 percent cargo scanning requirement

required by law (The Implementing Recommendations of the 9/11 Commission Act of 2007), what other steps are being taken to ensure that maritime cargo does not pose a security or safety threat?

Answer. In order to ensure the security and integrity of maritime cargo entering the U.S., CBP employs a layered, risk based approach to security. This includes the use of targeting tools such as the Automated Targeting System (ATS) to review in bound cargo and identify potentially high risk shipments. ATS is utilized by CBP officers at U.S. ports of entry as well as the National Targeting Center—Cargo and at various ports around the world under the auspices of the Container Security Initiative (CSI). Under CSI, bills of lading are reviewed at overseas ports and any potential high risk shipments are examined overseas prior to lading aboard U.S. bound vessels. In FY 2009, CSI officers reviewed over nine million bills of lading and conducted approximately 57,000 examinations of high risk cargo while over 80 percent of all U.S. bound cargo is currently screened at a CSI port prior to lading aboard U.S. bound vessels.

Additionally, CBP is engaged with the trade community through the Customs Trade Partnership Against Terrorism (C-TPAT), another key component in the layered approach to security. Through C-TPAT, CBP works with the various components of the trade (carriers, importers, manufacturers, etc.) to ensure the safety and security of their cargo as well as to ensure a robust security process is in place as goods move through the supply chain. This allows CBP to facilitate legitimate trade while focusing resources on those components and entities which may pose a threat to maritime cargo.

In addition to targeting tools and methodologies and working with the trade community, CBP has deployed or installed an array of Non-Intrusive Inspection (NII) technology such as x-ray or gamma ray equipment (both mobile and fixed site) and radiation detection equipment. Such NII is deployed or installed at U.S. ports of entry as well as the 58 ports around the world which are designated as CSI ports. The use of such equipment allows CBP to quickly and effectively examine potentially high risk cargo at various points along the supply chain, either prior to lading in a foreign location or upon arrival at U.S. ports of entry.

CBP is also working with foreign governments and through organizations such as the World Customs Organization to promote enhanced standards for supply chain security globally. Our capacity building efforts include partnerships with other nations to improve the effectiveness and professionalism of customs administrations world-wide. Such activities allow CBP to foster relationships that increase the likelihood that threats to the global supply chain in general and the U.S. in particular will be discovered and addressed.

Question 2. I was concerned to see the FY11 President's Budget decreased funding for Coast Guard's overall budget and eliminated five Maritime Safety and Security Teams (MSSTs), including the San Francisco based team. The San Francisco Bay Area has many critical infrastructure and tourist assets, including several bridges such as the Golden Gate Bridge and Bay Bridge, and two ports—the Port of Oakland and the Port of San Francisco. Can you assure the people of the Bay Area that the elimination of the MSST will not place the Bay Area at risk?

Answer. Yes. Coast Guard Sectors continue to be the backbone of Coast Guard security efforts in a port, including the Port of Oakland and the Port of San Francisco. Marine Safety and Security Teams (MSSTs) are deployable specialized forces that are not dedicated to a specific port, and routinely deploy in support of a designated national security event or in response to a natural disaster. When not deployed, MSSTs do augment local forces by conducting some operational activities under Operation Neptune Shield (ONS), such as escorts of high capacity passenger vessels. However, MSSTs perform a relatively small percentage of the high interest vessel security boardings in their respective homeports.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
ADMIRAL ROBERT J. PAPP

Question 1. Thank you for your response to my question regarding the detection of semi-submersibles and submersibles vessels used in drug smuggling. As a follow-up question, are the challenges of detecting and interdicting semi-submersible and submersible vessels of the type used in drug smuggling being addressed in the Department's Small Vessel Security Strategy with respect to port security?

Answer. Yes. Objective 1 of Goal B of the Department of Homeland Security's Small Vessel Security Strategy is to "Improve detection and tracking capabilities to better identify small vessels operating in or near U.S. waters."

Question 2. The Port Security Grant Program has played a vital role in funding key security projects to help detect and prevent terrorist attacks. It is my understanding that FEMA has indicated that it is interested in funding projects under the program that address maritime resiliency and business continuity but is seeking Coast Guard endorsement before adding the relevant language to the grant guidance material. What are your thoughts about making maritime resiliency and business continuity projects eligible under the Port Security Grant Program?

Answer. Federal Emergency Management Agency (FEMA) is the grant administrator of the Port Security Grant Program. The Coast Guard assists FEMA by providing subject matter expertise on maritime security issues. Since 2007, FEMA policy has required Port Wide Risk Management/Mitigation and Business Continuity/Resumption of Trade Plans for Group I and Group II port areas. These documents represent a five-year plan that supports each port's Area Maritime Security Plan and lays out a strategy and series of actions that must be undertaken to address the prevention of, protection against, response to, and recovery from major security incidents. The Coast Guard, in close collaboration with maritime industry through Area Maritime Security Committees, has assisted FEMA in developing these plans with the goal of closing maritime security risk vulnerability gaps.

Question 3. It is my understanding that current law and regulation allow an individual to be escorted to their job while they are waiting to receive their TWIC card. However, longshoremen tell me that "escorting" is not occurring in the state of Washington. Workers who file waivers or appeals wait months for their cases to be adjudicated. As a result, some workers are unable to financially support themselves through the process.

a. Are there actions the Coast Guard can take today to improve the TWIC escort process?

b. Going forward, do you believe the Coast Guard should take a more pro-active role in formulating escort policies and procedures with waterfront employers so that workers and their families will be able to support themselves while waiting on their TWIC card?

Answer. Throughout the implementation of the Transportation Worker Identity Credential (TWIC) program, the Coast Guard has been pro-active in formulating TWIC escort policies and procedures. Specifically, the Coast Guard provided the following TWIC escort related documents to industry (available at: <https://homeport.uscg.mil/TWIC>):

- Navigation and Inspection Circular 03-07 "Guidance for the Implementation of the TWIC Program in the Maritime Sector;"
- TWIC Program: Small Entity Guide of Applicants;
- TWIC Program: Small Entity Guide for Owners and Operators; and
- Five TWIC/Maritime Transportation Security Act (MTSA) Policy Advisory Council (PAC) Decisions related to escorting (PAC 02-07, 02-08, 03-08, 02-09, 03-09)

The TWIC Program aims to enhance security by requiring that all personnel needing unescorted access to secure areas of MTSA regulated facilities and vessels and all mariners holding Coast Guard issued credentials have passed a Security Threat Assessment.

A facility owner/operator is responsible for informing workers, including longshoremen, whether they will need a TWIC to perform their job (*i.e.*, whether they will need unescorted access to secure areas at that facility). If a longshoreman needs access to a secure area of a facility, but does not have a TWIC, the facility owner/operator has the authority to provide an escort. The Coast Guard guidance to the maritime industry provides facility operators with options to meet escort requirements; however, the TWIC escort provisions are not intended to be used in lieu of the TWIC for workers requiring frequent access to MTSA regulated facilities and vessels. Therefore, the facility operator may choose to not provide escorting procedures for these workers and thereby limit their access.

Question 4. Both the Puget Sound Area and the San Diego Harbor Area were chosen for the Department of Energy Domestic Nuclear Detection Office (DNDO) pilots focused on Small Vessel threats. The pilots, which included participation by the Coast Guard and Pacific Northwest National Laboratories, have provided an opportunity for state and local authorities in Puget Sound to better understand its current prevention and detection capabilities and limitations.

a. From the Coast Guard's perspective what are the most important lessons learned from the two pilot projects?

b. Based on the results of the pilots, would you recommend that DNDO conduct additional pilots or turn the pilot into a program?

Answer. The West Coast Maritime Preventive Radiological/Nuclear Detection (PRND) Pilot Project was a Department of Homeland Security/Domestic Nuclear Detection Office (DNDO)-sponsored effort in full partnership with the Coast Guard. Department of Energy's (DOE) Pacific Northwest Laboratory (PNNL) supported the Puget Sound Pilot while DOE's Lawrence Livermore National Laboratory (LLNL) supported the San Diego Pilot. In addition to the Coast Guard and DNDO, other Federal, State, Local and Tribal Law Enforcement agencies were full participants.

Lessons Learned—The most important lessons learned from the two pilots include:

A radiological/nuclear Subject Matter Expert serving as an advisor to the Command Staff is a critical factor in overall program success.

The pilots and the resultant Full-Scale Exercises reaffirmed the necessity for comprehensive planning and coordination.

Standardized Equipment and training are essential and are critical factors for implementing a successful program. The need for standardized communications systems and their effective use are critical factors in overall program success.

In response to question b., the capability demonstrated in the West Coast Maritime Pilot should be implemented in other port regions. However, the mechanisms for implementation will require continuing consideration.

Question 5. There are still identified security issues at foreign ports that, at worst, threaten our national security, and at best, slow our ability to receive cargo. When Senator Snowe and I introduced our amendment to the SAFE PORTS Act, the Coast Guard was then inspecting select foreign ports at a rate of once every 4 to 5 years.

a. What inspection rate does the current level of Coast Guard resources afford with respect to number of foreign ports covered and frequency of inspections? Are these resource allocation decisions risk-based?

b. Does the proposed FY 2011 budget allow for increasing inspection rates to once every 2 years, as originally designed in my amendment?

c. I believe the security of our homeland is improved when we are able to extend our security borders as far out as possible. I view the inspection of foreign posts as part of a layered approach to homeland security. Do you believe the Coast Guard requires additional resources in order to carry out its foreign port inspection mission?

Answer.

- The Coast Guard generally conducts assessments on a 2-year cycle attempting to visit approximately 70+ countries each year. A small number of country assessments go beyond the 2-year cycle mostly because the country's Designated Authority requested to reschedule or delay the visit.
- Resource allocation for foreign port inspections are based on a risk methodology that considers threat, a country's internal stability, and volume of trade.
- The Proposed FY 2011 budget does allow for an inspection rate of once every 2 years.
- The Coast Guard is currently able to perform our foreign port inspections.
- Those inspections depend on the consent of foreign governments and in some cases, there has been increasing difficulty in gaining access, despite reciprocal visits being offered.
- Coast Guard capacity building assistance, while limited, is often requested by countries to assist in enhancing their port security.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KAY BAILEY HUTCHISON TO ADMIRAL ROBERT J. PAPP

Question 1. Various ports across the Nation have indicated that the port security grant process is confusing, and that the distribution of funds is very slow, with FEMA and the USCG still working on delivering funds from 2007. What percentage of the Port Security Grant funds has not been distributed, and why?

Answer. Please see Table 1. 39 percent of total PSGP funding is currently available for grantees to draw down. This percentage has increased significantly from only 5 months ago when it was 21 percent. The expedited release of PSGP funds is a priority and the rate at which these funds become available is expected to increase significantly. Of note, although FEMA has released 39 percent of funding, grantees have only drawn down 7.4 percent of available funds. FEMA does not have the authority to mandate when grantees draw down funds.

Table 1.—Port Security Grant Program (PSGP) FY 2007 through FY 2009 Funding, Obligation, and Availability Summary, Including ARRA Funding for FY 2009

Fiscal Year	Amount Appropriated (Source: GD&A)	Amount Allocated (Source: GD&A)	Obligation (Source: IFMIS)	Current Holds (Source: PARS)	Available Funds (Source: PARS)	Award Balance (Source: IFMIS)	Draw Downs (Source: IFMIS)
2007	\$320,000,000	\$311,170,000	\$310,429,718	\$51,793,028	\$258,636,690	\$239,476,664	\$70,953,054
2008	\$400,000,000	\$388,600,000	\$387,999,310	\$301,769,730	\$86,229,580	\$377,910,595	\$10,088,715
2009	\$400,000,000	\$388,600,000	\$388,353,557	\$347,167,061	\$41,186,496	\$386,745,388	\$1,608,169
ARRA	\$150,000,000	\$150,000,000	\$150,000,000	\$57,943,799	\$92,056,201	\$141,525,804	\$8,474,196
Total		\$1,238,370,000	\$1,236,782,585	\$758,673,618	\$478,108,967	\$1,145,658,451	\$91,124,134

Total Available Funds as a Percentage of Obligation Amount: 39 percent
Total Draw Downs as a Percentage of Obligation Amount: 7.37 percent

Additionally, some grantees have expressed concern about the grantees' ability to meet the legislated cost share requirement for FY 2007 through FY 2009 (FY 2009 ARRA and FY 2010 PSGP cost share requirements were congressionally waived). Uncertainty about the cost share requirement resulted in a degree of hesitancy by grantees to expend funds and has led to some significant delays in commencing approved projects. To help alleviate this concern, FEMA issued Information Bulletin (IB) No. 322 to provide grantees with an understanding of what a cost share waiver is and how to request one. If a grantee requests a cost share waiver, the FEMA Program Analyst assigned to that award works closely with the authorized representative of the award to ensure that the request meets all criteria outlined in the IB and that all appropriate information is provided to allow the Secretary of Homeland Security to make an informed decision to approve or deny the request.

The reasons for delays in releasing funding are provided in the response to the following question.

Question 2. How can the distribution of grant funds be accelerated?

Answer. Since Fiscal Year (FY) 2007, the Department of Homeland Security (DHS) has awarded over \$1.2 billion in Port Security Grant Program (PSGP) funding. Of this amount, approximately \$91 million has been drawn down by recipients through FEMA's electronic Payment and Reporting System (PARS). This equates to approximately 7.4 percent of the total awarded funds drawn down by recipients. Although this is a relatively low percentage, drawdown figures should not be the sole gauge of a program's progress.

The release of PSGP grant funds can take several months or even years to complete due to numerous mandatory grant administration processes that must be met prior to a grantee spending grant funds. Many of these requirements are statutorily required. Often, due to the nature of their projects, these requirements have the greatest impact on the larger, higher risk port areas. These are also the port areas which receive the majority of PSGP funds. These processes include: development of a Concept of Operations (CONOPS) and a Port-Wide Risk Management Plan (PWRMP) for each port area; local and national review of proposed projects; creation, review and approval of award documents; review of project budget submissions, and compliance with a number of environmental and historic preservation laws which requires reviews of Environmental and Historic Preservation (EHP) impacts of approved projects.

Further, in FY 2007 and FY 2009 the PSGP received additional appropriations, essentially creating two rounds of grants for these years. The double appropriations doubled FEMA's workload.

Over the past several years, the combination of time consuming procedural and process requirements, increased workload, and other factors have contributed to delays in the release of PSGP funds.

The requirement for Group 1 and 2 port areas (*i.e.*, largest ports with significant grant awards) to develop a CONOPS and PWRMP was issued by FEMA with the FY 2007 Supplemental PSGP grants guidance. These deliverables can take 12–18 months to complete and grant funds may be used in their development (without any cost-share requirement). Development and approval of a typical PWRMP requires completion of a comprehensive vulnerability assessment for the port and identification of port area priorities by the Area Maritime Security Committee (AMSC) and the USCG Captain of the Port (COTP). The PWRMP takes into consideration the port priorities and vulnerabilities, existing resources and capabilities, and available funding options to produce a 5-year spend plan outlining how the anticipated port area funds will be expended. The PWRMP is then approved by the COTP, and submitted and approved by FEMA. Plans that do not meet the established criteria are returned for modifications as needed. Now that the majority of ports have completed these deliverables the process of identifying, prioritizing, and approving PSGP

projects is significantly more objective and efficient—the time saved has been clearly evident.

Once these deliverables are approved by FEMA, the port Fiduciary Agent (FA), FEMA's grantee, submits projects for review and approval. Even before FEMA receives the projects, they are reviewed and prioritized at the field level by the local COTP and AMSC. This process has evolved since the FY 2007 Supplemental appropriation, resulting in many process improvements and additional time savings. Soon after the congressional appropriations are finalized, FEMA provides guidance and outreach in person and via national conference calls. FEMA staff explains PSGP funding constraints, programmatic requirements, and various other aspects of the program in an effort to facilitate the submission of investment justifications, budgetary documents, EHP information, as well as required reports. Based on stakeholder feedback, the guidance is updated each year. The improved guidance has made it easier for the grant applicants/awardees to meet program requirements in terms of both quality and timeliness of their submissions, which has in turn reduced the need for time consuming resubmissions. Additionally, FEMA now places greater emphasis on the input and prioritizations provided by the AMSC and COTP. Rather than second guess the expertise of the port-level reviewers, the national level review focuses primarily on verifying that proposed projects fall within program constraints. This improvement to the review process saves time by minimizing redundant project scrutiny. It also improves the objectivity of the overall review process.

FEMA continues to find ways to improve its grant administration processes to accelerate the distribution of funds. Some delays however, are beyond our control. Once FEMA releases funds (either partial by project or the entire award), the recipient is notified and may draw down against the grant through the Payment and Reporting System (PARS). Of the \$1.2 billion in PSGP funding awarded from FY 2007 to present, \$478 million or 39 percent of total funding has been released to grantees. FEMA does not control or dictate when recipients must drawdown funds. Each recipient follows their local protocols, some of which can be quite burdensome and time consuming; for example, when the project and/or allocation of funds must be reviewed and approved by state or local government officials. Funds may be drawn down anytime during the award period and up to 90 days following the end of the award period. Because each FA is on a different timetable, FEMA continually receives project submissions and must reconvene panels of subject matter experts from across DHS for their review. These panel sessions are necessary to the approval and distribution of PSGP funds.

