S. Hrg. 110–676

ONE YEAR LATER: A PROGRESS REPORT ON THE SECURITY AND ACCOUNTABILITY FOR EVERY (SAFE) PORT ACT

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

OCTOBER 16, 2007

Available via http://www.access.gpo.gov/congress/senate

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

38–849 PDF WASHINGTON : 2009

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan	SUSAN M. COLLINS, Maine
DANIEL K. AKAKA, Hawaii	TED STEVENS, Alaska
THOMAS R. CARPER, Delaware	GEORGE V. VOINOVICH, Ohio
MARK L. PRYOR, Arkansas	NORM COLEMAN, Minnesota
MARY L. LANDRIEU, Louisiana	TOM COBURN, Oklahoma
BARACK OBAMA, Illinois	PETE V. DOMENICI, New Mexico
CLAIRE MCCASKILL, Missouri	JOHN WARNER, Virginia
JON TESTER, Montana	JOHN E. SUNUNU, New Hampshire

MICHAEL L. ALEXANDER, *Staff Director*
JASON M. YANUSSI, *Professional Staff Member*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
ROBERT L. STRAYER, *Minority Director for Homeland Security Affairs*
STEPHEN M. MIDAS, *Minority USCG Detailee*
TRINA DRIESSNACK TYRER, *Chief Clerk*

CONTENTS

WITNESSES

TUESDAY, OCTOBER 16, 2007

ALPHABETICAL LIST OF WITNESSES

APPENDIX

ONE YEAR LATER: A PROGRESS REPORT ON THE SECURITY AND ACCOUNTABILITY FOR EVERY (SAFE) PORT ACT

TUESDAY, OCTOBER 16, 2007

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:02 a.m., in Room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Akaka, Carper, Collins, and Coleman.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. Good morning, and thanks to everyone for coming to our hearing. We are here in our Committee's traditional role of oversight of government to evaluate the state of the Nation's port security 1 year after Congress passed, and the President signed into law, the bipartisan SAFE Port Act. We are here both in terms of our traditional Homeland Security and Governmental Affairs Committee's role of oversight, but also obviously as part of our responsibility to protect the security of the American people here at home.

In that regard, it is very satisfying to be able to say—and I believe our witnesses will corroborate—that implementation of the SAFE Port Act over the past 12 months has brought not just focus and energy to the mission of building a robust security regime domestically and abroad, but also a demonstrable improvement in port security. That is very important to our overall homeland security.

In August, the Government Accountability Office (GAO) rated the progress with which the Department of Homeland Security was fulfilling its core missions. I suppose as the old joke goes, there was bad news and good news here. GAO did report that the Department had made "substantial" progress in just one of the 14 categories they mentioned, though there was some progress in some of the others. But the good news this morning is that the one area in which GAO reported substantial progress was maritime security. And there can be no doubt—there certainly is not in my mind—that the SAFE Port Act contributed to that high ranking. The GAO evaluation was especially good news given the challenges of securing our ports and the critical importance of doing so.

Since aviation security was dramatically improved after September 11, 2001, the experts have told us that terrorists may turn to the more vulnerable maritime sector to smuggle people into the United States or, obviously, to bring weapons into this country. Ninety-five percent of our international trade flows through the ports. In the post-September 11, 2001, era, we must provide sufficient security without interrupting what has been our normal emphasis with regard to the ports, which is the smooth flow of commerce. The GAO report, I think, relieves some of the concerns that we have had about this with regard to the ports. So it is good news.

Now, does this mean we can step back and relax? Obviously not. Twenty-one thousand containers enter American ports every day. We are still physically inspecting just 5 or 6 percent of them, and there are other threats from the sea that we are only beginning to think about. For example, the Department of Homeland Security recently began a pilot project to detect radiation from small vessels entering our vast coastal waters outside of the major flow of commerce through established ports.

From my perspective, I think we have to continue to pay particular attention to five key areas as we go forward from the higher plateau we have achieved for port security to improve our maritime security overall. And, briefly, those five are:

First, the Secure Freight Initiative—the pilot program that was set up at three major foreign ports to test the feasibility of 100-percent scanning of cargo headed for the United States. Now, I want to clarify something because the terminology here can be confusing. I said earlier that only 5 to 6 percent of the containers coming in are inspected. Scanning uses imaging technology to identify the contents of the container. So the goal of the Secure Freight Initiative was to test the feasibility of doing 100-percent imaging of all containers, 100 percent, to identify their contents.

The program was established by legislation, I am proud to say, that emanated from this Committee on which Senator Collins played a leading role. It has been implemented over the past year, and I think we can begin to draw some conclusions about its effectiveness. So today we will want to ask: Are foreign ports capable of this kind of blanket scanning? How is the requirement affecting the flow of commerce and at what cost? What are its limitations? Who conducts the scanning? And what checks are in place to ensure it is, in fact, a secure operation?

Just this August, Congress enacted the second phase of our post-Sepember 11, 2001, reforms, again, based on legislation that we reported out of this Committee. The bill includes a provision calling for 100-percent cargo scanning by 2012, that is, of all cargo. We need to know if we are on the right track to achieve that, and the pilot programs and evaluations required by the SAFE Port Act will certainly help steer the Department toward achieving that goal.

Second, it is time to assess the effectiveness of the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C–TPAT). These two programs were established by the Department of Homeland Security in 2002 to screen—that is, to examine the paperwork describing the cargo—high-risk containers at overseas ports and, in concert with the private sector, to track containers as they traverse the oceans toward our ports. Three years

later, we need to determine whether these two programs have, in fact, helped to ensure the global supply chain is secure and create an expedited shipping process—or so-called GreenLane—into the United States.

Third is the TWIC program, which stands for Transportation Worker Identification Credential—which is critically important to the security of our ports. The development of a Federal credential for all U.S. port workers, which would seem to be a natural, fundamental requirement for security, just as we have tried to impose in other areas of transportation, has been frustrated by technological and logistical problems. Approximately three-quarters of a million port workers need to be credentialed by a September 2008 implementation deadline. So we all want to know if this program, including an adequate appeals process, will be able to process all those individuals by then and still keep our ports running.

Fourth, we need to ensure that we are on schedule to create interagency operations centers at our major ports as required by the SAFE Port Act. These centers are designed to improve the collection and sharing of maritime security information at local ports as well as to coordinate among Federal, State, and local partners. So far, actual centers have been set up in Charleston, South Carolina; San Diego, California; and Miami, Florida; and a virtual center exists at the port of New York. I will report that my staff has toured the operation center in Charleston and was impressed by the information sharing and coordination going on among the Department of Homeland Security personnel, Department of Justice personnel, and State and local officials. But I will have some questions about that program.

Fifth, and finally, I want to draw attention to the work of the Domestic Nuclear Detection Office (DNDO), which was created by President Bush in 2005 and formally authorized by Congress under the SAFE Port Act. DNDO's purpose is a critical one, which is to develop, test, evaluate, and deploy a nuclear radiation detection architecture across this Nation, including at our major ports, in order to prevent the nightmare scenario of a smuggled nuclear or radiobiological device—a so-called dirty bomb. Secretary Chertoff has said that the prevention of a nuclear or dirty bomb detonation is, in his opinion, the Department of Homeland Security's number one priority, which means that successful deployment of the radiation detection monitors must be the single most important immediate task that the Department of Homeland Security has.

We have been conducting, and will continue to conduct, careful oversight of this project because these radiation portal monitors absolutely must work. Success obviously will depend upon the effectiveness of the technology, but DNDO must also work closely with Customs and Border Patrol to ensure that there is a seamless hand-off from one agency to the other.

Bottom line, both the GAO report on maritime security, which had a lot of good news about progress made, and even these five areas in which I and other Members of the Committee will have questions nonetheless showed that there has been an enormous amount of activity that has gone on since September 11, 2001, to secure our ports and the rest of our homeland from a potential terrorist attack. And it is why we say with some confidence that

America is a lot more secure today than it was on September 11, 2001, although we all agree that we are not as secure as we want to be. The fact that there has not been, thank God, another terrorist attack on the United States is, of course, in part good fortune, but it is also because we have raised our guard, both through the Department and through the reform of our national intelligence agencies.

So it is in that combined sense of gratitude and shared understanding that we have a lot of work to do that I welcome the witnesses today, particularly Assistant Secretary Stewart Baker, who has worked very closely with this Committee and who has been a key figure in determining the direction of a number of the port security programs that we will discuss today.

I cannot resist saying, Secretary Baker, that I look forward to the day, hopefully not too far away, when I can greet you as the Under Secretary for Policy, not just the Assistant Secretary. As you know, we remain supportive of the efforts of the Department to elevate your position to that level of Under Secretary, and I will continue to do all I can to assist in that endeavor. Thank you.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman, and thank you for holding this important hearing today.

Just a year ago, the SAFE Port Act was signed into law. As the Chairman indicated, I was the co-author of this legislation, along with the Chairman, Senator Murray, and Senator Coleman, who did extensive work on this issue as well in his capacity as Chairman of the Permanent Subcommittee on Investigations.

This law was a necessary response to our heightened security concerns. As the Chairman indicated, about 95 percent of our foreign trade enters the United States through our seaports, including more than 11 million containers a year. Ports are tempting targets for those trying to move explosives, biological and chemical toxins, radiological and nuclear weapons, or even terrorists themselves into our country. In fact, each of these containers has the potential to be the Trojan Horse of the 21st Century. An attack on one of our ports could cause tremendous loss of life and damage to critical infrastructure. It also could have a devastating effect on our entire economy—disrupting commodity shipments, material for manufacturers, and products headed to market. The SAFE Port Act addresses these vulnerabilities.

Soon after the Act's signing, the Department of Homeland Security began implementing its port security enhancements. The Act strengthened two important programs: The Customs-Trade Partnership Against Terrorism (C–TPAT) program and the Container Security Initiative (CSI).

C–TPAT requires importers to adopt security enhancements in exchange for fewer inspections and, when warranted, prioritized inspections. A recent survey of C–TPAT members demonstrated that after joining the program, they doubled their average expenditures on supply-chain security. This is clear evidence that this program is working.

CSI places U.S. Customs inspectors in foreign ports to target high-risk cargo and to ensure that it is inspected before heading to the United States. In the last year, DHS has continued to expand that program strategically and now has inspectors in 58 foreign ports that account for 85 percent of cargo shipped to the United States.

Here on American soil, DHS also has installed more than 1,000 radiation portal monitors at critical seaports and land ports of entry to detect radiation before containers are allowed to enter the domestic supply chain. As required by the Act, by the end of this year, DHS will scan at least 98 percent of cargo for radiation at our major seaports.

DHS has also established the Secure Freight Initiative to develop and test integrated scanning systems that combine radiation-detection equipment and non-intrusive X-ray machines in seven foreign ports. Three of these ports—in Honduras, Pakistan, and England—will scan 100 percent of their U.S.-bound cargo, which will allow us to evaluate the technological and other challenges. This will fulfill the law's requirement for pilot projects in three foreign ports.

Beyond that statutory requirement, limited operational testing will take place in four other foreign ports. This testing will provide us with important information to help address the technical and logistical challenges associated with larger and more complex ports. Until this technology is proven through these pilot projects, I continue to believe that requiring the scanning of all cargo bound for the United States at every foreign port is misguided. It is contrary to the whole risk-based, layered system of security that was established by the SAFE Port Act, which required a focus on high-risk cargo and implemented a requirement for 100-percent scanning of all cargo designated as high risk.

The SAFE Port Act also authorized $400 million in port security grants for 5 years, totaling $2 billion. As we will hear this morning from Captain Jeff Monroe, the Director of Ports and Transportation in Portland, Maine, this funding has already produced significant improvements to the security of our ports. It is important that Congress took this multi-year approach because it will allow our ports to pursue multi-year security projects.

I am also pleased that DHS met the July deadline for issuing a Strategy for Enhancing International Supply Chain Security. This strategy document addresses all aspects of container security, from the packing at a foreign plant, to the arrival at a U.S. port, to the entrance into the national transportation system, to its destination at a retail business or manufacturing plant.

I am, however, concerned and share the concerns of the Chairman that there is a key aspect missing from this strategy, and that is that it does not detail how the private sector will be involved in responding to and recovering from a port security incident. Since port terminals and the relevant recovery equipment are almost entirely in the hands of the private sector, I believe this is a significant omission.

Another area where I am concerned that DHS has not made the progress we would like is in the area of the TWIC card, as the Chairman has indicated. It is obviously critical that we know who is gaining access to secure areas of our ports, and many deadlines

have been missed with regard to the TWIC program. Ten ports were supposed to be online by July of this year. That deadline obviously has not been met. And the first enrollment center for TWIC cards has only been open today, in Wilmington, Delaware. Although DHS has announced that 12 enrollment centers will be operational this year, the Department will almost certainly miss the January 2008 deadline for TWIC implementation at another 40 ports.

This also raises very practical questions for those serving in the merchant marine, for those working at our ports, as far as how they are going to be able to comply with the mandates in the law requiring their enrollment if DHS does not yet have the infrastructure up and running.

Nevertheless, I certainly agree with the GAO, with the Chairman, and with other experts that the Department has made significant progress in improving security at our Nation's seaports and at foreign ports as well.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins. Thanks for that very thoughtful statement.

I want to thank our colleagues Senator Akaka and Senator Coleman for being here. We will now go to Mr. Baker.

Mr. Baker, thanks for being here. You have had quite a distinguished career in public service, most recently in this position since October 7, 2005. We appreciate that you are here today, and we look forward to your testimony.

TESTIMONY OF HON. STEWART A. BAKER,[1] ASSISTANT SECRETARY FOR POLICY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. BAKER. Thank you, Chairman Lieberman and Ranking Member Collins, Senator Akaka, and Senator Coleman. It really is a pleasure to be here on the anniversary of the SAFE Port Act, particularly because this is an Act that is so typical of this Committee's work—bipartisan, overwhelmingly approved, a doable set of challenging but achievable goals set, and something that we have been implementing with enthusiasm since the SAFE Port Act passed.

Overall, I would say, as the Chairman said, we have done relatively well in implementing the Act, though there are plenty of challenges ahead. By our count, there were over 100 mandates in the SAFE Port Act. Almost 50 of them are now completed, again, by our count. And of the remainder, the overwhelming majority are on track, on schedule, and we expect to be able to complete them.

The kinds of things that we have managed to do, you touched on some of them. The Secure Freight Initiative pilots are up and running, and we are gathering information today about how to actually implement a 100-percent scanning and a 100-percent radiation monitoring check on all of the freight bound for the United States. That is going to teach us a great deal about the much bigger challenge that we have ahead as we expand that to other ports.

[1] The prepared statement of Mr. Baker appears in the Appendix on page 37.

Our foreign port assessments, security assessments, are now being performed on a 2-year schedule. We have caught up and expect to be able to do all of our foreign port assessments on the schedule that the statute mandates. Ninety-eight percent of the containers that now come into our ports will be put through radiation portal monitors. And as Senator Collins said, we have put out a national strategy for the supply chain security, and I will be glad to talk shortly about the resumption of trade protocols.

All that said, there are some challenges that we face and deadlines that we have not met, and I would not want to open this testimony without acknowledging those difficulties. Before I talk about the specifics, I would like to put one image in your head. Imagine the entire Mall from here to the Lincoln Memorial covered in containers two or three stories deep. Every day in this country, we have to fill them all two or three times over and then empty it again and fill it up the next day and empty it again. That is the number of containers that come into the country each day. We have to make sure that those containers continue to flow to meet the essential demands of our commerce. That is the first thing that we have to deal with.

The other two issues that I think have influenced our ability to get done everything that we wanted to get done is the fact that, as I think I said in the testimony, there are a couple of things you cannot rush. Technology, especially if you are trying cutting-edge technology, needs to be implemented step by step, and you have to recognize that from time to time you have to take a step back or two in order to meet the requirements of the technology and to make sure that it actually functions as is necessary, particularly in contexts where people's livelihoods, their ability to meet contracts, depend on the smooth flow of traffic.

And the other thing that cannot be rushed is diplomacy. Not every country puts the same priority we do on checking cargo. Not every participant in the trade has the same enthusiasm for additional security measures that we have. And we need to be able to persuade shippers and importers and foreign governments that it is in their interest to cooperate with our security measures. We have made great progress in doing that, but at every step of the way, we have to make that case, and sometimes it takes longer to make that case than we would like.

Briefly, I will talk about some of the areas where I think we still have work to do. As you said, the Transportation Worker Identification Credential is a very complex undertaking that is behind schedule by some months. It is probably the most sophisticated biometric credential that anyone has tried to introduce in the entire industry. These cards have to be capable of being read not just at one port but at many ports. Unpredictably, people may move from one port to another. They all have to be able to get into the port quickly and smoothly.

We pioneered some standards in constructing the TWIC system, and in a few cases, we pioneered what turned out to be the Beta videotape system, which slowed us down a little, but we are now implementing under a standard that is supported by the National Institute of Standards and Technology and which we think will be a very effective mechanism for identifying people as they enter on

our ports. And as both Senators I think indicated, we have begun enrolling people at the first port of Wilmington today, and we will be moving on to begin enrollment at Corpus Christi and then Baton Rouge, Honolulu, Oakland, Tacoma, Beaumont, and port after port.

We do believe that we can get everyone enrolled by September, and while that will be a challenge, so far things have gone smoothly, and we believe that the system we have in place will produce enrollments and the issuance of cards in that period of time.

We still have work to do to get the readers up and running. We have begun pilots to make sure that those readers are actually functioning in some very demanding environments—New York, Long Beach, Los Angeles. And, again, we are proceeding step by step. In a few cases, we have had to take a step or two back in order to make further progress. But I see no show stoppers in our rollout of TWIC. We may have to slow down if we encounter problems. I am always aware that for three-quarters of a million people or more, the most important thing in their life after their families is getting up and going to work at a port. And we cannot get in the way of their ability to earn a livelihood unless they actually pose a security risk. So we are bearing that in mind. It is a constant concern.

Two other challenges, and, again, you have touched on both of them. Our pilot programs to test 100-percent scanning are up and running. We are learning a lot, and the lessons for that are going to be enormously valuable as we try to meet the statutory requirement of achieving 100-percent scanning.

I, too, am daunted by the prospect of 100-percent scanning in every port. We will pursue that aggressively. It is a statutory mandate, and we believe that we can make a big dent in that and perhaps achieve it if everything goes right. But there are many unknowns there, and our pilots are showing us how complex the challenge is, even as they show us some successes.

And, finally, the container security device issue is something that we are looking at quite closely. We have been slow to release a requirement for the adoption of container security devices, either as a requirement generally or as a requirement for membership in the top tier of C–TPAT. They are a very interesting technology. They tell us something important. They tell us whether the doors have been opened in the traditional way. They do not tell us whether a container's security has been breached because there are many ways to breach the security of the container. But they do tell us when the doors have been opened, and they have value in particular in areas where we know the container was secure at Point A, and it has now been moved to Point B, and we want to know whether the doors have been opened. If there was no reason for those doors to be opened, then the container security device can tell us something very valuable.

We are still trying to determine what part of the trade, what part of the supply chain it makes most sense to use that particular technology in. And we are working on standards and also coming up with scenarios and places where we can test those container security devices. And I expect to have that done in the next few

months so that we can actually begin some testing in the real world of these container security devices.

I want to thank the Committee. All of these challenges are going to be difficult ones, but this is a Committee that has been supportive and understanding as well as demanding as we have tried to meet those requirements. And I look forward to talking to you as we continue to do that.

Chairman LIEBERMAN. Thanks very much, Secretary Baker. We will do 7-minute rounds of questioning.

Let me begin with a baseline question to you and ask for a relatively brief response because you could go on all morning.