Among the more significant changes, beginning with the FY 2010 PSGP, all FA projects submissions were due to FEMA 45 days after the application period closed. In July, FEMA reviewed all projects during a single session by a panel of subject matter experts. This approach puts all FAs on the same timetable going forward and eliminates the inefficient practice of reviewing projects on a rolling basis. Although FEMA clearly set a deadline for FY 2010 project submissions, there were still some ports that did not adhere to this deadline. Nevertheless, FEMA realized significant efficiency gains through this process improvement. For FY 2011, FEMA will require all applicants to submit projects at time of application to further reduce delays.

As mentioned with the PSGP guidance development process, FEMA routinely engages with port stakeholders to listen to concerns and suggestions for improving the program. This past fall, FEMA invited all of the PSGP FAs to Washington, DC for a two-day workshop on how to improve the efficiency of the program.

A significant concern among grantees includes the multiple disparate systems a grantee and FEMA staff must use in managing a single grant. FEMA plans to deploy a new grants management system, ND-Grants in FY 2011, with the end goal of having a single grants management system for the entire grants lifecycle. This system, in conjunction with a newly developed programmatic grant monitoring tool will provide a greater ability to document, justify, and report progress toward achieving the priorities of the PSGP.

The budget review process has also been improved. A budget detailed worksheet and instructions for its use is provided with the PSGP guidance and submitted by the grantee, either with their application or when projects are submitted. If the project(s) are approved for funding, the Grants Management Division (GMD) commences the budget review. GMD checks the budget for allowable expenditures and appropriate cost categories for funding, as well as to ensure that the submitted budget accurately reflects the awarded amount. If the award was adjusted, or if discrepancies exist within the budget, GMD contacts the grantee to request clarifications and/or revisions. There are frequent delays in grantee responsiveness, which can further slow the budget review process. If a grantee is un-responsive to numerous inquiries from GMD, GMD refers the matter to the PSGP Program Analyst for

assistance in coordinating with the grantee and gathering the required information. This process helps ensure that outstanding budget issues are resolved in a timely manner.

A similar, streamlined approach is employed for the Environmental and Historic Preservation Compliance Review (EHP). Federal EHP laws and Executive Orders (EOs) provide the basis and direction for the implementation of Federal EHP review requirements for FEMA-funded projects. These laws and EOs are aimed at protecting our Nation's water, air, coastal, wildlife, land, agricultural, historic, and cultural resources, as well as minimizing potential adverse effects to children, and low-income and minority populations. FEMA, through its EHP program, engages in a review process to ensure that FEMA-funded activities comply with those laws. The current EHP compliance review process includes a preliminary screening of all projects to identify further information that may be required to complete an EHP compliance review and determination, if any. Those projects that do not require further information to complete a review may be approved for EHP compliance at that time. If additional information is needed, grantees are notified of further data requirements. This information is necessary to support a determination of compliance with EHP laws and regulations. An EHP Screening Form and a formal submission process have been developed, and technical assistance made available, in order to assist grantees in identifying and providing the necessary information with their applications. Furthermore, FEMA has developed and finalized a Programmatic Environmental Assessment (PEA) that analyzed the EHP impacts of all projects funded by GPD. This PEA defined those project types that would not have any impact to the environment, as well as those that would require further study. For those project types defined as having no impacts, no further EHP information would be required. To date, this process has been very successful, and FEMA has received positive feedback from its stakeholders.

In summary, FEMA has made significant strides in releasing PSGP funding in a timely manner. Thanks to dedicated contract support personnel, the EHP backlog has been cleared. Additionally, it has been a priority of PSGP staff to review projects in a timely manner, release partial funds as projects are approved, and provide feedback to FAs as to status, particularly if projects are sent back requiring additional work. Finally, the majority of CONOPS and PRWMPs have been submitted and approved by FEMA, which now allows FEMA to concentrate on reviewing and approving projects.

Question 3. Is FEMA's role in financial oversight of the grants sufficient?

Answer. The financial grants management of PSGP awards is performed by FEMA's Grants Management Division (GMD), which acts as a centralized financial management and business support for all FEMA grant programs, which is comprised of several branches. The Operations Branch, comprised of trained Grants Management Specialists, performs all pre-award and award grant administration functions, and provides procedural and technical business support to award recipients. The Systems and Business Support Branch oversees development, implementation, maintenance, user support and training for the Agency's suite of grants management information systems. The Accountability, Management, and Oversight Branch develops and manages Agency-wide grant policies and operating procedures to assist Headquarters program offices and the Regions in the implementation, award, and management of FEMA grant programs. Together the GMD branches work with internal and external stakeholders to coordinate and manage the full financial grant lifecycle.

Each Grants Management Specialist (GMS) is trained to provide expert guidance and instruction for pre and post award financial grants management which includes: planning, awarding, and administration of FEMA grants and cooperative agreements. The Specialists work closely with grantees and the Program Office to provide financial grants management technical assistance and financial support with a strong concentration on providing high quality customer service to internal and external stakeholders. In order to provide continued guidance, the GMS's stay current on new grant policies, legal authority, and regulations to determine how changes will impact internal policies, procedures, and systems.

Both the Federal staff and contract support staff continually review and improve processes to ensure timely processing of pre and post award activity, while maintaining compliance with Federal laws governing financial grants management. One improvement that has largely impacted the grantees' ability to access award funds was the implementation of the Special Conditions-Release of Funds (SC-ROF) process in early FY 2009. This process was designed to accelerate the removal of Special Conditions stipulated in the award and allow grantees quicker access to draw down on grant funds. The SC-ROF process involves the expertise of the GMS's who review and approve the grantee pre-award financial budget documents for compliance with

FEMA financial reporting and fiscal integrity, while ensuring that all documents adhere to the Program Guidance, OMB Circulars, and Administrative Requirements. The success of this process is augmented by a well established coordination effort between GMD Operations staff and the Program Office to ensure full compliance with the terms and conditions of the award and financial reporting.

The extensive knowledge of financial grants management and combined experience of Federal staff, rooted in a dynamic environment that promotes openness for collaboration, pushes GMD forward to continue providing quality cradle-to-grave grant management service to internal and external stakeholders.

Question 4. Would the ports be better served if the Coast Guard handled distribution of grant funding?

Answer. FEMA is the grant administrator of the Port Security Grant Program (PSGP), and the Coast Guard assists FEMA by providing subject matter expertise on maritime security risk mitigation issues. The ports are best served by this collaborative relationship, whereby FEMA leverages its expertise in grant administration and financial management, and the Coast Guard leverages its expertise in maritime security. Further, the Coast Guard does not have the experience to function as the grant administrator of the PSGP. As a regulator of the maritime industry, it may also be considered a conflict of interest for the Coast Guard to serve as the grant administrator and would further complicate its coordination and facilitation role with maritime stakeholders.

Additionally, FEMA is now better staffed to manage the increased PSGP workload. In FY07, PSGP comprised of a staff of one Acting Section Chief and three program analysts, which was a significant strain at that time. Over the past year the staff has been expanded to include two full time Section Chiefs and eight program analysts. A contract support team is also available to provide surge support under direct Federal supervision as needed.

Question 5. The Coast Guard is responsible for securing 361 ports and 95,000 miles of coastline and navigable waterways. It also has 10 other missions, including maritime drug interdiction, search and rescue, immigration law enforcement at sea, and serving as the lead Federal agency responding to the *Deepwater Horizon* oil spill, and all of this with only 42,000 Active Duty personnel. Is the Coast Guard adequately staffed to secure our ports and fulfill all of its other responsibilities?

Answer. The Coast Guard's systematic, maritime governance model for port security consists of maritime security regimes, domain awareness, and maritime security and response operations and is a layered security approach that shares responsibilities with partners to provide a credible deterrence (while employing risk-informed decisionmaking).

Regarding general maritime security activities (escorts, patrols, and boardings), the Coast Guard's guidance to field commanders, Operation NEPTUNE SHIELD, prioritizes these activities based on risk and the availability of resources. Higher risk, higher consequence activities are provided with more attention and consideration than lower risk and consequence activities.

In responding to a maritime security threat, the Coast Guard employs threat-based, risk-managed principles, matching protective/preventative efforts to the threat's nature, *i.e.*, attack method, target, etc. By using these principles, the Coast Guard implements Maritime Security (MARSEC) level increases that are focused on a single or few Sectors or, if nationwide, only on the targeted type of maritime critical infrastructure and key resources (*e.g.*, maritime mass transit—ferries or vessels carrying Certain Dangerous Cargoes). The Coast Guard approaches its risk-informed decision-making methodology through the use of the Maritime Security Risk Analysis Model and has been used to prioritize security activities as well as validate applications for the Port Security Grant Program. The Coast Guard leverages the support of other government agencies and ensures that maritime industry stakeholders have increased their security efforts in accordance with their Coast Guard-approved facility and vessel security plans. Coast Guard Sector Commanders carrying out the operational security measures dictated by increased MARSEC levels may request additional resources, *i.e.*, deployable specialized forces, from the Deployable Operations Group via their Area Commander.

Maritime security and response operations as well as Maritime Transportation Security Act and the implementing regulations are not static efforts and should and will be modified to meet emerging threats and/or further reduce vulnerabilities as we refine risk mitigation strategies.

Question 6. Since the terrorist attacks of September 11, 2001, maritime security efforts have focused primarily on large commercial vessels, cargoes, and crew. Efforts to address the small vessel environment have largely been limited to traditional safety and basic law enforcement concerns. Small vessels are, however, read-

ily available for potential exploitation by terrorists, smugglers of weapons of mass destruction (WMDs), narcotics, aliens, and other contraband, and other criminals. Small vessels have also been successfully employed overseas by terrorists to deliver Waterborne Improvised Explosive Devices (WBIEDs).

What efforts is the Coast Guard making to address security threats posed by small vessels?

What is the Coast Guard doing to develop and leverage partnerships with recreational boaters and professional mariners who operate small vessels to increase awareness about security threats posed by smaller vessels?

Answer. Small vessels generally operate with great autonomy. The Department of Homeland Security (DHS) and the Coast Guard have taken numerous steps to address possible risks associated with small vessels while also recognizing the importance of preserving the traditional freedoms enjoyed by the boating public.

As described in our response to Question 12, numerous programs and activities supporting the SVS Strategy are already being implemented or have been completed, including:

- Maritime Domain Awareness initiatives:
 - America's Waterways Watch;
 - Citizens' Action Network;
 - Automatic Identification System (AIS) carriage requirements; and
 - Robust intelligence gathering and analysis, including Field Intelligence Support Teams at each Coast Guard Sector.
- Security Regimes:
 - Area Maritime Security Plans (AMSP), which conform to the Maritime Transportation Security Act (MTSA), include actions to mitigate small vessel attacks;
 - Coast Guard approved security plans are required for MTSA regulated vessels and facilities; and
 - Coast Guard Captains of the Port (COTPs) possess broad authorities to control port access, movement, and activity.
- Maritime Security and Response Operations:
 - The Coast Guard utilizes a tiered risk-based system, which aligns with and supports DHS' Homeland Security Advisory System.
 - A diverse set of operational activities, including:
 - Waterborne, airborne, and shoreside patrols and visits to critical infrastructure; and
 - Security boardings of small vessels.
- Vessel escorts of:
 - High Value military ships;
 - Vessels carrying high consequence cargoes; and
 - High capacity passenger vessels (*e.g.*, cruise ships, ferries).

The Coast Guard's numerous measures, together with port partner efforts, provide layered security against small vessel and other security risks in the maritime domain. Where appropriate, many of these measures include partnerships with recreational boaters and professional mariners who operate small vessels, such as America's Waterways Watch and Citizens' Action Network. DHS and the Coast Guard will continue to work hand in hand with industry and the public to ensure they are part of the solution.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. DAVID VITTER TO
ADMIRAL ROBERT J. PAPP

Question. The SAFE Port Act required the Coast Guard, within 180 days, to "update and finalize the rulemaking on notice of arrival for foreign vessels on the Outer Continental Shelf" (sec. 109 of P.L. 109-347). As I understand it, nothing has happened regarding this matter since the notice of proposed rulemaking was issued on June 22, 2009. Please explain how you will ensure that this requirement from the bill is completed.

Answer. The SAFE Port Act (Section 109) requires the promulgation of regulations detailing notice of arrival (NOA) procedures for foreign vessels planning to en-

gage in Outer Continental Shelf (OCS) activities. The Coast Guard published the NOA on the OCS notice of proposed rulemaking on June 22, 2009. The Coast Guard proposes to enhance maritime domain safety and security awareness on units and personnel engaging in activities on the Outer Continental Shelf by regulations which will require notice of arrival for units planning to engage in Outer Continental Shelf activities. The proposed rules would implement provisions of the Security and Accountability for Every Port Act of 2006 and increase overall maritime domain awareness by requiring owners or operators of United States and foreign flag floating facilities, mobile offshore drilling units, and vessels to submit notice of arrival information to the National Vessel Movement Center prior to engaging in Outer Continental Shelf activities.

The Coast Guard received and reviewed two detailed sets of comments and recommendations from trade associations (the International Association of Drilling Contractors and the Offshore Marine Service Association) in response to the NPRM. These comments are part of the public record and are being considered in the process of drafting a final rule.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV
TO HON. ALAN BERSIN

Question 1. Will the 100 percent scanning requirement apply to cargo containers destined for Canada and Mexico ports which are subsequently transhipped by truck and rail to the United States?

Answer. Section 232 of the SAFE Port Act, as amended, requires 100 percent scanning of containers at all foreign ports that ultimately ship containers to the U.S. A container is considered U.S.-bound if it is destined to a U.S. port. If the destination is Canada or Mexico, then it is not considered U.S.-bound, therefore not subjected to the 100 percent scanning mandate. Those containers that are unladed in Canada and Mexico and subsequently shipped to the U.S. via rail or truck are screened, targeted and if necessary examined at the U.S. ports of entry.

Question 2. Do you believe that we should look to assessing a port security user fee to help manage the growing cost associated with port security? We have seen a similar fee in the aviation context to defray the enormous costs associated with security. Should the cargo and shipping industries along with other users be required to pay a similar fee?

Answer. The significant cost and scope of work that benefits the facilitation of legitimate trade would certainly warrant additional research to determine if a fee structure could be created to defray some or all of the costs associated with port security. Determining which port security-related activities should give rise to fees is a prerequisite to the development of a fee structure. Currently, there are user fees that exist to support some of these activities. To move forward, U.S. Customs and Border Protection (CBP) would need to identify which port security-related activities do not currently receive fee funding and which activities CBP should seek to receive reimbursement, and determine whether the complete fee structure should be reworked or if it is sufficient to impose additional fees for services that are not covered by the existing fee structure.

Question 3. On December 2 of last year, Secretary Napolitano said that prohibitive challenges would require DHS to seek more time in the implementation of the 100 percent scanning mandate. S. 3639 extends the deadline to 2015 and clarifies the requirement to include either RPM or NII scanning. Do you support this approach?

Answer. CBP recognizes that 100 percent scanning may play a role in certain trade corridors where the scan data can provide additional information to improve the security of that particular supply chain but believes a risk-based approach should also be considered. CBP understands the need to proceed with future deployments in a responsible, fiscally sound manner that best achieves the goal of maximizing the security of U.S. bound maritime cargo while maintaining an effective risk-based strategy. CBP is currently identifying multiple options, including the resources needed to implement these options, that would scan 100 percent of all cargo prior to departure from a foreign port.

CBP notes however that the requirement to scan all cargo at foreign ports presents challenges in that some foreign governments view the requirement as extraterritorial and an affront to their sovereignty. They have indicated the likelihood of instituting reciprocal requirements for U.S. exports to their countries. Even countries that are cooperative are concerned about the feasibility on the basis of port efficiency, logistical limitations, and associated costs of implementation and operation.

Question 4. What is causing the delay for issuing technical standards for foreign-inspection equipment?

Answer. U.S. Customs and Border Protection (CBP) does not “issue” technical standards to foreign governments, so there is no delay. All equipment currently utilized in foreign environments under the Secure Freight Initiative (SFI) is CBP owned and thus meets current CBP minimum standards when initially deployed.

Should foreign governments pursue the purchase of their own equipment for a port under the Container Security Initiative (CSI), and information is requested during negotiations, CBP may provide the foreign government or equipment companies with current technical specifications that meet CBP minimum standards, ensuring compliance with CBP standards for participation in a CBP program. These standards are normally open source and accepted by the World Customs Organization and the international community. CSI keeps an inventory and matrix of all NII equipment that is utilized in CSI ports. Some of the NII equipment is owned by CBP or was previously owned by CBP and thus meets CBP standards. CBP cannot dictate to foreign governments from which vendors they must purchase equipment, but much of the foreign owned equipment is from the same vendors CBP purchases equipment and therefore meets CBP standards. Other foreign owned equipment meets or exceeds the penetration levels of CBP equipment. Also, CBP Officers are present during the examination of containers selected by CSI Officers and review the NII image for anomalies.

CBP’s mission to combat terrorism and facilitate legitimate trade relies on many types of technology, used in combination, to promote a layered enforcement strategy. An example of CBPs layered enforcement strategy includes the scanning of sea-cargo containers at foreign seaports under SFI. Section 232(b)(1) of the SAFE Port Act, as amended by the Implementing Recommendations of the 9/11 Commission Act, states, “A container that was loaded on a vessel in a foreign port shall not enter the United States (either directly or via a foreign port) unless the container was scanned by non-intrusive equipment and radiation detection equipment at a foreign port before it was loaded on a vessel.”

Through the Office of Information and Technology, CBP has developed standards for both non-intrusive inspection (NII) equipment and radiation portal monitors (RPM) used for scanning containers in the sea-cargo environment. Although there is a varying degree of industry sophistication in commercial-off-the-shelf NII equipment and RPM technology, the technical requirements listed in this document provide a guideline for a complete scanning system that combines NII equipment, RPMs and optical character recognition (OCR) technology into one integrated system. This integrated system would have a very small footprint and would be easily deployed, in a “turn-key” delivery, to any seaport environment in the world. The specifications listed should be used as minimum standards and are not all inclusive.

NII equipment technical specifications:

- System should have a minimum footprint and easily integrate with RPMs and OCR technology.
- Penetration of a minimum of 300 mm of steel.
- Minimum source strength not less than 6 MeV.
- Have low dose rate emissions per inspection.
- Capability to scan 20–53 foot chassis-mounted sea containers in a drive through capacity.
- System should scan a minimum 85 containers per hour and preferably up to 150 containers per hour.
- System should be able to transmit images to a designated location in the United States via the N–25 format (N–25 baseline version 1.4) and be N–25 compliant.
- Operate as an automated drive-through system.
- Must be integrated with redundant safety features.
- Must provide for radiation safety of operators, workers, stevedores and bystanders while maintaining a minimum footprint.
- Ability to operate effectively in extreme temperatures and accommodate world-wide deployment conditions.
- Ability to operate on universally accepted power standards.
- Must be compliant with all country deployed safety and certification requirements.
- Resolution requirements shall be .125 inches, preferred, but not less than .5 inches.

- Workstation and Interface System to include an Operator Console and all operating systems, software, cameras, controls and displays to depict a video and radiographic image of the target.
- Capable of capturing and displaying the radiographic and visible spectrum (video) images of the target to the Operator simultaneously.

RPM equipment technical specifications:

- System should have a minimum footprint and easily integrate with NII and OCR technology.
- RPMs should be able to detect gamma and neutron radiation using plastic scintillator (gross gamma counting) and helium three tube neutron detectors.
- Scintillator panels and neutron detectors should be mounted vertically.
- RPMs should at a minimum meet American National Standards Institute (ANSI), International Atomic Energy Agency (IAEA) and U.S. Department of Energy standards on detecting radiological material and shielded and un-shielded special nuclear material (SNM).
- RPMs should be able to detect heavily shielded SNM with a very low false alarm rate.
- RPM installations should be sensitive and capable of detecting radioactive material at a range of heights to intercept illicit material hidden in a multitude of cargo types, with detectors deployed on both sides of a monitored lane.
- System should be able to transmit RPM data to a designated location in the United States via the N-25 format (N-25 baseline version 1.4) and be N-25 complaint.
- RPM systems should consist of radiation sensor panels with presence sensors, stands, control units, annunciators (as needed), cameras/license plate readers (as needed) and alarm station displays.
- Ability to operate effectively in extreme temperatures and accommodate world-wide deployment conditions.
- Ability to operate on universally accepted power standards.
- Must be compliant with all country deployed safety and certifications requirements.
- Workstation and Interface System to include an Operator Console and all operating systems, software, cameras, controls and displays to depict a video and radiographic image of the target.

OCR equipment technical specifications:

- System should have a minimum footprint and easily integrate with NII and RPM technology.
- OCR component must automatically identify a sea-cargo container number (to include two TEU units on one chassis) as they are scanned.
- OCR technology must have a very low false alarm rate.

RPM, NII and OCR data should be integrated in near “real-time” so that personnel can quickly view images and adjudicate any radiological alarms. All technology should also integrate easily, via the N-25 format, with CBP systems. The Operator Console System should be deployed in a central alarm station that includes all operator work stations, servers, etc., and must have the capability to send data to a multitude of locations, to include transmission of scanning images/radiation spectra, from a foreign location to the United States. Additionally, all equipment must be installed so that it is easily accessible for maintenance and calibration.

System acquisition should provide operator training, on all equipment, in the English language with the potential for foreign language training. System acquisition should provide on-site maintenance, to include the potential for 24/7 on-site maintenance technicians. All proposals should also include “over height sensors,” signage, drop bars and any other safety equipment as deemed necessary by CBP.

As CBP moves forward with the deployment of technology and as the number of manufactures, models and designs continue to increase, CBP will work in a steadfast manner to ensure equipment performs to needed specifications. Additionally, as new technology develops and improves, CBP will work with both vendors and the scientific community to ensure that the most efficient, effective and state-of-art equipment is utilized, acquired and deployed.

Question 5. With the Secure Freight Initiative (SFI) and requirement for 100 percent scanning of U.S.-bound cargo containers, the U.S. security strategy may become

more dependent upon foreign governments to scan cargo containers. Containers scanned by foreign governments are not generally scanned again when they arrive in the United States. Does CBP systematically review or examine the inspections practices or training of host government customs services that conduct inspections of high risk U.S. bound containers?

Answer. No. However, U.S. Customs and Border Protection (CBP) has conducted targeting and interdiction training for a number of foreign Customs administrations. Further, in Container Security Initiative (CSI) ports where CBP staff is present, CBP officers participate in and witness the inspections of high-risk U.S. bound containers that are conducted by host government personnel and may request further inspection.

Question 6. What strategies does CBP employ to ensure foreign customs officials are sufficiently trained and that the cargo inspections are performed in accordance with U.S. standards?

Answer. CBP does not systematically review training of host government customs services that conduct inspection of high-risk U.S.-bound containers. However, CBP has conducted targeting and interdiction training for a number of foreign Customs administrations. In CSI ports where CBP staff are present, CBP officers participate in and witness the inspections of high-risk U.S. bound containers that are conducted by host government personnel and may request further inspection (*i.e.*, a physical exam of the container's contents) if necessary. In the port of Qasim, Pakistan, no CBP personnel are on the ground. However, Vetted Foreign Service Nationals perform the inspections and transmit the data to the National Targeting Center-Cargo (NTC-C) for further review and scrutiny in real time. In this situation, the CBP officers at the NTC-C make the final decision to release the container or request further examination.

Question 7. CBP officials responsible for managing the CSI program have reported that overall there has been a high level of cooperation at CSI seaports, though they acknowledged that the degree of involvement and participation that CBP officers have with foreign customs officials during the examination of high-risk cargo varies by country. How often do CBP personnel participate in or witness inspections of high-risk cargo bound for the United States at these foreign seaports?

Answer. CBP personnel regularly participate in and witness inspections of high-risk cargo at all CSI foreign ports with the exception of the two Container Security Initiative (CSI) ports in Mainland China.

Question 8. Are there any countries that restrict CSI teams from participating or viewing examinations of high-risk cargo?

Answer. Yes, the two CSI ports in Mainland China.

Question 9. CBP officials at the National Targeting Center: (1) assist the CSI teams at high-volume seaports to ensure all containers that pass through CSI seaports are targeted to identify high-risk container cargo; (2) carry out targeting responsibilities for CSI seaports that do not have CBP officials stationed there; and (3) conduct targeting for U.S.-bound container cargo that does not pass through CSI seaports using advance information (24-hour rule and 10+2) to identify high-risk container cargo. What are the advantages and disadvantages of conducting targeting from the United States versus targeting at CSI seaports?

Answer. The advantages of targeting at overseas Container Security Initiative (CSI) seaports are control, immediate access to the containers before they are laden on the vessels, and access to local host country intelligence in regards to trade entities. The primary disadvantage of targeting at overseas CSI seaports is the significant cost of staffing, data transmission and equipment. Conversely, targeting from the U.S. would allow for a lower cost of staffing, data transmission, and equipment. Targeting from the National Targeting Center-Cargo (NTC-C) also brings with it capabilities to receive highly classified intelligence, and close interaction with a multitude of other Federal agencies.

When CSI was first launched in 2002, the most practical and advantageous method of execution was to provide staffing to physically target cargo at the foreign CSI seaport locations. During that time, the relationships and reciprocal agreements with the host countries were in the development stage. Over the past 8 years, the program has evolved and matured to include global cooperation and the development of measures which improve shipping security for the U.S. and its partners. The nurturing of host government relationships along with the combined assets of CSI NTC-C and its hosts provides CSI a comprehensive network of intelligence to draw upon to in order evaluate manifest data. These factors may now tip the balance in favor of performing more of the targeting functions from the U.S. while maintaining a minimum staffing of U.S. Customs and Border Protection (CBP) Officers at the CSI ports to witness exams and collaborate with host nation officials.

Question 10. In DHS's Congressional Budget Justification FY 2011, CBP requested a \$50 million decrease for the CSI program shift CSI personnel currently stationed overseas, at the CSI ports, back to the U.S. at the National Targeting Center. What security impacts do you anticipate from transitioning personnel back to the United States?

Answer. While shifting some of the officers overseas to the National Targeting Center (NTC), U.S. Customs and Border Protection (CBP) would look to station a minimum number of officers in Container Security Initiative (CSI) ports overseas to continue to foster relationships and information sharing with host counterparts and to witness inspections. With this proposal, there would not be a significant impact on security.

When CSI was first launched in 2002, the most practical and advantageous method of execution was to provide staffing to physically target cargo at the foreign CSI seaport locations. During that time, the relationships and reciprocal agreements with the host countries were in the development stage. Over the past 8 years, the program has evolved and matured to include global cooperation and the development of measures which improve shipping security for the U.S. and its partners. The nurturing of host government relationships along with the combined assets of CSI, National Targeting Center-Cargo (NTC-C) and its hosts provides CSI a comprehensive network of intelligence to draw on in order evaluate manifest data. These factors may now tip the balance in favor of performing more of the targeting functions from the U.S. while maintaining a minimum staffing of CBP Officers at the CSI ports to witness exams and collaborate with host nation officials.

Question 11. Many of our imports come from China—which in the past did not allow CBP officials into the country to validate C-TPAT members' supply chains. During 2007, CBP undertook a pilot project to use third party contractors to validate the supply chain security of U.S. importers in China. In that pilot, only 14 of 307 eligible C-TPAT members had indicated an interest in using a third party to validate their security practices and only 1 had actually been validated. Why were C-TPAT members importing from China willing to forego the added benefits of validation as a Tier 2 or Tier 3 participant rather than submit to validation by a third party? Why did so few of the eligible C-TPAT members agree to cooperate in the pilot and what would be necessary to gain their support?

Answer. There are several possible explanations for the low number of volunteers participating in the project. First, in accordance with the SAFE Port Act the member was required to incur the cost associated with the third party validator. Second, members were concerned about sharing proprietary information with the third party entities. Finally, invited companies may have decided to see how the CBP—China Customs joint validation initiative progresses before incurring the cost associated with a third party validation. Engaging the services of a third party is an individual company decision which is based upon a cost/benefit comparison.

Question 12. CBP does not directly test C-TPAT members' security practices, but generally discusses security with officials, observes physical security, and reviews policies and procedures to validate members' security practices. Additionally, CBP has yet to identify outcome based performance measures to indicate C-TPAT's effectiveness at enhancing supply chain security. Absent direct testing and outcome based performance measures, what information is available to support that the C-TPAT program has enhanced the security of the international supply chain?

Answer. Custom-Trade Partnership Against Terrorism (C-TPAT) has positively impacted the security of the international supply chain through adherence to the program's security criteria and this impact is reflected in a series of performance measures. C-TPAT has developed a comprehensive validation strategy to ensure that strong security measures have been adopted by members throughout their supply chain. The member's security profile is closely reviewed by highly trained Supply Chain Security Specialist (SCSS) and subsequently subjected to rigorous on-site reviews. SCSS closely examine records such as container inspection and seal logs, personnel files, and business partner screening records. U.S. Customs and Border Protection (CBP) documents the records reviewed and all vulnerabilities including physical security deficiencies. CBP grants members 90 days to implement needed corrective actions which SCSS confirm through a variety of methods such as digital photos, invoices and physical onsite confirmation. Members which fail to implement the required enhancements are suspended from the program. C-TPAT data shows that members are on average 95 percent compliant in meeting the program's security criteria. In addition members must conduct an annual self-assessment where they are required to review, correct and/or update their previously submitted security profile. Failure to do so also results in suspension or removal from the program.

To further enhance the program's performance measures C-TPAT recently created a validation scorecard to measure how well companies are implementing supply chain security procedures. The scorecard measures how a company performed during the validation; it may also be used as a tool to show improvements or patterns of predictability over time such as potential supply chain security risks.

C-TPAT's security criteria and strong on-site validation procedures have been replicated around the world to the point that they have become the global standards for supply chain security. The governments of Canada, Jordan, Japan, South Korea, and New Zealand developed or improved their own business partnership programs to align with and be at the same level as C-TPAT. By setting and maintaining high standards, C-TPAT has in essence become the security program that foreign Customs Administrations want and need to replicate, particularly if they envision signing a Mutual Recognition arrangement with CBP.

Question 13. The 10+2 program was developed, in large part, to improve the quality of shipping information used by the ATS system to identify high risks containers. What are CBP's plans for collecting and analyzing information on how the 10+2 data are being used for targeting purposes and determining whether the data have a clear impact on CBP's ability to target high-risk containers?

Answer. The advanced data provided by the Importer Security Filing ("10+2") significantly increases the scope and accuracy of information gathered on the goods, conveyances and entities involved in the shipment of cargo to the U.S. via vessel. This additional advance data allows U.S. Customs and Border Protection (CBP) to make earlier and much better informed targeting decisions prior to cargo arrival in the U.S.

CBP continuously collects information about the frequency of the risk indicators identified in the importer security filing data set; risk indicators that may or may not have been previously identified by the manifest (bill of lading) and/or entry data sets. CBP periodically conducts structured analyses of its targeting methodology to measure its effectiveness. One aspect of that analysis is a measurement that a given data attribute predicts an outcome. Each of the targeting concepts developed from the "10+2" data will be measured using this analysis. While the "10+2" program is still in the early stages, there have been several instances which highlight the effectiveness and necessity of this new data.

For instance, real time analysis of the Imposter Security Filing (ISF) data enables CBP to identify potentially mis-manifested containers scheduled to arrive into U.S. waters by comparing the container numbers that are declared in the carriers' vessel stow plans against the containers derived from the 24 hour manifest data for the same shipments.

Based upon the "10+2" data alone, CBP Officers are now able to identify and timely mitigate any risk from potentially mis-manifested containers, while avoiding needless delays to the movement of all other cargo.

A second preliminary measure of the effectiveness of the "10+2" data is the earlier and much more precise identification of lower-risk parties involved in the supply chain. Prior to the collection of the "10+2" importer security filing data, CBP was unable to identify, with any high degree of confidence, that a party was indeed a trusted C-TPAT participant solely from the manifest data. Today, C-TPAT participants are identified immediately through their importer security filings and given their respective targeting "credit", which significantly reduces the chances of a shipment being targeted for an enforcement examination. Prior to "10+2", it was not uncommon for C-TPAT companies to undergo numerous domestic non-intrusive inspection (NII) exams due to questionable manifest data.

Lastly, CBP is able to identify and mitigate the presence of higher-risk entities earlier in the supply chain due to more precise information that is supplied as part of the "10+2" data. Over the course of the past 2 years, the Automated Targeting System (ATS) has identified hundreds of potential high-risk entities from the "10+2" data; matches that CBP would not have known about based on the manifest data alone. While an inconclusive or conclusive match is not necessarily indicative of the presence of dangerous cargo, it does allow CBP to gain valuable intelligence on the nature of the shipments being shipped or imported by these potentially terrorist-related subject matches.

Question 14. Are any of the 10+2 requirements to be used for purposes other than assessment of terrorist threat, such as detecting other illegal contraband?

Answer. The usage of the "10+2" data is not strictly limited to anti-terrorism efforts. In fact, U.S. Customs and Border Protection (CBP) targeters and analysts routinely use the "10+2" data to help identify the presence of shipments containing illegal contraband such as narcotics and other illegally smuggled goods—the same techniques used to introduce contraband into the U.S. may also be used by terrorists

to smuggle in weapons of mass effects. However, at this time, the Trade Act of 2002 and the SAFE Port Act of 2006 expressly forbid CBP from using the “10+2” data for pure trade compliance or trade enforcement purposes.