We are asking you to do a lot to secure our ports. We are asking private sector participants to spend a lot of money, as has been said this morning, to better secure our ports. Is it worth it? In other words, have we made a correct judgment or is this, as every now and then I hear somebody suggest, an overreaction to September 11, 2001?

Mr. BAKER. I think it has been worth it so far. We faced the prospect on September 12, 2001, that someone who had a nuclear weapon or a serious weapon of any sort could simply use our supply chain to deliver it within a block of where they wanted it to go off and do so from virtually any country in the world.

Chairman LIEBERMAN. Right.

Mr. BAKER. It is very difficult for that to happen. No terrorist organization can have confidence that they can use our supply chain against us now. And that is a very important step forward.

Chairman LIEBERMAN. I appreciate the answer. Of course, I agree with it. And also, as I mentioned in my opening statement, I appreciate that the Department is now beginning to not only think about but deploy detection devices aimed at stopping both terrorists and weapons from coming into areas of our coastal waters that are not really ports. We are blessed with a large country with enormous coastal areas, and so there is a natural way—this is the old question that the 9/11 Commission talked about—a failure of imagination before September 11, 2001, to imagine that people could do this.

So as we close and secure our ports, there is a temptation for a terrorist to try to bring devices in elsewhere. And I appreciate very much that the Department has moved to that area as well.

I want to go to the SAFE Port Act, which, as you have indicated, required the Department to implement a pilot program to scan all cargo containers within a year. Just this past Friday, DHS announced that the Secure Freight Initiative pilot begun last December is now fully operational, scanning 100 percent of the containers at the three main ports selected as required by law. They are Southampton Container Terminal in the United Kingdom, Port Qasim in Pakistan, and Port Cortes in Honduras. I know that you are working on an additional pilot program at four additional ports, though in a more limited capacity.

The initial report to Congress evaluating lessons derived from the pilot program is not due for another 6 months, but I want to ask you this morning if you or the Department has already been able to learn some things from the pilot since the scanning at the three ports has been going on for several weeks now. So that is my

question. What, if anything, can you say are the lessons learned thus far from the pilot?

Mr. BAKER. I would be glad to address that. If you would give me a little bit of time, I can actually do a show-and-tell, because I think one of the most useful things that we have encountered is that we have actually begun to bring back integrated data that pulls together the information that we are getting from the trade about the container and the scan and the radiation portal monitor so that we can display them in one place for analysts to say, looking at this entire package, am I concerned enough to stop them and ask for further security measures. I put up on the easel——

Chairman LIEBERMAN. This was not pre-rehearsed.

Mr. BAKER. No, it was not.

Chairman LIEBERMAN. OK.

Mr. BAKER. But when I saw what we were getting, I said that the Senators would want to see this.

Chairman LIEBERMAN. Are these at terminals at the ports or back here in Washington?

Mr. BAKER. Both.

Chairman LIEBERMAN. Both? Great.

Mr. BAKER. So this is actually what is seen by an analyst here in our National Targeting Center in Virginia for a shipment from Qasim to the United States.[1] And I cannot resist using my laser, but this is the X-ray, the scan of the contents of the container.

Over here you can see the description—you cannot read it, I do not think, but——

Chairman LIEBERMAN. We have copies up here.

Mr. BAKER. OK. So you see that there is a description of the container, it is sheets, and——

Chairman LIEBERMAN. Pillowcases.

Mr. BAKER. Yes. So if we saw one big, large, dark object in the scan, we would say, "Well, that does not look like a sheet or a pillowcase to me." And then below you can see the results of the radiation scan, which does not get above a level that would lead to an alarm. And all of this is available, plus additional information on the additional tabs that you can see along the top here that the analysts can call on to further investigate if there is something that leads them to want to know, Well, what could that object be that I am seeing on the scan?

So it is a very effective IT integration program that is already in operation, and I am actually quite pleased. IT integration always sounds like a great idea, and it often is much harder to do than you expect. And the fact that we have been able to do it as quickly as this I think makes us feel more comfortable about our ability to do this more generally as we move to broader scanning. There are other successes. I think traffic is moving fairly well, but I would suggest that we wait until we have had a longer period of evaluation to say that we think we can move the traffic smoothly.

Chairman LIEBERMAN. Thus far, any unexpected advantages or unanticipated negative consequences or challenges?

Mr. BAKER. One of the interesting questions is how do people who are actually shipping goods feel about this, and I think very

[1] The poster referenced by Mr. Baker appears in the Appendix on page 106.

early reads suggest a wide variety of reactions. In Pakistan, there are apparently shippers who prefer now to ship from Qasim, where we have this facility, as a way of reducing the likelihood that they will be stopped in the United States. But in Cortes, we have heard reports that some people are moving their shipment to other ports because there is a charge that goes with this and they want to avoid the charge. So I think that suggests that this is going to be a very complex set of effects when we begin rolling this out more broadly.

Chairman LIEBERMAN. Thanks. My time is up. Senator Collins.

Senator COLLINS. Thank you.

Secretary Baker, I want to follow up on the issues with the TWIC card. In his testimony later this morning, Captain Monroe, the Director of Ports for Portland, Maine, will make the point that the aviation system was able to clear and credential hundreds of thousands of workers in a relatively short time. And that was a point that was made to me by a group of airport directors from around the country.

Now it appears that we are going to two separate systems for aviation versus our ports, and 6 years after the attacks on our country, in contrast to the aviation system, we still do not have the TWIC card in place.

Why not look at piggybacking onto the system that has been used successfully by our airports? And why not have one system so that individuals do not have to get multiple credentials?

Mr. BAKER. I think those are fair observations, and we have looked at the possibility and I think will look if we run into trouble again at the possibility of changing our approach now.

Our general belief in this circumstance has been that, first, the amount of cross traffic between the airports and ports has been relatively limited. The port problem turns out to be much more complicated in many respects than the airport problem because in most cases airport workers work at one airport, whereas with ports you have truck drivers, in particular, and sometimes longshoremen who will move from port to port, who will do work at different ports, and who need to be credentialed to what amount to very decentralized systems. One port does not have to have an infrastructure connection to another port. But we need to be able to credential people in ways that allow them to be admitted to one port relatively easily if they happen to move from another.

That has accounted for some of the differences in approach and, I have to say, some of the complexity of the credentialing task—that plus the fact that we are doing a fairly elaborate set of biometrics in an environment that is less controlled and more hostile. There is more humidity and more salt in the air at our ports, and we are trying to get more people through with many fewer of our white-collar workers than in an airport context.

I think those account for the differences. That is not to say that in the long run we would not want to bring the programs closer together, or if we have bad luck with the program, which we currently believe is on track, we would go back and look at it. But at this point, we have a rollout strategy. We have a set of technology standards. People are enrolling and building the cards. I think it would set us back if we tried to switch gears again.

Senator COLLINS. I am very concerned not only about the homeland security aspects of dangerous materials coming into this country, but also about the impact on consumers. All of us are very aware of the recalls of dangerous toys from China and other products that have made the news recently. And it seems to me that the Department of Homeland Security has an important role to play in protecting consumers from dangerous products as well as protecting all citizens from possible terrorist attacks.

For more than a year, the Department has stated its intention to issue a rule that would require importers to provide additional information before products are loaded onto vessels overseas. And DHS already uses some of that information as part of its automated targeting system. But one of the pieces of information that would be required under the proposed rule is the manufacturer's name and address, and I am concerned about the vulnerability posed by the delay in requiring that information, not only because of its impact for helping you to target high-risk cargo, but also because it would allow Customs and Border Protection to target untested manufacturers who may be shipping potentially dangerous consumer products, including children's toys. It would allow CBP to do additional safety screening if it knew that it was dealing with either unknown manufacturers that are not trusted yet or those with a history of violations.

Could you tell the Committee when you expect that this rule, which is referred to as the "Advanced Trade Data Element Rule," which will require more information about the manufacturer, will be published?

Mr. BAKER. Thank you, Senator. Let me start by saying I completely agree with you about the importance of this rule. It is a valuable part of our effort to push our borders out and to try to catch suspect cargo before it gets close to our ports. And having this kind of information, some of which we get now but which we are not guaranteed to get, in a way we can count on is an enormously valuable part of our strategy.

At the same time, it is a new regulatory burden on importers and shippers, and it requires them to make changes in their information technology systems and to get the information to us. And so as I said at the start, it is important for us to do our diplomacy and to make sure that we have persuaded people that this is a reasonable requirement. We have been working with the trade for some time, and I think that generally the trade has acknowledged that of all of the security measures that we are working on now, this is probably the least expensive and the most valuable to us. We currently expect to get that rule to the Office of Management and Budget within 2 weeks. That is our target. It is one of our top 10 priority regulations to get done in the next year because of its value for a screening program that will allow us to do 100-percent screening in an effective way.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins. Senator Akaka.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman. I want to commend you and the Ranking Member for working to improve our

port security in our country and in other countries as well. I cannot emphasize enough that Hawaii's port system is critical to the economic life and health of my State, as you know. We depend entirely on the ocean shipping industry to import essential commodities. Any interruption in commerce, of course, would certainly hurt Hawaii. So I welcome this opportunity to hear your testimony and to ask you questions about our port security act.

Mr. Baker, we have heard today about the progress made by DHS in implementation of provisions of the SAFE Port Act. Last week, the Commerce Committee heard similar things. However, I am concerned that a number of important policy issues have not been adequately discussed or decided yet. These policy issues have held up progress in many fronts, and I am glad you mentioned the workforce.

With regard to TWIC, it is my understanding that the manufacturers of card readers do not have access to actual TWIC cards. They will only be available to maritime industry employees. If they do not have access to those cards, they clearly cannot test the readers.

Mr. Baker, will DHS make TWIC cards available to the card reader manufacturers so that they can properly implement their testing?

Mr. BAKER. I am not familiar with that concern, but I frankly share your puzzlement. We are in the process of enrolling people today. We will then begin issuing cards very shortly thereafter so that there will be cards available to workers within a month. And there should not be any reason why we cannot test the readers with real cards.

So I am not familiar with any reports that would suggest that the reader manufacturers are not able to test the cards now because the cards are going to be in production momentarily.