Question 15. Has CBP officially adopted a position that 10+2 will alleviate the need for 100 percent scanning?

Answer. U.S. Customs and Border Protection (CBP) has not adopted the position that 10+2 alleviates the need for 100 percent scanning.

Question 16. If so, what type of analysis was done to support this position and what reductions in what types of risk are expected as a result 10+2?

Answer. U.S. Customs and Border Protection (CBP) has not adopted the position that 10+2 alleviates the need for 100 percent scanning. However, CBP’s Importer Security Filing (ISF) initiative, also known as “10+2”, forms a critical enhancement to the advanced data component of CBP’s layered security strategy in the ocean cargo environment. The application of the advanced data from the ISF to CBP’s targeting process enhances the utility of the agency’s risk analysis exponentially. The level of detail provides greater transparency into individual transactions and the parties involved, enabling CBP’s targeters to more accurately identify high-risk and potentially problematic shipments while facilitating truly low-risk cargo. When combined with CBP’s currently deployed imaging and radiation detection technology and the expertise of our National Targeting Center and port targeters, ISF forms a cornerstone of an effective risk-based, layered security strategy.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO
HON. ALAN BERSIN

Question 1. Three years ago, Congress acted to require one hundred percent scanning of all containers coming to the U.S. However, last year the GAO found we are only scanning less than 5 percent of all U.S.-bound containers and that one hundred percent screening has not been achieved at even one port. Is the Department scanning more than 5 percent of the containers prior to arriving in the United States? If so, what is the percentage of containers that are now being scanned?

Answer. U.S. Customs and Border Protection (CBP) continues to scan less than 5 percent (collectively in Container Security Initiative (CSI) and Secure Freight Initiative (SFI) ports) of containerized maritime cargo before it is laden on a vessel bound for the U.S. CBP continues to screen 100 percent of all cargo manifests utilizing the Automated Targeting System and intelligence databases. One hundred percent of those shipments that are deemed high risk are scanned utilizing NII and radiation technology.

CBP defines scanning as examining cargo to both an x-ray image for anomalies and radiation screening for the presence of radiation. CBP defines screening as analyzing all cargo manifests utilizing the Automated Targeting System to identify high risk cargo.

Question 2. Although it was recommended the by Government Accountability Office (GAO), the Department of Homeland Security has not yet completed a feasibility or cost benefit analysis of the one hundred percent scanning requirement or any other alternative program. When will the Department conduct such an analysis so that we can determine the most effective way to move forward on container security?

Answer. U.S. Customs and Border Protection (CBP) has conducted initial research into the feasibility and cost benefit analysis of one hundred percent scanning. A complete cost of the SFI pilot ports has been documented in the bi-annual reports to Congress. CBP is currently identifying multiple options, including the resources needed to implement these options, for scanning 100 percent of all maritime cargo prior to departure from foreign ports. Once the analysis is completed, we will be pleased to provide a briefing on the results.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BARBARA BOXER TO
HON. ALAN BERSIN

Question 1. Several ports in my state have expressed concern about the 25 percent cost share for ports to participate in the Port Security Grant program because they believe it has been difficult to come up with the local match in this tough economy. Why does DHS continue to maintain a need for a cost share for the port security grant program when other Homeland Security grant programs such as the Transit Security Grant Program and the Urban Area Security Initiative (UASI) grant program do not have a required local cost share? Are you aware of ports that have had

to scale back or abandon port security projects because of the inability to come up with the local cost share due to decreased revenues in this tough economy? Do you believe this could be putting our ports at risk?

Answer. Cost-sharing is an effective way to ensure buy-in by a grant recipient, while incentivizing the recipient to leverage its own ongoing and planned investments in homeland security. The cost-share requirement is Congressionally-mandated under 46 U.S.C. § 70107(c). Although the cost-share is statutorily required, the Secretary of Homeland Security does have the statutory authority to reduce the cost-share for Port Security Grant Program (PSGP) projects in certain circumstances. The cost share requirement for FY 2009 ARRA and FY 2010 PSGP awards were congressionally waived, but the FY 2010 Homeland Security Appropriations Act conference report language (P.L. 111–83) specifically indicated that the cost share requirement for the PSGP is not expected to be waived in the future, except at the discretion of the Secretary. Some port representatives have expressed concern about the cost share requirement for FY 2007 through FY 2009 grants. Several fiduciary agents have informed us of difficulties in soliciting project proposals because sub-recipients are unable to cover the cost match in this current economic climate. However, we have no evidence to suggest that previously approved port security projects are being abandoned due to this concern.

Additionally, FEMA issued Information Bulletin (IB) No. 322 on July 15, 2009 to define the process grantees should follow to submit cost-share waiver requests for FY 2007, 2008, and 2009 PSGP grants. Such requests are evaluated on a project-by-project basis and generally not granted for an entire award. FEMA Program Analysts work closely with the authorized award representatives to ensure the request meets all criteria outlined in the IB. Each waiver request must contain a strong justification from the prime recipient, proof of written notice to the local Captain of the Port and Area Maritime Security Committee (AMSC), assurance that granting the waiver will not change the security compliance requirements the grantee is required to operate under within their approved security plan, and a revised budget. All cost-share waiver requests are considered by FEMA, USCG, and DHS leadership.

While cost-sharing is valuable in ensuring efficient and effective recipient use of Federal funding, we recognize that extenuating circumstances may arise. The cost-share waiver provision helps ensure that worthy PSGP projects continue to move forward. Thus far, all requests for waivers under this process that have been presented to the Secretary for consideration have been approved.

Question 2. I included language in the FY 2008 Omnibus Appropriations Act (P.L. 110–161) Conference Report to require the Commissioner of U.S. Customs and Border Protection (CBP) to report to Congress on the training of CBP officers assisting the FDA in monitoring the safety of our Nation’s food supply. Does CBP have enough officers at our ports to ensure the safety of our Nation’s food imports?

Answer. U.S. Customs and Border Protection (CBP) believes there are enough officers at our ports of entry to ensure the safety of our Nation’s food imports. CBP works closely with the Food and Drug Administration (FDA) to address the issue of food safety. FDA personnel are co-located at CBP’s National Targeting Center and the Commercial Targeting and Analysis Center. The FDA and CBP automated systems for prior notice and entry release are integrated, which allows both agencies to have advanced targeting in place to select potential shipments that warrant review and/or examination. At some ports of entry, but not all, FDA has personnel along side CBP to address these concerns. The partnership between CBP and FDA has streamlined and enhanced our efforts to address food safety concerns.

Question 3. What changes has CBP made since 2008 to improve the safety of our Nation’s imported food supply?

Answer. Since 2008, U.S. Customs and Border Protection (CBP) has designated “Import Safety” as a priority trade issue; an identified high risk trade area where CBP can focus our resources as part of a layered approach to risk management. These priority trade issues are commodities that can cause a significant revenue loss, economic risk to U.S. industry and/or represent health and safety concerns to citizens.

CBP has created two divisions, the Import Safety and Interagency Requirements Division and the Commercial Targeting Analysis Center both dedicated in identifying and addressing import safety concerns.

CBP has been an active participant in interagency workgroups such as the Import Safety Interagency Workgroup and President Obama’s recently announced, Food Safety Working Group. CBP is dedicated to working with the other government agencies on creating policy for CBP field resources to address import safety nationwide in a uniform manner. These work groups have been successful in multiple ini-

tatives, including but not limited to incorporating product safety in our trusted partnership programs, the establishment of other government officials at the ports of entry to interdict import safety concerns, and the possible cross laboratory training among participating agencies.

To enhance collaboration between CBP and other government agencies including FDA, the Import Safety Commercial Targeting and Analysis Center (CTAC) was established in 2009. The facility is located within CBP's Office of International Trade. The CTAC serves as a fusion center where CBP, FDA and other participating personnel are co-located at a single site, sharing targeting resources and expertise to achieve the common mission of protecting the American public. The CTAC enhances CBP and FDA's ability to streamline national trade targeting efforts and coordinate among the participating agencies; this includes the sharing of critical import safety information, sharing of best practices, reduction in duplicated targeting/examinations across agencies, and also serves as a central point of response for import safety events of interest to FDA, CBP, and other agencies present. The mission of the CTAC is in line with the President's Food Safety Working Group, which calls for agencies with an interest/authority in import safety to coordinate efforts and resources, and focuses on the core principles of prevention, surveillance, and response. Through a unique Memorandum of Understanding, agencies at CTAC are able to share information and systems access in order to conduct joint import safety targeting at a national level. Through this channel, the CTAC is an effective tool for CBP and FDA to enhance the safety of our Nation's food imports. At the center, personnel from both agencies respond collectively to allegations, develop food safety operations, coordinate with laboratories on food safety testing requirements, and pursue enforcement actions against shipments found to pose a threat to U.S. consumers.

CBP will continue to work with our Federal partners to prevent dangerous products from getting into the hands of the American consumers.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. BILL NELSON TO
HON. ALAN BERSIN

Question 1. Commissioner Bersin, how does transparency in trade data increase maritime security?

Answer. U.S. Customs and Border Protection (CBP) implements a risk-based, layered enforcement strategy toward securing maritime cargo. This multi-layered enforcement strategy includes the collection of advanced trade information (manifest and entry) from programs such as the 24-hour Rule, the Importer Security Filing ("10+2") and Customs-Trade Partnership Against Terrorism (C-TPAT). Prior to the collection of trade data provide to CBP as part of the "10+2" program, CBP primarily relied on the carrier's manifest data to perform security risk analysis prior to the lading of merchandise arriving by vessel. While manifest data by nature is timely, internal and external reviews have shown that alone, manifest data is not very detailed. As a result, CBP had found that in many instances, low-risk companies were being unduly targeted and examined. Conversely, and much more troubling from a security standpoint, is the fact that certain high-risk entities, questionable trade patterns and commodities of interest were not being identified and targeted 24 hours prior to vessel lading due to lack of quality trade data at that point in time.

The advanced entry data provided by the Importer Security Filing ("10+2") in conjunction with manifest data transmitted 24 hours prior to vessel lading has significantly increased the scope and accuracy of information gathered on the goods, conveyances and entities involved in the shipment of cargo, which vastly improves CBP's ability to identify high-risk shipments so as to prevent smuggling and ensure cargo safety and security. This advance knowledge allows CBP to make earlier and much better informed targeting decisions prior to cargo arrival which helps to foster and facilitate the movement of lawful international trade.

Question 2. The law requires CBP to make import and export data available for dissemination. Is complete data currently being made available to all of the appropriate entities who request it?

Answer. U.S. Customs and Border Protection (CBP) provides, daily in accordance with 19 CFR §103.31 (e) all available inward manifest information from its Automated Manifest System (AMS), within the Automated Commercial System, to those parties who subscribe to the CD-ROM service. Under CBP regulations at 19 CFR § 103.31(e) interested members of the public may purchase a single day or subscribe to AMS to receive the subject manifest data. Those companies or individuals who subscribe receive a CD-ROM daily with all CBP AMS manifest data wherein mani-

fest confidentiality has not been requested pursuant to 19 USC § 1431(c)(2) and 19 CFR § 103.31(d). The AMS data elements that may be released are enumerated in 19 CFR § 103.31(e)(3).

With regard to vessel outward manifest (export) data filed electronically, CBP provides a data push through a Virtual Private Network connection to those parties who have signed an Interconnect Security Agreement and met the technical specifications for the Information Technology interface. This data push currently encompasses 15 percent of outward manifests.

Access to outward manifests filed in paper or other than electronically, CBP currently permits access within its ports of entry to one requestor, and has been exploring means to accommodate additional requestors without interfering with port operations or over burdening port personnel with requests for review of copied information pursuant to section 19 CFR § 103.31 (b).

Question 3. If not, why?

Answer. Physical access to manifest documents at U.S. Customs and Border Protection (CBP) Ports of Entry by more than one entity has been identified as a logistical burden for the respective ports to manage, and raises concerns about safeguarding and securing those portions of the vessel manifest that are not available for public or press access. CBP continues to explore alternative methods to provide access to outward manifest data in an electronic format for interested parties.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARIA CANTWELL TO
HON. ALAN BERSIN

Question 1. In 2002, Customs and Border Protection established the rule requiring an electronic manifest be submitted 24-hours prior to loading onto any commercial ship destined for the U.S. This process identified cargo containers that required inspection at the foreign port of origin and also determined which cargo containers would be examined upon arrival in the United States. In addition, agreements were negotiated with foreign countries to allow U.S. Customs agents with overseas billets to work with their foreign Customs counterparts and effectively “push our borders out” to more thoroughly examine U.S. bound maritime cargo. However, today, I understand that CPB is withdrawing overseas billets and bringing a number of CBP Officers back to the U.S. Could you provide some additional details on this adjustment of overseas billets and what impact it will have on the Container Security Initiative?

Answer. The Container Security Initiative (CSI) program has developed significantly since its inception in 2002. The CSI program of tomorrow will be a hybrid of different (less personnel intensive, more technology driven) and more efficient and less costly concepts of operations to include remote targeting and remote examinations in a selected number of CSI ports, reciprocal relationships and the continued need for a minimal number of U.S. Customs and Protection (CBP) personnel stationed in foreign locations. CSI will maintain a foreign presence to witness exams, collaborate with host-country counterparts and maintain relationships with foreign customs administrations.

Question 2. Last month the GAO released a report on combating nuclear smuggling. What the GAO found quote “While DHS reports it scans nearly 100 percent of the cargo and conveyances entering the U.S. through land borders and major seaports, it has made less progress scanning for radiation: (1) in railcars entering the U.S. from Canada and Mexico; (2) in international air cargo; and (3) for international commercial aviation aircraft, passengers, or baggage.” For example, containers offloaded from foreign ships arriving in western Canadian ports, are placed on freight rail, and cross into our country over a land border. Are there differences between how U.S. and Canadian ports deploy radiation detection equipment and the procedures used to scan cargo entering each respective country?

Answer. There is no difference in the level of security scrutiny that cargo containers coming into the U.S. from Canada would receive versus containers entering directly from other foreign countries through U.S. ports. Conveyances arriving in the U.S. from Canada through land border ports of entry by truck or rail are considered to be arriving from a foreign country and are therefore subject to the same level of security scrutiny as containers being imported directly into U.S. ports.

Regardless of the mode of transportation, U.S. Customs and Border Protection (CBP) concentrates its efforts on its primary mission of preventing terrorists and terrorist weapons from entering the U.S., while at the same time facilitating legitimate trade and travel.

We are accomplishing these twin goals through the use of advance information, risk-management targeting systems, detection technologies, extended border strate-

gies and international partnerships. CBP employs a layered enforcement approach to safeguarding the U.S. from threats by land, air, and sea.

CBP recognizes that no single strategy or risk assessment is 100 percent effective and accurate, so CBP focuses on layering multiple initiatives together to accomplish its mission. CBP works aggressively with trade and government partners to legislate improvements regarding data timeliness and quality. This data enhances the ability of CBP's highly trained personnel, together with their use of cutting edge technology, to target, detect and interdict terrorists, or implements of terrorism, destined to the U.S.

Question 3. Do you believe this presents a potential vulnerability?

Answer. There is no difference in the level of security scrutiny that cargo containers coming into the U.S. from Canada would receive versus containers entering directly from other foreign countries through U.S. ports. Conveyances arriving in the U.S. from Canada through land border ports of entry by truck or rail are considered to be arriving from a foreign country and are therefore subject to the same level of security scrutiny as containers being imported directly into U.S. ports.

Regardless of the mode of transportation, U.S. Customs and Border Protection (CBP) concentrates its efforts on its primary mission of preventing terrorists and terrorist weapons from entering the U.S., while at the same time facilitating legitimate trade and travel.

We are accomplishing these twin goals through the use of advance information, risk-management targeting systems, detection technologies, extended border strategies and international partnerships. CBP employs a layered enforcement approach to safeguarding the U.S. from threats by land, air, and sea.

CBP recognizes that no single strategy or risk assessment is 100 percent effective and accurate, so CBP focuses on layering multiple initiatives together to accomplish its mission. CBP works aggressively with trade and government partners to legislate improvements regarding data timeliness and quality. This data enhances the ability of CBP's highly trained personnel, together with their use of cutting edge technology, to target, detect and interdict terrorists, or implements of terrorism, destined to the U.S.

Air Cargo Interagency Collaborations—Efforts between U.S. Customs and Border Protection (CBP) and other agencies have been established to address the strengthening of air cargo security; For example, Customs-Trade Partnership Against Terrorism (C-TPAT) is exploring opportunities with TSA's Certified Cargo Screening Program (CCSP) to increase information sharing between both programs through strategies such as collecting additional information during foreign validation visits and leveraging existing mutual recognition arrangements with foreign customs administrations.