Senator AKAKA. I see. And the importance of that, of course, is the Transportation Worker Identification Credentials.

Mr. BAKER. Absolutely.

Senator AKAKA. An important issue is whether or not the Coast Guard also, Mr. Baker, will require a 100-percent biometric identification rate. Many in the industry have emphasized the need to use biometric identification all the time because if someone loses his or her TWIC card, anyone can pick it up and use it since there will no longer be guards physically present to verify the picture or the card. Right now, the Coast Guard policy is to use biometric identification only at high-risk ports or when there is an elevated MARSEC level. In addition, these systems are also costly to the ports. If they are not used 100 percent of the time, it would be difficult for the ports to justify spending the money to build the infrastructure when they could be using it for something else.

So can you tell me the rationale for not using biometric identification 100 percent of the time?

Mr. BAKER. We certainly have designed the cards so that biometrics are the standard, and it is possible to use the cards with a biometric at all times. And it would be my expectation that would be the norm. I am always wary of saying anything will be 100 percent because you have to account for unusual circumstances, and, again, we do not want to be in a position of saying no one works

today because the biometric system is down, particularly if you have got back-ups that include such things as PIN numbers that would allow people to verify that they actually have unique knowledge that cannot be obtained by someone just picking up a card on the ground.

So I am cautious about saying it should be 100 percent, but it is our expectation that the norm will be biometrics.

Senator AKAKA. An outstanding policy that DHS has not yet made is related to the use of positive access control. The use of positive access control could have implications for the cruise industry as well, a big part of Hawaii's tourism sector. Cruise terminal porters must move passengers' bags in and out of secured areas quickly. The need to scan them into and out of secured areas could impact how quickly and how efficiently they can do their jobs. In fact, the aviation industry, also a very high-risk transportation sector, does not require positive access control. Instead, they use a visual challenge program instead.

With this in mind, Mr. Baker, when do you expect DHS to make a decision regarding the use of positive access control at the ports?

Mr. BAKER. Well, I think this ties back to my earlier suggestion that it is always dangerous to say this will be 100 percent. There may well be circumstances where you need to be able to make an accommodation so that people can move quickly back and forth across the line and not have to stop and do the biometrics at every stage. We would not say we have rejected that out of hand. There may be circumstances where that will be necessary to do. But I do not want to prejudge that. That is the sort of thing that ought to be decided with the captain of the port as part of a security plan for the entire port.

Senator AKAKA. You mentioned that on scanning containers you have already come to 98 percent. What is the 2 percent?

Mr. BAKER. The 2 percent, generally, is ports that are so small that containers rarely come through and it does not make sense to have a portal sitting there like the Maytag repairman waiting for somebody to go through.

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

Chairman LIEBERMAN. Thanks, Senator Akaka. And, of course, that 98 percent is for radiation.

Mr. BAKER. It is.

Chairman LIEBERMAN. Right. Senator Coleman.

OPENING STATEMENT OF SENATOR COLEMAN

Senator COLEMAN. Thank you, Mr. Chairman, and I would also like to associate myself with the preliminary comments of the Ranking Member, particularly in regard to the pilot programs and the prospect of 100-percent screening. We all want to get there. We want to get a system that works. I think as you said, you cannot rush implementation and new technology. We need to rush, but it does need to work. I am very interested in looking at the results from the pilot projects, but I just want to put myself on record as being in accord with the Ranking Member.

On the pilot programs, have we been experiencing any bottlenecks, any slow-ups in any of what we have seen to date?

Mr. BAKER. In general, we have not had too many slow-ups. We have had weather-related surprises. It gets very hot in Pakistan, well over 110 degrees, and that has caused some surprises with the gear. We have had cloudbursts in Honduras that have caused difficulties with the scanning machines. So we have certainly had surprises. But on the whole, the layouts, while they have been different in every port, have allowed us to move people pretty well.

Senator COLEMAN. Do you anticipate if we move to higher-volume ports that we would have the same kind of results on the issues here?

Mr. BAKER. No. As people in the Coast Guard keep reminding me, if you have seen one port, you have seen one port. [Laughter.]

The layouts are completely different at every one of these ports, and how they have squeezed in all of the equipment varies from place to place. And in some cases, it is an elaborate ballet that you have to perform to get your goods through the lanes.

As soon as you go from one lane to multiple lanes—and some of the ports have 40 or more lanes—it becomes much more complex to do the scanning and the portal monitor checks. And even more difficult is transshipment because in some cases you have cranes just picking the container up and moving it directly from one ship to another. It is not clear where you are going to do your scanning and your screening on those containers.

So I think we are going to encounter a lot of complexity as we move to bigger ports, and we are trying one lane in a few of these big, complex ports, but trying to move to a full coverage for a port like Hong Kong is going to be very difficult.

Senator COLEMAN. I believe the original ISIS program in Hong Kong had a very small number of lanes.

Mr. BAKER. Yes, that is correct. And, again, in Hong Kong, to show you the sorts of surprises you can encounter, we discovered the cement that they were using to pave the port gave off enough natural radiation that it was setting off the alarm regularly. So there are 100 problems that we will have to solve port by port.

Senator COLEMAN. I would like at some point to discuss this further, but are there technological bases that you need, infrastructure bases? I want to get an overall sense as you go beyond the pilot project and kind of analyze that and understand what we have to deal with.

Talking about technology changes. I saw this technology a number of years ago, and it moves quickly. How adaptable are the pilots that we have and as we look to the future to ship with new technology? Or are we wedded to a particular technology? Are we open to technological shifts? And how easily can they be accommodated?

Mr. BAKER. I think we have tried to build that in. And, of course, you never know for sure, but we have tried to build in the possibility of changes in the technology. For example, the radiation portal monitors that we have used abroad have been relatively undiscriminating in the kinds of radiation that they detect. And there is a second generation that is much better at identifying the kinds of radiation we are most worried about. We can install that in general in places that currently use the old technology, or we can add it as an add-on for particular checks.

The scanning equipment, I would say the most promising new technologies there are in software that can identify anomalies, and then, again, I think we can use the existing infrastructure and then just make the software better.

Senator COLEMAN. I want to get to a micro focus on the TWIC issue, but just one other question. Does the scanning help us to identify whether there are shielded materials? The concern I have with some of the radiological materials, if they are shielded, even the best equipment we have does not have the capacity to detect that, at least as I understand it.

Mr. BAKER. The equipment that would say is there radiation coming from this container, no, it can be shielded so that you cannot do that. But then that picture that we are looking at here, there would be a big black spot. And so the combination——

Senator COLEMAN. The combined systems give us an edge that we have not had before. The TWIC program, I was talking to a fishing guide in northern Minnesota; they need TWIC cards. Here we are talking about implementing a system, and this is a guy that is taking vacationers to fish for walleye up in Warroad, Minnesota. I also talk to barge operators talking about the size of their operations and some of the issues that they have—student workers who work for 2 or 3 months, and it takes 2 or 3 months to get a card. Clearly, we are looking at the major ports.

Can you talk a little bit about how we do not get bogged down in dealing with small-boat operators, the tugboat industry, and student workers? Is somebody working on that stuff?

Mr. BAKER. Yes. Obviously, our biggest job is to get the people who regularly work there through the process, and that is a big job and takes time. Once we are there, we are only talking about the new hires that have to go through the process, and there is nothing about the process that inherently takes months. We are giving people months now because it is a big new job for everybody to line up and enroll. We can do this much more quickly for new hires once we are through with the great bulk of the work.

There is a hard line that you have to draw. People who only occasionally come on to a port can be escorted by someone with a TWIC card, and I do not think that will change. Is there going to be a class of people who say, "I want to be able to go regularly on the port, but I do not want to have to"——

Senator COLEMAN. If I may interrupt, the problem is we have an image of a port, the port of L.A., or the port of New York. If you are a guide in Minnesota, technically we have international borders there, but there really is not a port. You are taking a fishing boat out of a dock and taking somebody fishing, and you have to have a TWIC card.

Mr. BAKER. That is a fair question, and let me look at that. I am not familiar with how far down we go in our definition of "port." I cannot believe we cover canoes, but——

Senator COLEMAN. You just may, is the concern. I can tell you that for these folks, they are going to travel a couple of hours to Duluth to the main area to go pick up a card to be able to take somebody fishing on a lake between Minnesota and Canada. Big Government sometimes forgets about the impact on that little guy, and we talk to those little guys.

Mr. BAKER. I appreciate your bringing that to my attention. Let me take a look at that.

Senator COLEMAN. Thank you, Mr. Secretary.

Chairman LIEBERMAN. Thanks, Secretary Baker. I have a lot more questions I would like to ask. I think I would like to ask one more and submit the rest to you in writing.

I wanted to ask you to talk a little bit more about the Domestic Nuclear Detection Office, to which, as I said earlier, Secretary Chertoff gives great priority, and I agree with him, and just to point out this is a detection program of nuclear devices coming into America by terrorists, potentially, that goes beyond the ports, but the ports are involved.

First, I know you are testing the technology. How soon do you think you will be able to report to Congress on how that is going? Second, this has to involve integration of different organizations, some that protect land entrance, some Federal agencies that take care of the ports, and then obviously if we are looking at major cities, for instance, we will be dealing with State and local law enforcers. So if you could give a short answer to both parts of that question.

Mr. BAKER. OK. First, I would like to say the same thing that the Secretary has said. This is one of our worst nightmares. DNDO has been enormously effective in identifying that as the problem and asking how are our solutions. And as you said, we have a number of solutions in place for containers and commercial shipping, and that ought to then be the benchmark in which we say do we have the same level of protection for small boats, for general aviation, for all the other ways in which terrorists might bring nuclear weapons into the country. And DNDO, with its focus, has been single-minded in asking questions that do not fall into one organizational responsibility to say, OK, well, let us think like a terrorist: What is our response? How do we prevent people from bringing it in this way or that way? So they have been enormously helpful in broadening out the focus of our components.