And, the implementation of "Smart Border" agreements that involve a number of actions to improve information exchange and adopt benchmarked security measures that will reduce the terrorist threat at our borders, such as the sharing of significant seizure information that would enhance future targeting efforts.

These layers are interdependent and deployed simultaneously, to substantially increase the likelihood that contraband, including terrorists and weapons of terror will be detected. No single strategy could provide the level of security that CBP has worked to achieve and maintain since the tragic events of September 11, 2001.

The rail vector presents unique challenges to CBP in deploying effective radiation detection technology. In its ongoing efforts to address the nuclear threat, CBP has procured a new prototype dual-energy rail radiography system that incorporates a passive radiation detection capability. This new prototype was procured as a possible replacement for the large-scale NII rail imaging systems currently deployed to rail border crossings. CBP intends to replace its inventory of older rail radiography systems with new and enhanced technology as the older systems reach their end-of-life-cycle. Acceptance of this prototype is contingent upon ongoing testing and evaluation efforts by both the vendor and CBP. Additional characterization efforts of the active radiography and passive radiation detection technologies' capability to function in a synchronized mode are currently in the planning stages.

Question 4. Section 122 of SAFE Ports Act of 2006 required CPB to seek to develop a plan for the inspection, prior to the loading of passengers and vehicles, for U.S. inbound ferries. There are 28 ferries operating from Ports in Canada, Mexico, the British Virgin Islands, and the Dominican Republic, to ports in the U.S.

Washington State operates the largest passenger ferry system in the country. There are a handful of ferry routes between cities in Washington State and British Columbia. As you may recall, the so-called "millennium bomber" entered the country on a ferry from Canada. For these reasons, ferry security is ever present in the mind of my constituents.

To paraphrase the report delivered to Congress on January 9, 2009—we (CPB) took a look at it, looks like too hard a problem to solve because of the challenges that have arisen during current discussions with the Canadians for pre-inspection at land border points of entry, so we consider that we fulfilled the obligation.

I intend to raise the issue of ferry security when the Senate takes up reauthorization of the SAFE Ports Act. Are you willing to work with me between now and then in trying to figure out how to clear some of the hurdles to enable the development of a plan as envisioned in Section 122?

Answer. Yes. U.S. Customs and Border Protection (CBP) is aware that inbound ferries are a potential vulnerability. CBP currently receives some ferry Advance Passenger Information System (APIS) data voluntarily that allows for some advance screening. CBP would appreciate the opportunity to work with you to address these issues.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. MARK PRYOR TO
HON. ALAN BERSIN

Question 1. It is CBP's duty to "steadfastly enforce the laws of the United States while fostering our Nation's economic security through lawful international trade and travel." Customs has the sole responsibility of ensuring that duties assessed on unfairly traded imports are collected. The duties are often put in place on certain imports to serve as a deterrent against unfairly traded imports which were found to have injured U.S. companies and workers. It has come to my attention in recent months that there is a growing problem with import fraud by countries and companies seeking to evade certain duties. What steps are being taken by CBP to end this practice?

Answer. U.S. Customs and Border Protection (CBP) takes all matters of anti-dumping and countervailing duty (ADCVD) evasion very seriously, and in coordination with U.S. Immigration and Customs Enforcement (ICE) employs every available method in accordance with law to address these matters. Such actions may include entry summary reviews and/or cargo examinations by the ports; domestic importer premises visits; domestic broker/filer visits; sampling by the ports for CBP laboratory testing; and when available, foreign manufacture visits by the ICE attaché's office to review production capability and/or existence of operations. However, the volume of ADCVD cases and the complexity of regulating them pose a significant challenge.

ADCVD is a Priority Trade Issue (PTI) for CBP and as such, CBP conducts an assessment of our implementation and enforcement efforts on an on-going basis.

Question 2. Are you aware of such fraud issues as they relate to steel pipe and tube products from China?

Answer. U.S. Customs and Border Protection (CBP) has received multiple allegations of circumvention of antidumping cases on Chinese steel pipe and tube. CBP continues to work with U.S. Immigration and Customs Enforcement (ICE) as well as the domestic manufacturers of steel pipe and tube to address these matters.

Question 3. Does CBP have the resources to ensure the proper collection of all duties and prevent import fraud?

Answer. CBP is currently monitoring approximately 300 AD/CVD cases for which the Department of Commerce (DOC) has ordered the imposition of AD/CVD duties and dozens of AD/CVD cases that are in preliminary status. As you may know, DOC assigns various different duty rates for specific manufacturers within AD/CVD cases, providing incentive and opportunity for circumvention. For example, DOC assigned 195 different manufacturer deposit rates for the Chinese wooden bedroom furniture case. In addition, DOC issued 155 messages on that case, which includes scope rulings and injunctions. These points illustrate the challenges CBP has with administering and enforcing only one AD/CVD case.

CBP recently issued a vacancy announcement to add personnel to our National Targeting and Analysis Groups (NTAG), including the AD/CVD NTAG.

Question 4. With the ongoing focus of putting CBP resources on the border, what impact is that having on inspecting imports at ports of entry including U.S. ports?

Answer. While CBP has increased enforcement personnel along the southwest border with Mexico, particularly Border Patrol agents, we have not diminished our trade enforcement activities at seaports or airports.

CBP understands that there is a monetary gain in not paying the ADCVD duty on the subject products, and that certain foreign manufactures and U.S. importers will attempt to circumvent ADCVD cases. As such, CBP will continue to target im-

porters and manufactures for potential evasion of ADCVD cases and will use all available means to enforce the cases.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. KAY BAILEY HUTCHISON TO
HON. ALAN BERSIN

Question 1. The Coast Guard is responsible for securing 361 ports and 95,000 miles of coastline and navigable waterways. It also has 10 other missions, including maritime drug interdiction, search and rescue, immigration law enforcement at sea, and serving as the lead Federal agency responding to the *Deepwater Horizon* oil spill . . . and all of this with only 42,000 Active Duty personnel.

CBP also has an enormous number of tasks to accomplish with limited resources. Although you have only been on the job since the spring, in your estimation, is CBP adequately staffed to handle all the port security tasks?

Answer. The FY 2011 budget request includes the appropriate funding level to support U.S. Customs and Border Protection (CBP) personnel assigned to carry out their responsibilities. CBP has conducted staff modeling to assess where best to position its resources, and our major and minor ports all receive a share of resources based on operational need.

Question 2. The level of transportation security abroad has an important impact on our domestic homeland security efforts. The weaker cargo security standards are at foreign ports, the greater the risk to U.S. bound cargo. To that end, both the Coast Guard and CBP have developed international programs to improve and build a layered approach to port security.

CBP has developed a number of programs aimed at international port security including the "Customs-Trade Partnership Against Terrorism" (C-TPAT), the Container Security Initiative (CSI), and the "10+2" security filing. Given all the cooperative arrangements that are inherent in these programs, especially those with the private sector, is CBP able to quantify how these programs have contributed to cargo security?

Answer. During FY2009, Container Security Initiative (CSI) conducted 56,781 cargo exams of high-risk shipments in overseas ports. Since they were examined overseas, there was no reason to inspect them for security purposes once they were unladen in domestic ports and were more than likely released into the economy unless they were targeted for a non-security related inspection (*i.e.*, trade, narcotics, agriculture, etc.). To date, no instruments of terrorism have been detected in maritime containerized cargo destined for the U.S. CSI is currently operational in 58 ports worldwide. With these 58 ports, CSI processes approximately 86 percent of all maritime containerized cargo imported into the U.S., and U.S. Customs and Border Protection (CBP) continues to screen 100 percent of cargo manifests and related information.

For several years CBP has successfully utilized a layered enforcement strategy, involving different programs such as those described in the question and other security programs. The programs are inter-related and secure different parts of the supply chain. Each program has its own set of productivity measures all of which continue to increase each year and as a whole they combine to form a strong security posture which also serves to facilitate legitimate trade. The private sector continues to support a risk based cargo enforcement strategy. CBP recently concluded the 2010 Customs-Trade Partnership Against Terrorism (C-TPAT) member survey and the results will be made public later this year. More than 3,900 member companies, nearly half of all membership, chose to participate. This study demonstrates the effectiveness of C-TPAT in causing thousands of companies to give closer scrutiny to the security of the goods they handle and ensuring that their overseas suppliers have implemented sound security practices.

The 2010 study identified several collateral benefits for C-TPAT members that support the argument that the C-TPAT program has enhanced the security of the international supply chain:

- Decrease in supply chain disruptions.
- Establishment of supply chain security procedures where none existed before.
- More frequent review of service providers security standards.
- Reduce cargo theft and pilferage.
- Improved security for workforce.
- Access to security training sessions, tips, and techniques.

Question 3. How can these programs be further improved?

Answer. U.S. Customs and Border Protection (CBP) continues to pursue means of operating more effectively and efficiently as new technology becomes available. Container Security Initiative (CSI) targeters have implemented the Importer Security Filing data into targeting methodologies and continue to work closely with host country nations on information sharing.

CBP's security programs are relatively mature and stable at this point and we continually making process improvement so that CBP can effectively segment risk and ensure legitimate trade moves quickly through the supply chain. For example, in 2010 Customs-Trade Partnership Against Terrorism (C-TPAT) established an internal Evaluation and Assessment Branch to ensure validations are conducted consistently and in accordance with established standard operating procedures.

Question 4. One CBP program that has encountered numerous challenges is the Secure Freight Initiative (SFI), which Congress mandated to test the feasibility of 100 percent scanning of U.S. bound cargo at foreign ports.

The GAO recommended that CBP conduct a feasibility study of the SFI program before moving forward with any future implementation, but to date, CBP has not completed such a study. Why has the study not been completed?

Answer. U.S. Customs and Border Protection (CBP) has conducted initial research in the feasibility and cost benefit analysis of one hundred percent scanning. A complete cost of the Secure Freight Initiative (SFI) pilot ports has been documented in the bi-annual reports to Congress.

Question 5. Do you believe the costs of 100 percent scanning outweigh the benefits to securing U.S. bound cargo?

Answer. U.S. Customs and Border Protection (CBP) recognizes that 100 percent scanning may play a role in certain trade corridors where the scan data can provide additional information to improve the security of that particular supply chain but believes a risk-based approach should also be considered.

Some governments, as a result of concerns over sovereignty, feasibility, logistics, their own regulatory authority, and cost may decide to forego 100 percent scanning in their ports. Such concerns affected the participation of at least one major trading partner in the SFI study. CBP will continue to work with foreign governments, carriers, and shippers globally to improve risk-based targeting and enhance supply chain security.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV
TO STEPHEN L. CALDWELL

Question 1. Pending the release of the implementation plan for the DHS Small Vessel Security Strategy, what are the potential options for mitigating threats from small vessels? To what extent would a new requirement that small vessels carry transponders—so they could be tracked—be a viable solution? How does this option compare to increased “neighborhood watch” type programs to encourage watermen and pleasure boaters to report suspicious activity?

Answer. Please see the question below for a joint response.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. KAY BAILEY HUTCHISON TO
STEPHEN L. CALDWELL

Question. Since the terrorist attacks of September 11, 2001, maritime security efforts have focused primarily on large commercial vessels, cargoes, and crew. Efforts to address the small vessel environment have largely been limited to traditional safety and basic law enforcement concerns. Small vessels are, however, readily available for potential exploitation by terrorists, smugglers of weapons of mass destruction (WMDs), narcotics, aliens, other contraband, and other criminals. Small vessels have also been successfully employed overseas by terrorists to deliver Waterborne Improvised Explosive Devices (WBIEDs). GAO previously noted that technology systems used by the Coast Guard to track small vessels have not worked properly at night or during inclement weather. In your view, is it cost-effective to track small vessels?

Answer. Governmental agencies, both in the United States and abroad, have exercised several options to address the risks presented by small vessels. As we previously reported in April 2010,¹ the Department of Homeland Security (DHS)—in-

¹ GAO, *Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain*, GAO-10-400, (Washington, D.C.: Apr. 9, 2010).

cluding the U.S. Coast Guard and U.S. Customs and Border Protection (CBP)—and other entities are taking actions to reduce the risk from small vessels. These actions include the development of the *Small Vessel Security Strategy*,² community outreach efforts through the America's Waterway Watch (AWW) program and Operation Focused Lens, port-level vessel tracking efforts with radars and cameras, port-scale nuclear detection pilot projects, establishment of security zones in U.S. ports and waterways, and escorts of possible targets of waterborne improvised explosive devices. CBP and the Coast Guard also have other efforts under way to prevent small vessels from transporting weapons of mass destruction, terrorists, or narcotics from foreign countries into the United States. CBP's Office of Air and Marine reports that it is using airborne assets such as four engine P3 Airborne Early Warning and Long Range Tracker aircraft and soon maritime reconnaissance versions of unmanned Predator drones, to detect smugglers' vessels, including semisubmersibles, sailing to the United States. The Coast Guard and CBP's Office of Air and Marine also report that they station patrol vessels along smuggling routes to intercept smugglers' vessels before they reach U.S. shores. At the request of Chairman Bennie Thompson and Ranking Member Peter King of the Committee on Homeland Security, House of Representatives, we are currently reviewing CBP's Office of Air and Marine program and examining the agency's use of its resources and expect to issue the results of this review next year. Outside of the United States, the government of Singapore began a program in 2007 called Harbour Craft Transponder System where all vessels not covered by the International Maritime Organization's (IMO) International Convention for the Safety of Life at Sea (generally, this convention covers vessels 300 gross tons or more on an international voyage and cargo ships of 500 gross tons or more) were required to install and operate transponders that broadcast their position. The program was implemented jointly by the Maritime and Port Authority, the Police Coast Guard and the Republic of Singapore Navy, and an estimated 2,800 small vessels were equipped when its operation commenced in 2007. User costs include the transponder device, which ranges in cost from approximately \$700 to \$730 plus applicable taxes, depending on whether the model is portable or fixed, and an annual operating cost of approximately \$90.

As we reported in March 2009, the expansion of vessel tracking to all small vessels—through transponders or other methods—may be of limited utility because of the large number of small vessels, the difficulty identifying threatening actions, the challenges associated with getting resources on scene in time to prevent an attack once it has been identified, and the limitations of certain equipment.³ For vessels not required to carry automatic identification system (AIS)⁴ equipment, cameras may be utilized, though not all ports have cameras suited to overcome challenges posed by low lighting during operation at night or in bad weather. Even when vessels carrying transponders are tracked in ports, recognizing hostile intent is very difficult. During our reviews of maritime security efforts, we were provided evidence of vessels intruding into security zones where unauthorized access was prohibited. While no attacks occurred, such vessels were able to travel freely near potential targets. Coast Guard officials have told us that their ability to enforce security zones is constrained by their limited resources. Moreover, the Coast Guard has not been able to meet its own internal standards for the frequency of escorts of potential target vessels. The difficulty in recognizing potentially threatening activity and the limited response capability indicates that expanding tracking to all small vessels would not necessarily diminish the risk posed by small vessels. While such tracking would likely lead to increased observation of prohibited activities, such as intrusion

²The goals of DHS's *Small Vessel Security Strategy* are consistent with the critical infrastructure protection maritime sub-sector goal to enhance the resiliency of the maritime transportation system. According to the strategy, reducing the risk from small vessels will contribute to the security of our ports and help prevent the disruption of commerce and the negative impact of a vessel security incident by reducing the potential consequences of such an incident. The primary consequence of a terrorist incident (as well as other transportation security incidents) arising from the use of a small vessel could be devastating for the U.S. economy if it damaged critical infrastructure or resulted in closure of a port. By reducing the risk and the associated consequences from small-vessel risks, the strategy contributes to the resilience of the maritime sector and associated critical infrastructure.

³As we reported in March of 2009, some cameras have the ability to operate in low light or use infrared images that distinguish objects by the heat they emanate. These capabilities allow them to be effective when cameras using visible light prove ineffective, such as at night or in bad weather. However, these cameras can still be affected by high surf conditions, which can hide vessels smaller than the height of the waves. For additional information, see GAO, *Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed*, GAO-09-337 (Washington, D.C.: Mar. 17, 2009).

⁴AIS is a technology that uses global navigation satellite data and radios to transmit and receive information about a vessel's voyage, including its name, position, course, and speed.

into security zones, it would not necessarily help to differentiate between vessels that entered security zones with hostile intent and vessels that entered for other reasons, such as better fishing. In addition, with the increased number of vessels to observe, watch standers could be overwhelmed by the amount of information they must track or monitor. While the Coast Guard has research underway to automate its ability to detect threatening behavior by vessels, even if these efforts are successful they would not improve the agency's ability to respond quickly. DHS's *Small Vessel Security Strategy* also states that small-vessel risk reduction efforts should not impede the lawful use of the maritime domain or the free flow of legitimate commerce—making the need to decipher vessel behavior essential. As the strategy states, given the size and complexity of the maritime domain, risk-based decision-making is the only feasible approach to prevention, protection, response and recovery related to small-vessel threats.