They have been doing testing, as you know, already, and we are about to begin actual testing in place. So I do not know what our current schedule is for getting you a report on the actual implementation testing. But I will get you an answer to that in writing.

Chairman LIEBERMAN. Fine.

Mr. BAKER. Organizationally, as I say, I think their focus has been research, procurement, and making sure people are thinking about the threat in a coherent way. And in all those respects, they have done an excellent job.

Chairman LIEBERMAN. And you believe that they are integrating the different agencies that have overlapping responsibility?

Mr. BAKER. Yes. For example, in some of our general aviation work and in our small boats initiatives, in both cases they were able to bring together TSA, CBP, and Coast Guard initiatives to say how do we build the best possible defenses against a nuclear weapon, and no one agency could have done that.

Chairman LIEBERMAN. Fine. When you get back to us with the information about the test data, obviously part of it is when the GAO can begin to review it on our behalf. Thanks very much.

ANSWER FROM MR. BAKER TO THE FOLLOWING QUESTION FROM SENATOR LIEBERMAN

Question: Regarding DNDO testing of nuclear detection capability, what is the schedule for getting Congress a report on how the testing is progressing?

Answer: On May 25, 2007, DNDO briefed your office on the classified results of the ASP Phase 1 testing. The Phase 3 Test Report, which will also be classified, is currently in final review within the Department, and the Blind Test Report is presently being prepared. DNDO would be happy to provide you with a status briefing on how the testing is progressing.

Senator LIEBERMAN. Senator Collins.

Senator COLLINS. Thank you. Secretary Baker, one of the most important provisions of the SAFE Port Act required the Department to develop protocols and a plan for restarting our ports in the event of an incident. We know from the West Coast dock strike of a few years back, which was an event that was both peaceful and anticipated, that the closure of ports can have enormous economic consequences. And if there were an attack on one of our ports, most likely for a time all ports would be shut down. And that is why we felt so strongly that we needed to have the Department engage in this plan, and the Department has done so.

But as I referred to in my opening statement, the private sector entities have come to us to express concerns that there is not sufficient detail in the plan about the role that would be played by port authorities, by first responders, by those in the private sector, which, after all, own most of the emergency equipment as well as control our ports.

What is the Department doing, having made a good first step in this area, to fill in the gaps and come up with a strategy that will ensure that we have a safe, logical, planned procedure for reopening our parts in the event of an attack?

Mr. BAKER. That is an excellent question, and we are quite aware of the concern on the part of the trade about this. A couple of basic principles I think have governed what we have done so far, and we are at work on some more detailed documents that will give some further guidance.

First, we do not want to do what the private trade should do. We are not going to be telling people, well go to this port, go to that port. In most circumstances, they have dispatchers who are much more capable of making those judgments than the government.

The second principle I would say is that we have to be flexible about our plan, and here I think there is some inevitable frustration on the part of the trade. They would like nothing better than a guarantee that says within 3 days, if you are not the port that is attacked and you meet certain criteria, we will let you in without any change in procedures. The difficulty with that is that we do not know what kind of attack we are going to be recovering from, and if it is a simple explosion in a container, that is a different sort of attack than a nuclear weapon found in a container, or a biological weapon. So we cannot know for sure how we will reconstitute trade until we know what we are reconstituting from. So we cannot give them guarantees.

We do think that—and this is what we are working on now—a critical element is for everyone in the trade to know what the communication chain is going to look like, that we will be reaching out and getting information from them about what they're experiencing

as they try to make deliveries, and to give them all the guidance that we can to make sure that everyone gets news as quickly as possible about what we can say. If we can say certain ports are open and we are accepting cargo in those ports, then everyone should get that information quickly. If we are restricting certain kinds of cargo or cargo from certain destinations, then we need to get that information out.

So what we will be building as a resumption of trade protocol will focus on the communications lines and some basic principles of the sort that I have been talking about. I hope that will make the trade more comfortable, but I think there is probably an inevitable divergence because the trade would like guarantees that we cannot responsibly give to them.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thank you, Senator Collins. Senator Coleman.

Senator COLEMAN. Thank you, Mr. Chairman.

A lot of stuff comes into this country in a non-containerized form: Automobiles, petroleum products, and dry bulk goods. Is CBP considering a CSI-like program for non-containerized forms of maritime cargo?

Mr. BAKER. We have a variety of programs for those products. It is harder to have a single program because it varies so much. If it is scrap steel, it has one profile, and if it is petroleum, it is a completely different profile. And so we have had to work individually with shippers of particular products to determine that the supply chain is such that we are comfortable with it.

It is a little less likely that someone would sneak a weapon into some of these shipments, but you cannot rule it out for certain kinds of shipments where the handling is gentle enough that a weapon could reasonably be expected to get through. But with those sorts of products, we have to very substantially vary our security measures according to the nature of the cargo.

Senator COLEMAN. I appreciate it. Thank you, Mr. Secretary.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Coleman.

Secretary Baker, thanks for your testimony. Very thoughtful. I always have the feeling when I hear you again this morning that you are on top of things, and just hearing the way in which we are talking about some of these scenarios, including the discussion of potential nuclear attack on the United States via weapons smuggled in by terrorists, it is unsettling, of course, in one sense. It also, I think, reassures us that people in important positions like your own are not going to be guilty of another failure of imagination. That is, to imagine the extremes that our enemies might go to inflict damage on us personally and our country.

So I thank you for that. This is, as I say, good news. We appreciate what you have done so far. We are going to keep the pressure on. Most of all, we all have a common interest in seeing this work, and it is in that spirit that this Committee looks forward to continuing to work with you and everybody at the Department of Homeland Security. Thank you very much.

Mr. BAKER. Thank you.

Chairman LIEBERMAN. The second panel, please. As you are coming up, I will introduce the panel members. We have two representatives from other offices of the Federal Government and a representative of local government.

Reginald Lloyd is the U.S. Attorney for the District of South Carolina, whose office has been charged with coordinating the efforts at Project SeaHawk at the Port of Charleston, South Carolina.

Stephen Caldwell is the Director of Homeland Security and Justice Issues at the Government Accountability Office, and he has been responsible for conducting reviews of virtually every port security program the Department of Homeland Security has implemented. His work has been very important to this Committee.

Captain Jeffrey Monroe is the Director of the Department of Ports and Transportation of the city of Portland, Maine. He has had a long and distinguished academic and professional career in the maritime and transportation sectors.

We are grateful that you are all here. We look forward to your testimony now. I want to tell you, Mr. Lloyd, that I am sure I speak for Senator Collins and Senator Coleman, we know you have a big job being U.S. Attorney in South Carolina where Lindsey Graham resides, but we feel that you can take care of that and handle that effectively.

To become more serious, he is our good friend and has a good sense of humor and shares our interest in homeland security.

We welcome your testimony at this time. Mr. Lloyd.

TESTIMONY OF REGINALD I. LLOYD,[1] U.S. ATTORNEY, DISTRICT OF SOUTH CAROLINA, U.S. DEPARTMENT OF JUSTICE

Mr. LLOYD. Thank you. Mr. Chairman, Ranking Member Collins, Senator Coleman, Members of the Committee, it is an honor to appear before you today to talk about a port security initiative in Charleston, South Carolina, called "SeaHawk."

When I first became U.S. Attorney in South Carolina and learned about SeaHawk, the first question that I kept asking was: What value does SeaHawk bring to the port that did not exist before? What I learned is that while each Federal agency responsible for maritime security has a core mission at the port, there is no national standard to coordinate resources, operations, or intelligence with Federal agencies or with our State and local jurisdictions. This leads to potential gaps that may be exploitable by criminals or extremists. SeaHawk seeks to seal the seams between Federal, State, and local port security activities. It does not replace the good work of the Federal agencies at the port. Rather, it enhances their missions by integrating them through co-location, unity of command, innovative development of technology, and information sharing.

I am proud to tell you, Members of the Committee, that since its establishment, Project SeaHawk has achieved many of its goals and objectives. We have established a full-time, multi-agency, co-located task force of Federal, State, and local law enforcement using a Unified Command structure for decisionmaking that helps

[1] The prepared statement of Mr. Lloyd appears in the Appendix on page 46.

to promote cooperation and enhance information sharing and investigative resources.

We have developed an intelligence section to provide support to law enforcement operations and investigations. We have created an Operations Center that provides situational awareness and resource coordination. We have developed and integrated and linked radiological detection and monitoring architecture. And we operate a proactive security mission to identify and deter criminal or extremist-related illicit activities.

None of these accomplishments would have happened without the strong partnerships established among the agencies that secure our maritime borders. Full-time commitments to SeaHawk have been made from the U.S. Coast Guard, Customs and Border Protection, Immigration and Customs Enforcement, Defense Criminal Investigative Service, the South Carolina Law Enforcement Division, and every State and local municipality around the port.

SeaHawk's mission is enhanced by its co-location and strong relationship with the FBI's Joint Terrorism Task Force, as well as its integration with our South Carolina Fusion Center. We operate through a Unified Command structure where each agency brings unique resources that support SeaHawk's operations. We also created a SeaHawk Executive Steering Committee to focus on long-term strategic goals that includes myself, the captain of the port, the port's director, the chief of our State Law Enforcement Division, the FBI SAC, the resident ASAC for ICE, the Transportation Security Administration's Federal Security Director, and all of the sheriffs and chiefs of police who have personnel dedicated to SeaHawk.

One of the challenges was to create a screening process that would help the Unified Command to make decisions and allocate resources. This has been addressed through the development of a data capture process in which maritime information is collected and filtered through a data logic model comprised of a variety of indicators of suspect activity. Federal agents are augmented with task force officers from all of the surrounding local municipalities and jurisdictions. The real value of SeaHawk is the ability to pool limited resources and then apply them against a risk-based ranking of all identified security issues.

The SeaHawk intelligence team screens all vessels and crew bound to the Port of Charleston and provides the results to the Unified Command on a daily basis so they can plan their actions. The intelligence team also provides information and analysis on the global war on terrorism and its specific implications to South Carolina.