Much of the seaborne smuggling of narcotics and undocumented migrants into the United States currently makes use of small vessels, such as high-speed "go fast" boats and semisubmersibles. While CBP and the Coast Guard are also taking actions to intercept smugglers at sea, their ability to prevent this smuggling is mixed. In its Fiscal Year 2009 performance report, the Coast Guard reported removing 15 percent of the cocaine being transported on noncommercial vessels bound for the United States in Fiscal Year 2009. Conversely, the Coast Guard reported that it interdicted approximately 84 percent of undocumented migrants who attempted to enter the United States via maritime routes in Fiscal Year 2009. CBP's performance report did not include similar measures for maritime narcotic or migrant interdiction.

With the critical task of mitigating the risk posed by small vessels before the Coast Guard and CBP, we believe a risk management approach coupled with strong intelligence-gathering efforts would lead to the greatest benefit. Intelligence-gathering efforts at the port level, such as AWW, should help uncover potential threats before they develop into full-fledged attacks. The program's outreach to over 400 local watch group members in and around the Puget Sound region for the Vancouver 2010 Winter Olympics demonstrated its potential as means of increasing vigilance and communication. Moreover, targeted efforts aimed at protecting critical infrastructure and valuable vessels, along with random escorts and patrols, should help provide deterrence against a small vessel attack inside U.S. port areas. Off-shore, intelligence efforts aimed at uncovering smuggling operations should also help to target patrols and interceptions. These efforts would include random patrols, which add uncertainty to where these assets will be at any one time. A risk management approach that focuses limited resources on the greatest risks is even more critical given the Federal Government's current budget climate.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JOHN D. ROCKEFELLER IV
TO STEPHEN L. CALDWELL

Question 2. Regarding security in foreign ports, your statement emphasized the importance of risk management and indicated that your work had shown potential to apply more risk management to the Coast Guard inspection of foreign ports. What did your work specifically show and how could the Coast Guard use risk management more effectively? Can the Coast Guard do this on its own, or would legislative changes be needed to implement changes in the frequency or intensity of visits to foreign ports?

Answer. Since we issued our report on the Coast Guard's International Port Security Program in April 2008, the Coast Guard has adopted a new risk management program.⁵ In April 2008, the Coast Guard was just beginning the next phase of the program, revisiting countries to reassess the security measures of 138 trading partners. As part of this next phase, the Coast Guard planned to place greater emphasis on countries that were not in compliance or that were struggling to comply with International Ship and Port Facility Security (ISPS) Code requirements. To accomplish this with available resources, the Coast Guard planned to prioritize its country visits and capacity-building efforts using a risk-based approach that would allow Coast Guard officials to spend more time in countries not in compliance and whose lack of compliance poses a higher risk to the United States. At the time of our report, the Coast Guard was in the process of developing this risk-management approach and had created working groups to consider how to implement this approach. Since the issuance of our report, the Coast Guard reported that the program finalized its methodology which analyzes the risk a country potentially poses to the

⁵ Our April 2008 report is restricted and not available to the public.

United States, how well a country is implementing the ISPS Code, and the likelihood that capacity-building efforts in the country would be effective considering a variety of political, economic, and social preconditions. According to the Coast Guard, the results of the methodology are used to manage risk and limited resources by helping establish assessment team size, determining countries and ports where capacity-building resources would be most effective, and finally identifying high-risk countries that need additional oversight. We have not conducted a detailed review of this methodology or the Coast Guard's implementation of it.

Although we have not analyzed or directly reported on this issue as it relates to the Coast Guard, another approach the Coast Guard could consider to incorporate risk management into the program is to use mutual recognition arrangements with other countries, similar to that developed by CBP for international customs. We reported in August 2008 that CBP worked with the international customs community to achieve a system of mutual recognition—an arrangement whereby the actions or decisions taken by one customs administration are recognized and accepted by another administration.⁶ For a system of mutual recognition to work, however, there must be an agreed-upon common set of standards that are applied uniformly so that a level of confidence exists between countries. As international standards exist for maritime security through the ISPS Code, the Coast Guard could consider developing a similar system of mutual recognition for international maritime security. For example, the European Union has developed detailed regulations for the consistent implementation of the ISPS Code by its member states and established a process for verifying the effectiveness of its member states' maritime security measures. This process includes an inspection of member states' ports that results in a report identifying any nonconformities with the regulations and making recommendations to address the nonconformities. Should the Coast Guard develop confidence in the European Union's regulatory and inspection approach to determine whether its members have fully implemented and maintain international maritime security standards, under a mutual recognition arrangement with the European Union the Coast Guard could agree to recognize and accept one another's security practices. The Coast Guard could then give countries with which it has such agreements lower priority for a country visit. During a meeting in September 2010 to follow-up on our report, Coast Guard officials told us that more flexibility to determine whether an assessment is necessary for countries with which there is confidence in the implementation of international maritime security standards would be helpful to the program in allocating program resources toward the highest-risk countries. Changes to increase the frequency of visits to foreign ports would not require a legislative change, whereas a decrease in frequency may require a legislative change.

In regard to the Coast Guard's ability to spend more time in countries not in compliance to assist with capacity building, we reported in April 2008 that the International Port Security Program was subject to limitations on its ability to offer capacity-building assistance outside of assessment activities or to other countries that may comply with the ISPS Code standard, but struggle to maintain their compliance. Coast Guard officials stated that while authorities allowed for certain types of capacity-building activities, several of the authorities limited those activities to ports in foreign countries that have been found to lack effective antiterrorism measures. However, with the enactment of the Coast Guard Authorization Act of 2010,⁷ the Coast Guard has new authorities to provide assistance to what the Coast Guard describes as a broader range of countries. For example, the act authorizes the Coast Guard to provide specified types of assistance to foreign ports based on risk assessments and comprehensive port security assessments rather than a finding of the lack of effective antiterrorism measures before providing assistance. In terms of changes to the frequency of visits to foreign ports, although the Security and Accountability For Every Port Act of 2006 (SAFE Port Act) currently requires that a minimum number of reassessments of the effectiveness of antiterrorism measures in foreign ports be conducted at a rate of not less than once every 3 years,⁸ the International Port Security Program strives to conduct reassessments every 2 years to follow the direction contained in the conference report accompanying the Fiscal Year 2007 DHS Appropriations Act.⁹ The Coast Guard states that in addition to the reassessments, it visits all countries at least annually, with countries that have ports with nonconformance issues it has identified more frequently. Consequently,

⁶GAO, *Supply Chain Security: CBP Works with International Entities to Promote Global Customs Security Standard and Initiatives, but Challenges Remain*, GAO-08-538 (Washington, D.C.: Aug. 15, 2008).

⁷Pub. L. No. 111-281, Stat. _____ (2010).

⁸Pub. L. No. 109-347, 120 Stat. 1884, 1918 (2006).

⁹H.R. Conf. Rep. No. 109-699, at 142 (2006).

to decrease the frequency of visits to an amount less than the established frequencies in the SAFE Port Act would require legislative changes whereas an increase in frequency would not require legislative changes.

Question 3. S. 3639 authorizes the Coast Guard to provide assistance to foreign governments or ports to enhance their maritime security. Does GAO support this provision?

Answer. Provisions in S. 3639 to authorize the Coast Guard to provide assistance to foreign governments or ports to enhance their maritime security are similar to provisions recently enacted in the Coast Guard Authorization Act of 2010. While we have not directly looked at this issue, based on our work, Coast Guard technical assistance to other countries could be another way to improve port security in certain circumstances with available Coast Guard resources. During our review of the International Port Security Program, Coast Guard officials told us that funding is a major challenge for most countries struggling to meet and sustain ISPS Code requirements.¹⁰ For example, Coast Guard officials stated that in several African countries, the designated authority within the government does not have the resources to provide security for ports or funds to provide grants for ports in need of improvements. However, according to Coast Guard officials, the Coast Guard also does not have resources to supply physical security assets, such as fences and guards, to those countries that cannot afford them. Program officials have sought to raise awareness about low-cost methods that can be used to meet certain international security requirements, such as the use of “tabletop” exercises rather than conducting full-scale drills and exercises.

In addition to the budgetary limitations, Coast Guard officials stated that the program faced legal limitations in the capacity-building efforts they could provide under their previous legislative authorities. As discussed above, while previous authorities allowed for certain types of capacity-building activities, several of those authorities limited those activities to ports in foreign countries that had been found to lack effective antiterrorism measures. However, with the enactment of the Coast Guard Authorization Act of 2010, the Coast Guard has new authorities to provide assistance. For example, the Act authorizes the Coast Guard to provide assistance based on risk assessments and comprehensive port security assessments rather than a finding of a lack of effective antiterrorism measures. Another capacity-building authority authorizes the provision of technical assistance when it is provided in conjunction with regular Coast Guard operations. The Coast Guard Authorization Act of 2010 amended this authority to expressly authorize the use of funds for certain purposes such as the activities of traveling contact teams, including any transportation expense, translation services, seminars, and conferences involving members of maritime authorities of foreign governments, and the distribution of publications pertinent to engagement with maritime authorities of foreign governments.

Question 4. Does the Coast Guard have an adequate workforce of inspectors who can operate in foreign environments to inspect foreign ports? To what extent would that workforce be affected by proposals to change the frequency or intensity of visits to foreign ports? How would it be affected by proposals to increase technical assistance to foreign governments and ports outside of the normal visit/inspection cycle?

Answer. We reported in January 2010 that during this decade, the Coast Guard has been challenged with expanded mission responsibilities, and concerns have been raised about whether the Coast Guard has a sufficient workforce to fulfill these mission responsibilities.¹¹ The impact of expanding missions underscored shortcomings in the Coast Guard’s ability to effectively allocate resources, such as personnel; ensure readiness levels; and maintain mission competency. Similarly, when we concluded our review of the International Port Security Program in April 2008, we reported that the Coast Guard also faced challenges in ensuring that it had trained staff available to meet assessment and assistance needs. According to Coast Guard officials, personnel working in the program have unique demands placed on their skills since they must be proficient security inspectors and must also be culturally and diplomatically sensitive liaisons to foreign countries. The challenge was made more difficult by Coast Guard plans to compress its schedule for completing follow-up visits so that all were to be completed within a 2-year time-frame and by the Coast Guard personnel rotation policy that moves personnel between different positions every 3 to 4 years.

¹⁰Our April 2008 report is restricted and not available to the public.

¹¹GAO, *Coast Guard: Service Has Taken Steps to Address Historic Personnel Problems, but It Is Too Soon to Assess the Impact of These Efforts*, GAO-10-268R, (Washington, D.C.: Jan. 29, 2010).

We also reported that the Coast Guard did not have a fully developed strategic workforce plan for the program. Coast Guard officials noted that the calculations for the number of program personnel required were straightforward as the number of countries to assess was limited to approximately 138 and the amount of time required to conduct assessments was known. When we asked Coast Guard officials about ensuring the availability of sufficient resources for the next phase of the program, Coast Guard officials stated that they believed they had sufficient resources to conduct assessments and provide capacity building within the current authorities provided to the program. However, we reported that they had not completed aspects of workforce planning, such as processes to regularly analyze staffing data and workforce demographics and develop strategies for identifying and filling gaps, as human capital management guidance provided by the Office of Personnel Management suggests. Without such planning, we reported that it may be difficult for the Coast Guard to meet its program goals. As a result, we recommended that the Coast Guard develop and incorporate a workforce plan as part of the risk management approach it was developing to prioritize the performance of program activities. DHS and the Coast Guard concurred in part with our recommendation. Specifically, they noted that the Coast Guard has analyzed its workforce needs to carry out the functions currently mandated and had begun to develop a methodology to determine where best to conduct capacity-building efforts. They stated that more analysis would be done when and if authorities are provided to expand the capacity-building activities of the program. While we agreed that the Coast Guard would need additional authorities to carry out certain capacity-building activities beyond countries not in compliance, the Coast Guard's workforce planning efforts were not consistent with those called for by human capital management guidance, even for the program's current authorities.

While we do not have the data or information to determine how the Coast Guard's workforce would be affected by potential changes to the frequency or intensity of visits, or changes to increase the technical assistance to foreign governments and ports, since the issuance of our report the Coast Guard has reported taking additional actions to more fully develop a workforce plan for the program. Although the program does not envision a separate "stand-alone" plan, the Coast Guard reported reviewing human capital management guidance and is incorporating some of the principles in its program management. Among other things, the Coast Guard reported that the program continues to refine its human capital management including using an analysis to identify training needs for new personnel entering the program and promulgation of guidance on resources that should be devoted to conducting assessment visits for various categories of countries. The program also reported finalizing its methodology which looks at the risk a country potentially poses; how well it is implementing the international security standard, the ISPS Code; and the likelihood that the capacity-building efforts in the country would be effective. While we have not assessed these actions, we believe they contribute toward the implementation of our recommendation and thereby better position the Coast Guard to ensure that it has an adequate work force. Should the program be given additional capacity-building authority, the Coast Guard stated that the program will use its methodology to identify additional personnel needs and where they should best be stationed.

Question 5. Has GAO's work made a formal determination of whether the 100 percent scanning requirement is consistent with risk management?

Answer. The application of risk management for container security can be considered at the strategic level (*e.g.*, assessing risks to the entire supply chain and designing appropriate security programs) or the tactical level (*e.g.*, assessing risks to individual containers and applying extra scrutiny through existing layered security programs). At the strategic level, Federal law and Presidential directives call for the use of risk management in homeland security as a way to protect the Nation against possible terrorist attacks, and CBP uses risk management in its processes for mitigating potential threats posed by U.S.-bound cargo containers. Risk management generally calls for establishing risk management priorities and allocating limited resources to those assets that face the highest risk. Risk management is necessary in the context of container security because CBP, like other DHS components, cannot afford to protect all commerce against all possible threats. According to risk management frameworks developed by GAO and DHS, key phases of risk management should include: (1) assessing the risk posed by terrorists' use of cargo containers; and (2) evaluating alternative measures to counter that risk based on factors such as the degree of risk reduction they afford and the cost and difficulty to

implement them.¹² This process includes a cost-benefit analysis of countermeasure options, which is useful in evaluating alternatives because it links the benefits from risk-reducing countermeasures to the costs associated with them. While we have not conducted an assessment of whether the 100 percent scanning requirement is consistent with risk management, our prior work indicates that 100 percent scanning is not consistent because this strategic analytic process did not occur. Specifically, our work has shown that DHS has not evaluated the cost-effectiveness of 100 percent scanning as a countermeasure as part of a risk management framework for cargo container security.¹³

At the tactical level, opponents of 100 percent scanning have taken the position that it is better to assess the risk posed by each container and apply a countermeasure that is tailored to that container—as opposed to assessing the risk posed to supply chain security by cargo containers in general and then determining the most cost-effective countermeasure to reduce that risk (e.g., 100 percent scanning, CBP’s layered security approach, or another alternative). From this perspective, the 100 percent scanning requirement is a departure from existing CBP container security programs because it requires CBP to scan all containers before performing analysis to determine their potential risk level. This position applies risk management principles—establishing strategic goals and priorities and allocating limited resources to those assets that face the highest risk—at the individual container level. According to this view, the 100 percent scanning requirement is inconsistent with risk management principles because it does not distinguish among containers based on risk; rather, it assumes that all containers have an equal risk of carrying terrorist weapons and are to be subjected to the same level of scrutiny with the same amount of resources. Thus, resources are applied uniformly across all cargo containers rather than being allocated based on the potential risk they pose. Opponents of 100 percent scanning who have generally taken this position include CBP, foreign governments, and industry. For example, the former Acting Commissioner and current Commissioner of CBP have said that the 100 percent scanning requirement is not a risk-based approach. Similarly, foreign governments have expressed the view that 100 percent scanning is not consistent with risk management principles as contained in the World Customs Organization (WCO) Framework of Standards to Secure and Facilitate Global Trade (commonly referred to as the SAFE Framework). For example, European and Asian customs officials told us that the 100 percent scanning requirement is in contrast to the risk-based strategy, that serves as the basis for other U.S. programs, such as the Container Security Initiative (CSI)¹⁴ and the Customs-Trade Partnership Against Terrorism (C-TPAT).¹⁵ The WCO, representing customs agencies around the world, stated that the implementation of 100 percent scanning would be “tantamount to abandonment of risk management.” In terms of industry, in 2008 the Association of German Seaport Operators released a position paper that stated that implementing the 100 percent scanning requirement would undermine mutual, already achieved security successes and deprive resources from areas that present a more significant threat and warrant closer scrutiny. Closer to home, the Commercial Operations Advisory Committee—an official industry group to CBP—has recently called for the repeal of the 100 percent scanning requirement and a move toward a more risk-based approach.¹⁶

Still at the tactical level, supporters of 100 percent scanning have expressed concerns about the effectiveness of existing CBP programs that attempt to assess the risks of individual containers and subject those deemed higher risk to closer scrutiny, including non-intrusive inspection (NII) scanning. Members of Congress who spoke in favor of the 100 percent scanning requirement noted that scanning all containers overseas could help detect weapons of mass destruction concealed in con-

¹² GAO-06-91 and DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: January 2009).