SeaHawk has an Operations Center that serves as a central hub for the South Carolina ports. Ships are followed with radar and video as they enter and leave the harbor area. This allows SeaHawk to keep apprised of ongoing events that may affect the security of the port.

SeaHawk has used its resources to improve capabilities across four broad areas, including voice and data communications, law enforcement investigative and intelligence tools, information technology, and sensor programs. One cutting-edge program is a mobile

radiological detection program that deploys a sensitive radiological sensor in a vehicle and a boat.

Project SeaHawk, Mr. Chairman and Ranking Member Collins, is truly a successful example of Federal, State, and local agencies working together very effectively to secure the ports of South Carolina and to serve as a national model of innovation to enhance our Nation's port security.

I want to thank you very much for inviting me here today to participate in this discussion with you, and I am very happy to answer any questions you may have.

Chairman LIEBERMAN. Thanks very much, Mr. Lloyd, for that excellent testimony. I appreciate the question with which you started, which was is this going to add anything to the status quo, and I am encouraged by your answer, which is that it has.

Mr. Caldwell, thanks for being here. I just want to repeat that you have been really invaluable to this Committee in our oversight responsibilities, and I thank you for everything you have done and welcome you this morning.

TESTIMONY OF STEPHEN L. CALDWELL,[1] DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. CALDWELL. Thank you very much, Chairman Lieberman and Senator Collins, and thank you for inviting me to speak on this important topic of the SAFE Port Act. Given the breadth of the Act and the already lengthy written statement that I submitted, as well as some of the comments by other witnesses, I will focus my comments on container security because that has come up again and again in the hearing.

To some extent, the supply chain programs that we have are at a crossroads, and I will get to that at the end. As you know, we currently have a layered strategy of various different programs to provide supply chain security. These are run by CBP as well as other agencies, both within DHS and other departments such as DOE. These include things we have already talked about: The 24-hour rule, ATS, inspections at domestic ports, radiation screening at domestic ports, CSI, Megaports, and C–TPAT. And as we have noted in our reports, a lot of progress has been made. We were very happy that a lot of the recommendations that we had made to DHS and its components had been incorporated into the SAFE Port Act, and DHS has made progress in implementing many of these. Some examples include improved strategic planning and better utilization of human capital.

Despite the progress made, we still are reviewing two of the programs right now for this Committee, both CSI and C–TPAT, and we will be providing you more details on that early next year with our full reports. But some of our preliminary findings are in the written statement that I provided.

One area where CBP is still challenged is the area of actually measuring outcomes as opposed to activities. This is a problem that is endemic to any agency involved in homeland security. But that

[1] The prepared statement of Mr. Caldwell appears in the Appendix on page 53.

is an area where we are still hoping they can make some more progress.

Perhaps one of the most important areas of progress in supply chain security are the partnerships that CBP has formed. Assistant Secretary Baker also emphasized this point in his statement—at least his written statement—and the partnerships are with many groups, but there are at least three groups that I want to emphasize.

First, the partnerships are with foreign nations. These are the nations that have agreed to be our partners in CSI or are negotiating with us on "mutual recognition," which I will get to later.

Second, there have been partnerships with the private sector. Companies have decided to join C–TPAT, provide information on their security, obviously provide resources, as was mentioned, to provide for their security. And CBP is also consulting with COAC, ISO, and other private groups.

The third partnership I would like to mention is with international and regional organizations. There has been an international framework developed with U.S. participation and leadership called the "Safe Framework" by the World Customs Organization. In addition, there are a couple of joint cooperation forums now with both the European Union and with APEC.

As one indication of the progress of these partnerships, other nations and international organizations have adopted programs that are very similar to CSI and C–TPAT. These partnerships are critical because, as we know, the Federal Government cannot do it all by itself. To push out our security envelope and to deal with things that are nongovernmental, we need to reach out to others and develop good relationships with these partners. But there are some signs that some of these critical partnerships are starting to fray. As I said, these critical relationships are partnerships, so other nations have volunteered to join CSI. The United States worked through international organizations. Companies decided to volunteer to join the C–TPAT program or, in some cases, to go beyond that and to meet ISO standards. In summary, our partners decided to be our partners. It was a mutually beneficial relationship.

Now, CBP, somewhat on its own initiative and somewhat mandated by legislation, is adding or proposing new layers to this layered strategy. These include container security devices, "Ten Plus Two" data requirements, the Global Information Exchange, the Secure Freight Initiative, and 100-percent scanning. In some cases these are voluntary, and in some cases they are not. But some of our partners are starting to ask: Does the United States have a layered strategy or a strategy of layers, with new layers being added continually and unilaterally? In the meantime, foreign nations and private company partners are asking what is in it for them. Where is the promised green lane that is talked about in concept but is not really implemented in a way that can be determined?

Foreign governments are certainly willing to help us in terms of scanning things overseas as part of CSI, but they do want some assurances that these containers will not be scanned one or more times when they get to the United States. And private companies have increased their resources to improve security, but again, they

are hoping to get some benefit in terms of expedited scrutiny of their shipments.

One of the biggest concerns of these partners at large is the 100-percent scanning of all U.S.-bound containers. This Committee, as well as DHS, has received letters from these partners expressing some of their concerns about this new requirement. While we have not done a detailed review of SFI—it only went operational 3 days ago, according to the Assistant Secretary's statement—we have visited two of the pilot ports as they were getting ready for SFI. The topics of 100-percent scanning and SFI came up frequently in the discussions that we had with foreign governments.

Based on these discussions, we have identified six challenges involved in the 100-percent scanning requirement. Assistant Secretary Baker already previewed some of these challenges in his statement where he noted that neither technology nor diplomacy reacts well to being rushed.

The first challenge is that the 100-percent scanning approach is counter to the risk management approach that GAO has pushed, Congress has pushed, the 9/11 Commission has pushed, and CBP has really incorporated into almost all of the other programs that it has and the United States has agreed to in the World Customs Organization SAFE Framework. This is our largest concern because the 100-percent scanning in some ways could reduce our security rather than enhance it.

The reason a risk management approach is important is that it forces you to prioritize your limited resources. If you are focusing attention on all of the containers, you are not focusing your attention on any one container.

Here are the remainders of some of the challenges we have identified, and I will just summarize these briefly because we have more details in our report. The second challenge is that the United States could probably not reciprocate if other countries adopted the same requirement.

Third, the logistical feasibility is unknown and may vary by port.

Fourth, the maturity of the technology is still not proven.

Fifth, the resource requirements and who would pay them is not determined at this point.

And finally, sixth, the use and ownership of the scanned data is not fully determined.

So as I said at the beginning, these programs are at a crossroad. We have come a long way to build these programs, and our various partners have come a long way with us. What began as U.S. unilateral programs after September 11, 2001, have not only been accepted but have been internationalized. A risk management approach has been adopted by foreign governments, international organizations, and private companies as a logical way to increase security but keep the flow of commerce moving.

We were in a position of moving to leverage our own limited resources by developing mutual recognition with some of our partners, and that process goes on. Under mutual recognition, two nations would understand, verify, and trust each other's customs security regime so that a C–TPAT member in one country would be trusted in the equivalent program of the other country by their customs officials. And when mutual recognition is developed among a

number of nations, each nation's resources are, in effect, being leveraged to help the others, increasing the worldwide level of security.

With some of the latest proposals, though, the partnerships that we have relied on may be at risk. I am not saying they are severely at risk, but they are starting to fray. Regarding other nations, they may be reluctant to join CSI or stay in CSI if there is already a unilateral requirement on them that they scan 100 percent of all U.S.-bound cargo. In accordance with the agreements that we have already signed with them, they may ask for reciprocity, which CBP would be hard pressed to provide; the United States would have to scan 100 percent of our containers before they are outbound for the other countries.

Regarding the private sector, companies may be reluctant to join or continue in C–TPAT if 100 percent of their containers are going to be scanned anyway.

In closing, I hope I have provided some useful perspectives on supply chain security for you. I am also ready to answer questions on the whole area of the SAFE Port Act. Thank you.

Chairman LIEBERMAN. Thanks, Mr. Caldwell. You have supplied useful answers to us, and we will have questions. Thanks.

Captain Monroe, welcome back. Good to see you.

TESTIMONY OF CAPTAIN JEFFREY W. MONROE,[1] DIRECTOR, DEPARTMENT OF PORTS AND TRANSPORTATION, CITY OF PORTLAND, MAINE

Captain MONROE. Good to see you. Thank you very much for inviting me this morning, and it is a pleasure to be here, as always. I always like to start off by talking about our little port of Portland, which happens to be not only the largest port in New England and the largest port in the State of Maine, but also the largest foreign inbound tonnage transit port in the United States, and I know the Senator loves all the adjectives I add to that.

One of the things that is unique about Portland is we are a very diverse port. It was one of the reasons that the U.S. Coast Guard, in doing their first assessments of ports, looked at Portland, Maine, because of the diverse economic mix and the many operations that went on there. And we are happy to see that the SAFE Port Act, when it was put together, contained many of the critical provisions that looked at supply chain security. And I use supply chain security as a very definitive term because one of the things that we need to understand is that container security and port security are not necessarily synonymous.

We deal particularly in Portland with millions of tons of oil, dry bulk cargo, petrochemicals, other ports near us deal with automobiles, we all deal with hazmat and certainly project cargoes, and we have to understand in this mix that if we are talking about port security, it is all elements of different types of cargoes, all different types of operations, all different types of vessels.

The SAFE Port Act was a very big step. Overall, progress is good but certainly not as fast as it needs to be. And Senator Collins

[1] The prepared statement of Captain Monroe appears in the Appendix on page 102.

mentioned the TWIC card before, and this has been sort of a source of concern for us up in Portland, as well as in the industry.

These are my credentials. Kind of interesting. We carry quite a few of them. This is my airport credential. The one thing that is interesting about our organization is we operate the airport, the seaport, and coordinate all the surface transportation system. I required a very definitive background check to get this. This is my merchant mariner's document. I also required a very definitive background check to get this. This merchant mariner's document was not acceptable as a document to get this airport credential. This is my port document. We have no standards for that as yet. And while I recognize what DHS has said in many cases about aviation and the maritime world being very different from each other, no question about that. But the quintessential common area here is the background check, and most of us in the port industry recognize at this time, no matter what standard TWIC winds up coming out with, we are going to wind up issuing our own cards anyway because the reality is that is the best way to maintain tight control in our various ports. So one card fits all might be great for at least getting the issuance, but may not be best for all of the access.

I am happy to report I have been through four separate background checks to get my credentials. They have not found anything yet, which I am very happy to see.

Programs like C–TPAT are a good standard. We are working toward that, and that is expanding. That needs to continue. So does CSI, our radiation scanning program, and the high-risk scans. And I agree with Senator Collins that certainly scanning every container is counterproductive and does not work that well. But the focus of this is to push out the borders, and that is really what we need to do.

All of these things have to occur in foreign ports. And we are worried that cargo and port security sometimes lags within the Department of Homeland Security, may be low profile, and I fear sometimes that it is low priority.

I think the Office of Cargo Security, as defined within the SAFE Port Act, was a good concept. Last year, Senator Collins proposed legislation that called for a much higher level of policy decision-making area that looked at all of the aspects of cargo, and I think that is really where we need to go. That needs to occur as effectively as possible.

Cargo is a critical element, it is a critical threat, and if we look at all aspects of cargo, not just container, we begin to realize that the priority of this has to move up much higher within DHS. And once that occurs, I think that is going to speed up progress on many of the things that we are doing.

There are some bright spots. I do not like to be all doom and gloom. Many of the public officials and port professionals certainly in our area are working together very well. Public officials and our port and terminal operators understand the complexities of working together. The Incident Command System, I think that has worked out well.

We are very happy to see that our municipality, not waiting for the national standard of operations center, developed through

Homeland Security money our own operations center led by our dynamic fire chief, who approached the entire thing from a holistic view, not only the transportation system but the entire community, and developed an emergency operations center, which we have used on multiple occasions to look at all of the systems that are going on, all of the activities, all of the threats. And we have had some practical applications, unfortunately, such as last year's Patriots' Day storm, which allowed us to respond quickly to a lot of damage and loss of power and threats to citizens from just natural disaster.

We have used the port security grant money very effectively. We are certainly not spendthrifts, but it has helped us put up fencing to access control, develop informational platforms which have allowed us to communicate with each other and to share data and information. Ultimately, someday we think that we will be able to flip a switch and you will be able to see everything that is going on in Portland, Maine, right here in Washington, DC.

But this money has allowed us to ramp up quickly, and it is as important to have this money available to smaller ports as it is the major mega ports, which certainly need the money, but also have the resources in many cases to do this.

When we approach port security, when we approach transportation security, it has to be done in a systematic approach, not in a modal approach. And the unfortunate thing is that we have lived too long with the modal approach in transportation, which I think sometimes is working its way into homeland security, where we think of aviation or ports or even the surface transportation system as different from each other. Wings, wheels, or propellers, the system needs to work together. And one size in many cases can fit all, even with the differences in these various systems. High-level coordination is certainly critical, and that will be key if we ever have an incident.

The restoration of the marine transportation system is only one element of the restoration of the entire transportation system, and that even though industry seems concerned sometimes, I think the reality is not looking for definitive answers, but just looking for definitive standards so that someone in DHS understands what every facility is capable of and is able to immediately restore the system, redirect cargo.

If we had an emergency, for example, up in Maine in the middle of February, by heavens, we would be trying to think of ways to get oil up there to meet the needs of our homes and our factories and our communities. And the bottom line is unless somebody has a holistic picture of that and clearly and definitively directs it, it is not going to work effectively. It cannot be just a series of communications. It has to be some very definitive direction.

We saw that on September 11, 2001, with the confusion that was going on, and that needs to be looked at and corrected. This restoration trade is a very significant issue. We noticed that right before Hurricane Katrina. The maritime industry was able to direct its cargo. It anticipated the problems. But that is something that needs to occur on a national level.

The one thing we need to keep in mind is that cargo does not vote, so it is the responsibility of our agencies, the responsibility of

our elected officials to look at this very critical supply chain and all of the elements attached to it and make sure that not only is it safe and secure, but that it can be restored quickly.

For right now, we are not quite getting the job done. We are certainly much better than we were. There is no question we have made an enormous amount of progress through the sheer will of a lot of good people working on the ground in the trenches like myself, and certainly the direction of the Department of Homeland Security has worked well. But all of this needs to come together much closer. There needs to be much more definitive leadership out of the Department of Homeland Security. We need to worry less about our various Federal agency directives and think about it in a more holistic standard. And we also need to look at our entire transportation system in a holistic, systematic fashion as opposed to just looking at the various elements of different parts of security where we think are threats.

Thank you very much, and thank you for the time to speak with you today, and I will be happy to answer any questions.

Chairman LIEBERMAN. Thanks very much, Captain. You are a good witness. It is good to hear your report from the ground. I was a little disappointed to hear that the cargo will not be voting in the Maine election—— [Laughter.]

Next year because I know, based on all that Senator Collins has done to make the cargo safe, that they would be voting for her.

Senator CARPER. We are familiar in Delaware with the term "cargo preference." It would probably have application in Maine as well.

Chairman LIEBERMAN. Exactly. OK. Senator Carper, welcome. On this very day, the TWIC program has begun to enroll port workers in Wilmington, Delaware, so we appreciate that you are here today.

Let me begin, Mr. Caldwell, with you, and as I said earlier, you have tremendous expertise in this area. Step back, if you would, and give us your overall rating of the Department's progress in maritime security in the year since the passage of the SAFE Port Act. If you were giving them a grade, what would it be?

Mr. CALDWELL. I think "incomplete" is the term I used in the last hearing we had.

Chairman LIEBERMAN. That is true.

Mr. CALDWELL. So I need to stay consistent here. But I would like to point out something fairly important. We did a very large effort for the Committee here on a progress report of DHS, and the cut-off on that was October 2006. We actually did not use the SAFE Port Act in setting the expectations that we then used to rate the Department on. And so the assessment I have now is updated from that earlier progress report assessment.

As my written statement demonstrates, there is continued substantial progress in many of the requirements of the SAFE Port Act. I would have to agree with Assistant Secretary Baker that the components look like they have made it already or they are in line to make it.

There are four areas that we pointed out in that earlier report, and these are the four areas where we still think there are some challenges. I can just go over those again real quickly.

Chairman LIEBERMAN. Why don't you highlight them? That is the "incomplete" part of it.

Mr. CALDWELL. Yes. There is developing port-specific plans for recovery. I would agree with——

Chairman LIEBERMAN. Recovery meaning what here?

Mr. CALDWELL. Recovery after an incident. We need to think of incidents as being beyond the initial security response to include recovery from environmental incidents or natural disasters and things like that.

Chairman LIEBERMAN. Sure.

Mr. CALDWELL. When you ask what the Department is doing, the components are going to use their International Supply Chain Security Plan. They also have something called the Maritime Infrastructure Recovery Plan, which is also a national plan. Now they have to bring that level of planning down to the individual port levels. That is where they are incomplete. They need to rewrite all the area maritime security plans to add in that recovery portion.

The other incomplete area is implementing national access control. TWIC is underway. They are certainly making progress compared to where they were a couple of years ago. The next incomplete area is long-range tracking systems to improve maritime domain awareness. We are currently doing some work to look at both the classified as well as the unclassified tracking systems, and so we may find out they made more progress there than we had initially reported.

Chairman LIEBERMAN. OK.

Mr. CALDWELL. And then, finally, in terms of developing programs to screen cargo for radiation, that is another program where we thought they needed to make more progress than indicated. We have reported in several recent reports about the testing that was done in terms of the new technology for radiation scanning.

Chairman LIEBERMAN. Thanks. We will obviously count on you to keep an eye on those four areas particularly, and we will continue to work with you and your colleagues at GAO.

Mr. CALDWELL. Yes, sir.

Chairman LIEBERMAN. Mr. Lloyd, I appreciate the good report on Project SeaHawk. I love the combination of the Federal, State, and local officials for a common purpose, including the Joint Terrorism Task Force. This is exactly the kind of work that was not really occurring prior to September 11, 2001.

I wonder if you think that State and local law enforcement agencies will continue to participate in programs like Project SeaHawk if they are unable to receive Federal assistance, which was one of the things that is being contemplated.

Mr. LLOYD. Thank you, Senator, and I would likewise agree that the Department has for a long time held the view that our partnerships with State and local particularly law enforcement agencies are key to us getting our mission done.

The issue of what happens after the pilot project with SeaHawk ends as far as it relates to our State and local partners down there is our biggest question. Those issues I think will be worked out in a little more detail and with some more concrete specificity once DHS is finished going through its process of identifying exactly how the project will be transitioned, i.e., which component, if any,

of DHS will take over SeaHawk, or will the Department itself sort of step into the role that DOJ is currently undertaking.

Obviously, our State and local partners feel a lot of pressure from other priorities that they face, and what we hear on our end is that the issue of funding for them or reimbursement for them is key, as well as how soon they are going to know about the transition that is going to occur.

What we have done is with rebudgeting, we have been able to extend the project life to the end of fiscal year 2009. That has allowed them some more time at the local and State level to be able to hopefully identify funds or grants that may allow them to continue their participation.

Chairman LIEBERMAN. Excellent. Thanks.

Just a quick question, Captain Monroe. As you know, we established a Port Security Grant Program, which Senator Collins and I and all the Members of the Committee worked on. And these grants have been used to make much needed improvements in the physical safety of our ports and waterways. The SAFE Port Act authorized $400 million annually for the program.

The Department of Homeland Security recently announced that it intends to make implementing the requirements of the TWIC program a primary purpose of the overall Port Security Grant Program, and obviously, we all understand the importance of TWIC with the comments that you have added. Are you concerned that this may make it more difficult for you and other local port administrators to get funding for other critical port security improvements, like surveillance equipment or equipment to detect underwater explosive devices?