¹³ GAO, *Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers*, GAO-10-12 (Washington, D.C.: Oct. 30, 2009).

¹⁴ CBP places staff at participating foreign ports to work with host country customs officials to target and examine high-risk container cargo for weapons of mass destruction before they are shipped to the United States.

¹⁵ Through the C-TPAT program, CBP develops voluntary partnerships with members of the international trade community comprised of importers; manufacturers; customs brokers; forwarders; air, sea, and land carriers; and contract logistics providers. Private companies agree to improve the security of their supply chains in return for various benefits, such as reduced examination of their cargo.

¹⁶ The Commercial Operations Advisory Committee advises the Secretaries of the Treasury and Homeland Security on the commercial operations of CBP and related DHS and Department of the Treasury functions.

tainers that are not identified as high risk because of weaknesses in CBP's layered security strategy. That is, 100 percent scanning would be a more effective way to counter the risks posed to cargo containers than existing initiatives intended to identify high-risk containers. In making these arguments, certain Members of Congress also cited GAO work that had identified potential weaknesses in programs that make up the layered security strategy. Our work identified weaknesses including a lack of validation of CBP's targeting practices through strategies like re-teaming; inadequate validation of C-TPAT members' security practices prior to granting them program benefits, such as a decreased likelihood of having their shipments scanned or physically examined; and not ensuring that containers identified as high risk but not scanned at CSI ports overseas are scanned upon arrival in the United States.¹⁷ The concerns we raised were open issues at the time Congress considered the 100 percent scanning requirement; however, since that time, these CBP programs have matured, and many of our recommendations have been implemented.¹⁸

As mentioned above, risk management includes not just assessing risks, but also evaluating alternative measures based on such factors as the degree of risk reduction they afford and the cost and difficulty to implement them. Our work has documented that there are operational challenges—such as logistics, technology, and infrastructure—to implementing 100 percent scanning.¹⁹ However, CBP has not done a detailed analysis to determine the feasibility of 100 percent scanning within the context of its risk-based layered security strategy. In this case, part of evaluating alternative measures is determining a concept of operations—a description of the operations that must be performed, who must perform them, and where and how the operations will be carried out—for how 100 percent scanning would work at foreign ports, which would include conducting studies and analyses at each port to determine locations where NII equipment would be able to scan 100 percent of containers going to the United States with a minimum of disruption to the flow of commerce at the port. For instance, transshipment—cargo containers from one port that are taken off a vessel at another port to be placed on another vessel bound for the United States—poses a particular challenge to 100 percent scanning. According to European customs officials, implementing the 100 percent scanning requirement at large ports with complex operations would likely result in the need for a fundamental redesign of several ports, entailing substantial costs to terminal users. For other scanning options, the costs may not be as great. For example, as we describe in more detail in the next section, scanning with only radiation portal monitors (RPM) is less costly in terms of both equipment and impact on the flow of commerce.

No homeland security program can guarantee complete success or freedom from risk, and CBP officials have acknowledged that they will likely not be able to achieve 100 percent scanning of U.S.-bound cargo containers by the statutory deadline.²⁰ However, we believe additional analysis, done within a risk management framework, can help improve container security. In our October 2009 report on the Secure Freight Initiative (SFI) and 100 percent scanning, we recommended that among other things, CBP perform feasibility and cost-benefit analyses to: (1) better position itself to determine the most effective way forward to enhance container security, (2) improve its container security programs, and (3) better inform Congress. DHS agreed in part with our recommendation that it develop a cost-benefit analysis of 100 percent scanning, acknowledging that the recommended analyses would better inform Congress, but stated that the recommendation should be directed to the Congressional Budget Office. While the Congressional Budget Office does prepare cost estimates for pending legislation, we think the recommendation is appropriately directed to CBP. Given its daily interaction with foreign customs services and its direct knowledge of port operations, CBP is in a better position to conduct any cost-

¹⁷See for example, GAO, *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security*, GAO-05-404 (Washington, D.C.: Mar. 11, 2005), and *Homeland Security: Summary of Challenges Faced in Targeting Ocean-going Cargo Containers for Inspection*, GAO-04-557T (Washington, D.C.: Mar. 31, 2004).

¹⁸We previously reported on the maturing of these programs and the implementation of our recommendations in GAO, *Maritime Security: The SAFE Port Act: Status and Implementation One Year Later*, GAO-08-126T (Washington, D.C.: Oct. 30, 2007).

¹⁹GAO, *Supply Chain Security: Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers*, GAO-08-533T (Washington, D.C.: June 12, 2008).

²⁰The statute provides that containers loaded at foreign ports on or after July 1, 2012 shall not enter the United States unless they were scanned by NII equipment and radiation detection equipment prior to loading. It also provides for renewable, two-year extensions if DHS certifies to Congress that certain conditions exist at a port or ports, such as equipment not being available for purchase and installation, physical constraints, or a significant impact on trade capacity and flow of cargo. See 6 U.S.C. §982(b).

benefit analysis and bring results to Congress for consideration. We believe that such analyses could help to guide DHS, CBP, and Congress in their efforts to either implement the 100 percent scanning requirement or assess other approaches to enhancing container security.

Question 6. S. 3639 makes a technical amendment so that all U.S.-bound containers be scanned with either RPM or NII, but not both. It also extends the deadline for the requirement by 3 years from 2012 to 2015. What are the advantages of this approach to 100 percent scanning?

Answer. Based on our review of the 100 percent scanning requirement, scanning containers with RPMs instead of in combination with NII equipment may be more achievable from a technology, logistics, political, and cost standpoint.²¹ However, there are limitations to relying solely on RPMs for scanning cargo containers that should be taken into consideration.

- *Technology/logistics:* Scanning containers with RPM equipment is generally less time-consuming than scanning with NII equipment. While the actual NII scanning time per container can take as little as 20 seconds, depending on the system, the entire inspection time can take longer than 6 minutes. As part of the scanning process, customs officers need time to: (1) stage the container to align it properly between the system's radiation source and detector array, (2) verify the container information with the manifest, (3) ensure that the system is set to receive scanned images, (4) interpret the scanned images and verify them using manifest information, (5) identify and document any anomalies, (6) save the scanned images, (7) check the integrity of the seal and verify the seal number, and (8) prepare the system for the next container. While scanning cargo containers with NII equipment involves several steps, in contrast it takes the driver of a standard tractor trailer from 4 to 7 seconds to pass through a RPM.²²
- *Political:* Although 173 members of the WCO expressed their opposition to the 100 percent scanning requirement, in a letter to Members of Congress in September 2008, the WCO noted that it did not object to the requirement that all cargo containers be subjected to radiation detection processes (*i.e.*, RPM scanning) prior to shipment to the United States. In addition, foreign government officials we spoke with stated that they are generally not opposed to the use of radiation detection equipment—such as the RPMs that are used as part of the Megaports Initiative²³—but they are opposed to the use of NII equipment because of the likelihood that it may hinder trade and reduce security by consuming a large amount of scarce resources (*i.e.*, key dock space and increased time needed for cargo container inspections) for comparatively little benefit.
- *Cost:* RPM equipment is less expensive than NII equipment. The price for polyvinyl toluene monitors—the type of RPMs most commonly used at U.S. seaports—is \$425,000 per unit (including deployment costs). In contrast, the purchase price for large-scale NII systems used by CBP at U.S. seaports is approximately \$3 million per system (including deployment costs).
- *Limitations of RPMs:* Scanning containers with RPMs alone introduces the vulnerability of not detecting shielded nuclear material. However, if customs officials believe based on targeting data that further inspections are necessary, they can have a container scanned by NII equipment.

In addition to the factors listed above, the Department of Energy's National Nuclear Security Administration (NNSA) has a goal through the Megaports Initiative of scanning as much global cargo container traffic as possible with RPMs. Since the start of the Megaports Initiative in Fiscal Year 2003, NNSA has completed installations of RPM equipment at 27 foreign ports, and implementation is under way at an additional 16 foreign ports. The Megaports Initiative seeks to equip 100 ports with radiation detection systems by 2015, scanning approximately 50 percent of global maritime containerized cargo.

²¹ GAO-10-12.

²² Containers that trigger a radiation alarm at the RPM undergo a second exam with a handheld radiation detection device to help ensure that the source of the alarm is identified and resolved. The exam with the handheld radiation detection device typically requires 5 to 10 minutes to perform.

²³ Through the Megaports Initiative, the Department of Energy installs radiation detection equipment at key foreign ports, enabling foreign government personnel to use radiation detection equipment to scan shipping containers entering and leaving these ports, regardless of the containers' destination, for nuclear and other radioactive material that could be used against the United States and its allies.

Question 7. DHS and CBP have cited the Strategic Trade Corridor and the Importer Security Filing (10+2) as alternative ways to enhance supply chain security. They have also stated that new technology for containers themselves, and the equipment used to scan them, is another path forward to improve supply chain security. What work does GAO have on these programs and what is the status of these DHS efforts?

Answer:

Strategic Trade Corridor Strategy

The Secretary of Homeland Security has endorsed the concept of a strategic trade corridor strategy as the path forward for implementing the SFI program, but DHS and CBP have not yet selected the ports or funded the expansion of SFI. In particular, in April 2009, the Secretary of Homeland Security was presented with three options for implementing the SFI program, ranging from implementing SFI at 70 ports that account for shipping over 90 percent of U.S.-bound containers to seeking repeal of the 100 percent scanning requirement. The strategic trade corridor strategy option selected by the Secretary focuses cargo container scanning efforts on a limited number of ports where CBP has determined that SFI will help mitigate the greatest risk of potential weapons of mass destruction entering the United States. According to CBP's report, *Risk-Based, Layered Approach to Supply Chain Security*, sent to Congress in April 2010, the data gathered from SFI operations will help to inform future deployments to strategic locations.²⁴ The report further added that CBP plans to evaluate the usefulness of these deployments and consider whether the continuation of scanning operations adds value in each of these locations and in potential additional locations that would strategically enhance CBP efforts. However, in DHS's *Congressional Budget Justification for FY 2011*, CBP requested a decrease in the SFI program's \$19.9 million budget by \$16.6 million and did not request any funds to implement the strategic trade corridor strategy. According to the budget justification, in Fiscal Year 2011, SFI operations will be discontinued at three SFI ports—Puerto Cortes, Honduras; Southampton, United Kingdom; and Busan, South Korea—and the SFI program is to be established at the Port of Karachi, Pakistan. We issued a report in October 2009 that provides further details about the implementation of the SFI program.²⁵

Importer Security Filing Program

While CBP has implemented the Importer Security Filing and Additional Carrier Requirements,²⁶ collectively known as the 10+2 rule, and is using the information to identify high-risk unmanifested containers, CBP has not yet fully incorporated the collected data into its targeting process. In January 2009, CBP implemented the 10+2 rule, which mandates that importers and vessel carriers submit additional cargo information, such as country of origin, to CBP before the cargo is loaded onto a U.S.-bound vessel.²⁷ Collection of the additional cargo information (10 data elements for importers and 2 data elements for vessel carriers) and their incorporation into CBP's Automated Targeting System (ATS)²⁸ are intended to enhance CBP's ability to identify high-risk shipments and prevent the transportation of potential terrorist weapons into the United States via cargo containers. CBP has assessed the submitted 10+2 data elements for risk factors, and according to CBP officials, access to information on stow plans²⁹ has enabled CBP to identify more than 1,000 unmanifested containers—containers that are inherently high risk because their contents are not listed on a ship's manifest. However, although CBP has conducted a preliminary analysis that indicates that the collection of the additional 10+2 data elements could help determine risk earlier in the supply chain, CBP has not yet finalized its national security targeting weight set for identifying high-risk cargo containers or established project time frames and milestones—best practices in project

²⁴ U.S. Customs and Border Protection, *Risk-Based, Layered Approach Supply Chain Security, Fiscal Year 2010 Report to Congress* (Washington D.C., Apr. 13, 2010).

²⁵ GAO-1012.

²⁶ Importer Security Filing and Additional Carrier Requirements, 73 Fed. Reg. 71,730 (Nov. 25, 2008) (to be codified at 19 C.F.R. pts. 4, 12, 18, 101, 103, 113, 122, 123, 141, 143, 149, 178, and 192).

²⁷ Under other requirements that preceded the 10+2 rule, importers are also required to provide customs entry information, and carriers are required to provide cargo manifest information under the 24-hour rule.

²⁸ ATS is a computer model that CBP uses to analyze shipment data for risk factors and target potentially high-risk oceangoing cargo containers for inspection. For more information on ATS, see GAO, *Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System*, GAO-06-591T (Washington, D.C.: Mar. 30, 2006), and GAO-04-557T.

²⁹ Stow plans depict the position of each cargo container on a vessel.

management—for doing so. We recommended that CBP establish milestones and time frames for updating its national security weight set to use 10+2 data in its identification of shipments that could pose a threat to national security. DHS concurred with this recommendation and said it plans to complete its updates to the national security weight set by November 2010. More information on the results of our review can be found in our September 2010 report.³⁰

Container Security Technologies

DHS is testing and evaluating technologies for detecting and reporting intrusions into and tracking the location of cargo containers as they pass through the global supply chain, but it will take time before the evaluations are complete and the technology and implementation challenges are overcome for some of these technologies. In particular, CBP has partnered with DHS's Science and Technology Directorate (S&T) to develop performance standards—requirements that must be met by products to ensure that they will function as intended—for four container security technologies with the goal of having the ability to detect and report intrusion into, and track the movement of cargo containers through the global supply chain. If S&T is able to demonstrate through testing and evaluation that container security technologies exist that can meet CBP's requirements, then it plans to provide performance standards to CBP and DHS's Office of Policy Development to pursue for implementation. From 2004 through 2009, S&T spent over \$60 million and made varying levels of progress on its four container security technology projects. Each of these projects has undergone laboratory testing, but S&T has not yet conducted operational environment testing to ensure that the prototypes will satisfy the requirements so that S&T can provide performance standards to the Office of Policy Development and CBP. Performance standards are expected to be completed for two of the technologies by the end of 2010, but it could take time before they are complete for the other two technologies. More information on the results of our review of container security technologies may be found in our September 2010 report.³¹

Cargo Advanced Automated Radiography System

We also reviewed DHS efforts to improve NII scanning through the cargo advanced automated radiography system (CAARS) program. DHS intended for CAARS to be used by CBP to automatically detect and identify highly shielded nuclear material in vehicles and cargo containers at U.S. ports of entry. However, DHS's Domestic Nuclear Detection Office (DNDO) pursued the acquisition and deployment of CAARS machines without fully understanding that they would not fit within existing primary inspection lanes at CBP ports of entry. This occurred because during the first year or more of the program DNDO and CBP had few discussions about operating requirements at ports of entry. Further, the development of the CAARS algorithms (software)—a key part of the machine needed to identify shielded nuclear materials automatically—did not mature at a rapid enough pace to warrant acquisition and deployment. These factors contributed to DNDO's December 2007 decision to make a "course correction" in the program resulting in cancellation of the acquisition and deployment plans for CAARS. Through this action, DNDO significantly reduced the scope of CAARS to a research and development effort designed to demonstrate the potential capability of the technology. While the development of CAARS-type or other advanced radiography equipment capable of automatic detection of highly shielded nuclear material in cargo containers has been ongoing since 2005, one senior CBP official acknowledged that it is not known when the technology will be sufficiently mature for agencies within DHS, such as CBP, to justify acquiring and deploying it in large numbers. On September 30, 2010, the Director of DNDO announced that DNDO is terminating the CAARS program. However, the technology developed under the CAARS program may be utilized by other programs. More information on the results of our review of CAARS may be found in our September 2010 statement for the record for the Senate Committee on Homeland Security and Governmental Affairs.³²

³⁰GAO, *Supply Chain Security: CBP Has Made Progress in Assisting the Trade Industry in Implementing the New Importer Security Filing Requirements, but Some Challenges Remain*, GAO-10-841 (Washington, D.C.: Sept. 10, 2010).

³¹GAO, *Supply Chain Security: DHS Should Test and Evaluate Container Security Technologies Consistent with All Identified Operational Scenarios to Ensure the Technologies Will Function as Intended*, GAO-10-877 (Washington, D.C.: Sept. 29, 2010).

³²GAO, *Combating Nuclear Smuggling: Inadequate Communication and Oversight Hampered DHS Efforts to Develop an Advanced Radiography System to Detect Nuclear Materials*, GAO-10-1041T (Washington, D.C.: Sept. 15, 2010).

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. KAY BAILEY HUTCHISON TO
STEPHEN L. CALDWELL

Question. Various ports across the Nation have indicated that the port security grant process is confusing, and that the distribution of funds is very slow, with FEMA and the USCG still working on delivering funds from 2007. What insights can GAO offer for a better, and more efficient, way to distribute port security grants, so that our Nation's ports receive funds in a timely manner? GAO has made a number of recommendations to TSA and FEMA to improve the grant process for rail and transit security grants. Do any of those recommendations apply to port security grants? Is the Fiduciary Agent process an effective way to distribute port security grant funds?

While we have not reviewed issues related to the distribution of funding under the PSGP since 2005, and thus cannot offer solutions to current PSGP problems, we reported in our June 2009 report on the TSGP that defining agency roles, tracking grant activity, and distributing funds in a timely manner are important principles of grant management.³³ For example, given that the Federal Emergency Management Agency (FEMA) and Transportation Security Agency (TSA) share responsibility for the TSGP, we recommended that the two agencies define their respective roles and responsibilities for managing the TSGP. Similarly, FEMA and the Coast Guard should define their respective roles and responsibilities for managing the PSGP. We also reported that the systematic collection and tracking of grant activities under the TSGP is essential to effective grant management. At FEMA, the Grants Program Directorate (GPD)—which also oversees the PSGP—is responsible for this record keeping. However, GPD officials reported in March 2010 that the development of an updated grant management system—scheduled for completion in 2011—had been halted because of budget cuts. Last, because of delays that transit agencies experienced in receiving funding, we recommended that TSGP grant management officials establish time frames for making funds available to stakeholders that have had projects approved. Establishing such time frames could help grantees implement projects within the designated performance periods of the grants.

In addition to negotiating, tracking, and distributing funds, the process must also include key internal controls. In its *Guide to Opportunities for Improving Grant Accountability*, the Domestic Working Group reported that internal controls are needed to ensure that funds are properly used and achieve intended results.³⁴ It cites four areas where internal controls are important: (1) preparing policies and procedures before issuing grants, (2) consolidating information systems to assist in managing grants, (3) providing grant management training to staff and grantees, and (4) coordinating programs with similar goals and purposes. Establishing effective internal controls may slow the distribution of grants, as these systems should be in place prior to the grant award. However, the Domestic Working Group reported that inadequate internal controls make it difficult for grant managers to determine whether funds are properly used.

In terms of using a fiduciary agent, until Fiscal Year 2009, TSGP grant funding was first processed through a state administrative agency (SAA). However, the DHS appropriations acts for Fiscal Years 2009 and 2010 required funding to be provided directly to transit agencies.³⁵ We expect to follow up with transit agencies to identify the impacts of this change and determine whether the removal of the fiduciary agent added any efficiencies to the grant process as part of our upcoming review of grant management processes of selected DHS preparedness grant programs, requested by Ranking Member Peter T. King of the House Committee on Homeland Security, and Senator George V. Voinovich of the Senate Committee on Homeland Security and Governmental Affairs.

³³ GAO-09-491.

³⁴ The Domestic Working Group, consisting of 19 Federal, state, and local audit organizations, was formed to identify current and emerging challenges and explore opportunities for greater collaboration within the intergovernmental audit community. The group identified grant accountability as a concern and created a project team to address this concern. The results are presented in the following report: *Domestic Working Group Grant Accountability Project: Guide to Opportunities for Improving Grant Accountability* (Washington, D.C., October 2005).

³⁵ Pub. L. No. 110-329, 122 Stat. 3574, 3671 (2008); Pub. L. No. 111-83, 123 Stat. 2142, 2159 (2009).

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. BILL NELSON TO
STEPHEN L. CALDWELL

Question. Mr. Caldwell, does TSA share the information it gathers in its background investigations for Transportation Worker Identification Cards with state law enforcement entities?

Answer. TSA reports that it does not share the information that it gathers during the background investigations of TWIC applicants with state and local law enforcement entities on a routine basis. Pursuant to MTSA provisions restricting the use of applicant information and the TWIC Privacy Impact Assessment, TSA and the Coast Guard limit their sharing of information on applicants and card holders. MTSA also provides, however, that such information may be shared with other Federal law enforcement agencies. According to TSA officials, on a case-by-case basis, TSA can decide to share information if TSA determines that there is an imminent threat (terrorist or criminal) of loss of life or property. According to TSA officials, in such a situation, TSA would provide only basic information, such as the type of threat, location, and individuals involved, but would likely not provide other information from a person's TWIC application. Additionally, state and local law enforcement entities may contact TSA if they identify criminal use of a TWIC card (*e.g.*, a TWIC card used in commission of a crime, or presentation of a fraudulent TWIC card for entry into the secure area of a MTSA-regulated facility) or to verify the authenticity of a TWIC card.

Additionally, the Coast Guard and TSA have processes in place to share threat information with other Federal law enforcement or terrorism centers. In the event that a TWIC applicant or TWIC cardholder is determined to pose a security threat, Coast Guard and TSA have developed a protocol to ensure effective interagency coordination and timely action to minimize the potential threat and risk to the maritime community associated with these individuals.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. FRANK R. LAUTENBERG TO
STEPHEN L. CALDWELL

Question 1. The Port Authority of New York and New Jersey is unable to move forward on a number of projects to improve the security of the port because of the twenty-five percent cost share requirement for port security grants. It is my understanding that waiving this requirement is a long, arduous process that is rarely successful. What should be done about this cost-share requirement so that it does not impede the security of our ports?

Answer. Matching contributions—also known as cost-share requirements—are a key factor for effective Federal grants for two reasons. First, it is important that Federal dollars are leveraged to ensure that Federal grants supplement stakeholder (whether public or private) spending rather than serve as a substitute for stakeholder spending on grant-funded projects. If a grant program is not designed to encourage supplementation, other stakeholders may rely solely on Federal funds and choose to use their own funds for other purposes, meaning that Federal funds cannot be leveraged to the extent they otherwise could be. We reported in September 2003 that the inclusion of matching requirements is one method through which to encourage supplementation of Federal grants.³⁶ Second, matching requirements are reasonable given that grant benefits can be highly localized. For example, regarding port security grants, we reported in December 2005 that,

“Ports can produce benefits that are public in nature (such as general economic well-being) and distinctly private in nature (such as generating profits for a particular company). The public benefits they produce can also be distinctly local in nature, such as sustaining a high level of economic activity in a particular state or metropolitan area. Thus, state and local governments, like private companies, also have a vested interest in ensuring that their ports can act as efficient conduits of trade and economic activity. Given that homeland security threats can imperil this activity, it can be argued that all of these stakeholders should invest in the continued stability of the port.”³⁷

However, in the December 2005 report, we also recognized the differences of opinion among policymakers regarding the inclusion of matching requirements in Fed-

³⁶ GAO, *Homeland Security: Reforming Federal Grants to Better Meet Outstanding Needs*, GAO-03-1146T (Washington, D.C.: Sept. 3, 2003).

³⁷ GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91 (Washington, D.C.: Dec. 15, 2005).

eral grants. Some might see substitution of Federal funds for local funds as reasonable given differences in fiscal capacity, while others may view homeland security as a shared responsibility. For policymakers who place greater value on reducing the substitution of Federal funds for local funds, strengthening matching requirements offers one option in administering grants. One way to implement this requirement involves using a sliding scale for matching Federal funds depending on the fiscal capacity of the grant applicant. Additionally, the matching requirement under the Fiscal Year 2009 Port Security Grant Program (PSGP) stated that the match may be in the form of cash or in-kind contributions, allowing grant recipients flexibility in meeting this requirement. However, the cost-share requirement was waived for Fiscal Year 2010 port security grants.

Aside from matching requirements, there are other key factors to consider in ensuring an effective grant process, such as efficiency, timeliness, and oversight. For example, the DHS Office of Inspector General reported in March 2010 that DHS has a variety of preparedness grant programs with similar purposes, redundant application processes, and differing program requirements.³⁸ In our June 2009 report on the Transit Security Grant Program (TSGP), we identified problems with grant management and made recommendations related to defining agency roles when more than one agency is involved in the grant program, developing a plan for measuring effectiveness, developing a process to systematically collect data and track grant activities, and communicating the availability of grant funding to transit agencies.³⁹ Lacking these grant management characteristics, the TSGP experienced delays in approving projects and making funds available. As a result, about \$21 million of the \$755 million in awarded funds for Fiscal Years 2006 through 2008 had been expended by transit agencies. At the request of Ranking Member Peter T. King of the House Committee on Homeland Security, and Senator George V. Voinovich of the Senate Committee on Homeland Security and Governmental Affairs, this month we are initiating a review of grant management processes of selected DHS preparedness grant programs.

Question 2. Over a million maritime workers have gone through background checks and obtained TWIC cards, to gain access to secure areas of our ports. The Port Authority of New York/New Jersey is one of the sites testing these TWIC cards. However, this technology has been fraught with challenges and has not been working as intended. How do the challenges with the TWIC program affect the security of our ports?

Answer. In November 2009, we identified several Transportation Worker Identification Credential (TWIC) program challenges.⁴⁰ As noted in the report, the TWIC pilot is currently under way to test the use of TWIC cards with biometric card readers. Specifically, this pilot is intended to test the technology, business processes, and operational impacts of deploying TWIC readers at secure areas of the marine transportation system. As such, the pilot is expected to test the viability of selected biometric card readers for use in reading TWIC cards within the maritime environment. It is also to test the technical aspects of connecting TWIC readers to access control systems. After the pilot has concluded, the results of the pilot are expected to inform the development of the card reader rule requiring the deployment of TWIC readers for use in controlling unescorted access to the secure areas of Maritime Transportation Security Act of 2002 (MTSA)—regulated vessels and facilities.⁴¹ However, as noted in our November 2009 report, shortfalls in TWIC pilot planning have hindered the TSA and the Coast Guard's efforts to ensure that the pilot is broadly representative of deployment conditions and will yield the information needed—such as information on the operational impacts of deploying biometric card readers and their costs—to accurately inform Congress and the card reader rule. For instance, because of schedule constraints, TSA did not conduct its more rigorous laboratory testing of readers to be used at pilot sites prior to testing them at pilot sites as initially planned.

Since we issued our report in November 2009, TSA has received the results of the more rigorous laboratory-based reader durability testing. However, TSA has not shared the information on reader results with pilot participants. According to rep-

³⁸ Department of Homeland Security, Office of Inspector General, *Efficacy of DHS Grant Programs*, OIG-10-69 (Washington, D.C., Mar. 22, 2010).

³⁹ GAO, *Transit Security Grant Program: DHS Allocates Grants Based on Risk, but Its Risk Methodology, Management Controls, and Grant Oversight Can Be Strengthened*, GAO-09-491 (Washington, D.C.: June 8, 2009).

⁴⁰ GAO, *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers*, GAO-10-43 (Washington, D.C.: Nov. 18, 2009).

⁴¹ Pub. L. No. 107-295, 116 Stat. 2064.

representatives of four of the seven pilot participants we met with, not sharing the results of reader testing has limited their ability to acquire the equipment that meets the environmental and durability needs of their port facilities and vessels and has resulted in their expending important port security funds without any assurance that their investment will be fruitful. Further, not all the approaches proposed in the Advanced Notice of Proposed Rule Making for using TWIC cards with readers will utilize the electronic security features on the TWIC card to confirm that the TWIC card is valid and authentic.

We are currently conducting a review of the TWIC program's internal controls related to enrollment, background checks, card production, card activation and issuance, and use. The results of this work, including related covert testing at port facilities, will be published in February 2011.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. AMY KLOBUCHAR TO
STEPHEN L. CALDWELL

Question. As recently as this month, the U.S. Coast Guard estimated that as many as 15 countries are not maintaining effective antiterrorism measures at their port facilities. If foreign ports or facilities fail to maintain these measures, the Coast Guard has the authority to deny entry to vessels arriving from such ports or impose specific conditions on the vessels in order to be allowed entry to the U.S. Can you tell us more about this assessment and what the conditions on the ground are at these ports? How are we working with foreign governments to increase protective measures at their ports? What steps are we taking to address the national sovereignty concerns of nations whose ports are being examined under the International Port Security Program?

There are a variety of reasons and circumstances whereby the Coast Guard deems a country and its ports as not in compliance with international port security standards. In regards to the conditions in countries currently considered not to be maintaining effective antiterrorism measures at their port facilities, the Coast Guard considers this information as sensitive and it therefore cannot be publicly released. However, the Coast Guard told us that its concerns about these countries generally center around the failure of the contracting government to audit the ISPS Code compliance of its port facilities and on the individual port facilities' failure to adequately control access of personnel and cargo. During the assessment the Coast Guard conducts of foreign ports⁴² through its International Port Security Program, Coast Guard officials visit and review the implementation of security measures in foreign ports, examining the physical security measures and access controls at the ports as well as the policies, procedures, and training related to the ISPS Code. Based on its visit and the information provided by the foreign country, the Coast Guard team determines the extent to which the country has substantially implemented the ISPS Code. The Coast Guard team makes a determination that a country has "substantially implemented" the ISPS Code if the team concludes that effective security measures are in place at the ports that meet the requirements of the ISPS Code and the government exercises effective oversight. If the team does not observe these items, the team makes a determination that the country "has not substantially implemented" the ISPS Code. In addition to being an outcome of a country visit, the Coast Guard may also find a country to not have substantially implemented the ISPS Code if it denies access to its ports, it fails to communicate information on its compliance to the Coast Guard or the IMO, or a credible report by another U.S. Government agency or other source finds that substantial security concerns exist.

In cases where a country has been found not to have substantially implemented the ISPS Code, the Coast Guard explains the identified deficiencies and makes recommendations to the country for addressing the deficiencies and provides possible points of contact for assistance to help the country improve. In addition, Coast Guard officials work with the appropriate American embassy to identify other capacity-building resources that might assist the country. As part of the program, the Coast Guard has been collecting and sharing best practices it has observed during its visits with a special emphasis on low-cost security practices or innovative appli-

⁴² While the focus of the program is country based, the implementation status of specific ports or port facilities is considered on a case-by-case basis if the country has not substantially implemented the ISPS Code. In certain cases, a port facility that has implemented the ISPS Code in a country that has not may request that it be considered separately from the country. Requests are handled on a case-by-case basis and are generally limited to only those port facilities critical to maritime trade with the United States based on factors such as the volume and importance of the cargo imported from or exported to that port or port facility.

cations that are easy to implement and do not require a significant financial investment. The Coast Guard shares these best practices with other countries and makes them publicly available through the program's website to assist foreign governments in making improvements in their port security. The Coast Guard team then revisits the country to observe whether identified deficiencies have been addressed. Depending on the progress observed and the cooperation received from the country, the team may decide to continue to work with the country and make a revisit or place conditions on vessels that try to enter U.S. ports after visiting the country's ports. During our review, Coast Guard officials cited their efforts in one Caribbean Basin country as an example of how the Coast Guard works with foreign governments to increase protective measures at their ports. In that case, the Coast Guard initially found that ports in the country were not substantially implementing the ISPS Code. After several rounds of sharing information on security training, discussions of best practices for security exercises, and suggestions for specific physical security improvements, the Coast Guard found that the country had made substantial progress toward implementing the ISPS Code.

In regards to national sovereignty concerns, the Coast Guard is aware of such concerns and has considered ways to address them. The Coast Guard has stated that because of sovereignty concerns and "assessment fatigue," it is becoming increasingly difficult to gain access to countries such as China, Egypt, India, Libya, Russia, and Venezuela for reassessments. During our review, Coast Guard officials stated that an effort was underway to conduct joint visits when possible with other U.S. Government agencies as well as increase the sharing of assessment data among various agencies to reduce the "footprint" of U.S. Government activities in the countries. As another approach, Coast Guard officials stated that they have also considered partnering with other foreign governments and international organizations to complete assessments. However, the Coast Guard has not partnered with any international governments to conduct reassessments because the international community has not developed an approach or methodology as the Coast Guard has for inspecting ports. The Coast Guard has also reported that it works frequently with international organizations such as the Asia Pacific Economic Cooperation (APEC) and the Organization of American States on capacity-building projects and utilizes the information obtained when conducting such actions as part of the assessment process. For example, as part of APEC's Transportation Working Group's maritime expert group security subcommittee, the Coast Guard assisted in creating the Port Security Visit Program and has participated in several of the assessment visits to member economies. In addition, the Coast Guard has conducted joint visits with auditors from the Secretariat of the Pacific Community in Pacific island nations. In the short-term, program officials stated that the best way to mitigate a possible lack of cooperation from sovereign nations is to continue to reach out and diplomatically work with countries. The recently enacted Coast Guard Authorization Act of 2010 now mandates that unless the Coast Guard finds that a port in a foreign country maintains effective antiterrorism measures, that the Coast Guard notify appropriate governmental authorities of the foreign country and allows the imposition of conditions of entry (requiring vessels to take additional security measures) "unless the Coast Guard finds effective anti-terrorism measures in place in foreign ports." In cases where countries still deny the Coast Guard access to their ports, program officials will implement and utilize these provisions as required and work with other Coast Guard programs in the domestic arena—specifically, programs that examine foreign vessels to verify their compliance with ISPS Code requirement—and conduct offshore security boardings of vessels to help limit the access of high-risk vessels to U.S. ports.