Captain MONROE. Well, over the course of time, many of us have already ramped up to that location. We have already looked at the aspect of surveillance, so we are sort of in the second tier of this.

Chairman LIEBERMAN. Yes.

Captain MONROE. The bottom line is that we do not have a standard really that works for TWIC. Things like document readers and biometric readers and all the other technology that they are talking about, in some cases they do not even exist. So nobody has really any idea what the cost is going to be or the long-term implications or, in many cases, even the use for this thing.

I think the bottom line is that as every year goes on, you begin to see where the holes potentially are.

Chairman LIEBERMAN. Right.

Captain MONROE. And, of course, we have all of the rules and regulations that call for multiple assessments. So we find ourselves in the position of always continually trying to apply for money that we need. We do not try to do excess. We just try to do what we think is essential. And we have gone a long way with many of the things that we have done, but we are a smaller port. The challenge is in some of the bigger ports that are much more diverse. And I think ultimately, if you talk to some of my colleagues, they will tell you that in many cases port security grant money needs to be expanded because there are certainly many more challenges.

The other side of that is that many of the bigger ports also have the resources to be able to meet these needs, where in our par-

ticular case, the citizens of the city of Portland would have had to have borne the cost of these mandated fundings.

Chairman LIEBERMAN. Understood. Thanks. My time is up.

Senator COLLINS. Thank you, Mr. Chairman.

Captain Monroe, to follow up on the funding issue that the Chairman just raised, he and I have had to fight so hard to secure funding for port security grants. The Administration, as you know, year after year has proposed folding port security grants into a general homeland security grant program, whereas we have advocated for dedicated funding.

Could you speak to the importance of being able to rely on dedicated funding for port security grants and also on the importance of having multi-year funding? It seems to me from seeing the projects that you have underway in Portland that many of them are multi-year projects that are going to require additional investments. But if you could comment on those two issues.

Captain MONROE. Well, homogeneous funding programs are very difficult because one of the things that happens is you begin to lose the expertise necessary to properly evaluate what is necessary. I would find it particularly difficult if I had to go up against aviation funding because the needs are very different. There is no question about that. We have been able to use our multi-level funding and our multi-year funding to really step out not only with our new facilities and put in surveillance and all of the access control and all the other things that we have needed, but we are one of the first ports now to start looking at TSA-style screening for cruise line passengers and the international ferry. So that multi-year funding is very critical because one of the things that it is changing over the course of time are the regulations and the assessments. And as new intelligence becomes available, we begin to look at new threats.

So I think the reality is that this is very specific. Right now we have a great evaluation program on the maritime side, on the aviation side. There is not a very good system in place for the surface transportation, and they are really groping around trying to figure out what they need to do. But the reality is, I think, if you try to put it all into one place, like the Administration says, you are going to lose an enormous amount of good evaluation capability, and then it is just going to become a matter of competition, and needs may not be met in that circumstance.

Senator COLLINS. Thank you. I certainly agree with that assessment.

Mr. Caldwell, you stated in your testimony that 100-percent scanning could actually reduce security rather than enhance it. And since I agree with that assessment, I was very happy to hear you say that for the record.

Is it fair to say that requiring 100-percent scanning, regardless of the impact on trade, regardless of cost, regardless of the risk of the cargo at hand, is inconsistent with basic risk management principles?

Mr. CALDWELL. I would agree with that. If I could just give an example?

Senator COLLINS. Yes. Thank you.

Mr. CALDWELL. Could we get the chart back up that Assistant Secretary Baker used in his presentation?[1] You have three things shown on this chart that are valuable: You have the NII, which is the imagery screen; you have the radiation screen as well; and then you have the ATS score. These are three very important things. But from Mr. Baker's description, it sounded like you need to have a person at the National Targeting Center look at all three factors. How many thousands of people are we going to need, either overseas or here, to look at that? I just do not know what kind of resource level would be needed to make these 100-percent scanning images useful. If you are just taking the scans and storing them, you are not improving security.

Senator COLLINS. And isn't that what is happening in Hong Kong? We hear a lot about the Hong Kong project, but, in fact, unless there has been a change recently, it is my understanding that while images are being captured, no one is looking at the images. And if no one is reviewing the results of the scan, you are no further ahead, and, in fact, it may produce a false sense of security to have the scan done. But if no one is analyzing the results, there really is no progress.

Mr. CALDWELL. I was in Hong Kong in 2004, and I got the demonstration of their system. I cannot say I audited it, so I do not know how well it works. It was pretty impressive how they are trying to combine these different technologies. But, again, what I do not know is what was being done with those images.

One of the most promising areas—and, again, Assistant Secretary Baker brought this up—is potential improvements in software. What if you could have a software program that would tell us that, based on the manifest and this type of item, the item should have this kind of radiation signature, and it should have this kind of density. And then the software would combine all those things through an algorithm to indicate that an item seems within the normal deviations and that we should not worry about it. At that point, it is not too different than the ATS system currently being used.

Senator COLLINS. Right. That is essentially a targeted system.

Mr. CALDWELL. Correct, it identifies the containers that need extra scrutiny.

Senator COLLINS. Exactly.

Mr. CALDWELL. And that may be where they are going in the long run, but I am not sure. As I said, SFI has been fully operational only for 3 days now, so we need to be careful making premature judgments. When we were in Honduras, or when we were in Busan 6 to 12 months ago, they were just laying the plans to install SFI. Many of these questions had not been worked out in terms of who is going to own the images, who is going to review them, how do you store them, and who is paying for it.

Senator COLLINS. Thank you.

Mr. Lloyd, it is my understanding that there is talk of transitioning the project that you have described from the Department of Justice to the Department of Homeland Security. And, indeed, I think that it was housed in the Department of Justice to

[1] The chart submitted by Mr. Baker appears in the Appendix on page 106.

start with because it was an earmarked project. And it is a good example of an earmark that has produced very valuable information and a pilot that we may want to replicate elsewhere. But do you have concerns about the transition from DOJ to DHS?

Mr. LLOYD. Thank you, Senator. It was actually started, obviously, as a special pilot project before the creation of DHS, and what we have seen is that it has been a wonderful program and it has done, I think, the type of things that needed to be done in terms of bringing varying agencies together into a unified command at a port.

Our concern would be that you would in a transition, obviously, lose some of the effectiveness of that unified command, that you would lose the presence of the State and local partners, who we think are very valuable. But ultimately I think that is something that DHS would have to evaluate as to which components programwise of SeaHawk they would want to keep, replicate around the country, or move to a different model. But what we have found right now is that all of our participating components find all of those programs that we are currently operating there to be very useful in terms of augmenting their missions.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. Thanks, Senator Collins.

I was interested in the discussion with Senator Collins and Mr. Caldwell, and those are important questions about the personnel required for the 100-percent scanning. I visited the port in Hong Kong during August, and I suppose the most significant thing is that the system, the integrated system, both radiation monitoring and imaging works, and it works in a way that does not, to my eye, and I guess to those looking at it, unnecessarily burden the flow of commerce. What is required to then use the information that technology provides us with? And I am informed that they are beginning both in Hong Kong and in Singapore, in addition to the three other ports we mentioned more fully, to try to make judgments about that.

I suppose the thing to say—it may be obvious but worth saying—is that modern technology gives us a capacity to even contemplate 100-percent scanning without unnecessarily interfering with the flow of commerce, which would have been unimaginable not so long ago. So we will work on that.

Senator Carper, the bell goes off, but that means we have enough time for a good solid round of questions.

Senator CARPER. Great.

Chairman LIEBERMAN. By the bell, I mean not to call us into the center of the ring, but to take us over to the Senate because there is a rollcall vote just starting.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you, Mr. Chairman.

Gentlemen, thank you for joining us today and for your testimony and for your responses to our questions. As the Chairman alluded to earlier in our hearing, and I suspect you all discussed it on the previous panel, the TWIC program is actually getting implemented, up and running in the port of Wilmington today, which is about 5 or 6 miles from where I live. I have been out to the port

a lot. When I was governor, we were very much involved. The State of Delaware took over the port from the city of Wilmington and spent a lot of time, energy, and money to try to bring them into the 21st Century. So it is something that we care about and have thought a lot about and know a lot of the folks who work out there.

A lot of the people who work out there, not all but a lot of them, are folks who have had scrapes with the law in their past, and my suspicion is if you go around to major ports around the country, you would find some of the folks who are doing a lot of the work at ports—a lot of it is back-breaking work, a lot of physical labor—are people who have had in some cases brushes with the law, in some cases rather serious ones.

As we bring TWIC up and running, there are some folks at our port who are concerned that they may lose their jobs, pretty good-paying jobs, considering in some cases the degree of education they have and their criminal record. Captain Monroe, are you concerned about the impact that the TWIC card could have on port operations?

Captain MONROE. Well, I am not, really, and the reason being is that we had the same issues when we implemented the background screening for aviation. There are a lot of folks who felt that because of whatever the issue, something might knock them out.

I think the reality is that all of these background checks are directed toward people who may be a potential threat, and I think that certainly does not encompass the vast majority of folks.

Now, if you do have a violent offender, somebody who has been arrested for something fairly significant——

Senator CARPER. Like terroristic threatening?

Captain MONROE. Yes, terroristic threatening or even murder, or anything like that, certainly I think I, as a port director, would have a lot of questions about having them working on my port to begin with. But I think what we realized is that no matter what the fear was, when we implemented the aviation program, most of the people did not have issues, even those people who did have some sort of issues or background problems or even misdemeanors or some arrests. It didn't necessarily knock them out.

So I think that is a fear in many cases that is overblown by folks because of the uncertainty of the program.

Senator CARPER. How do we strike the right balance to make sure that folks who do not pose a threat, given at least their behavior in the past, but who have made mistakes, how do we find the right balance so that the folks who pose the threat maybe are not invited back for a continued engagement and those who do not, have the opportunity to continue to prove themselves?

Captain MONROE. Well, I think the simple way to do that, Senator, is basically take people on a case-by-case basis. You are only going to find a small percentage of these folks, I think, that are going to be identified, and then take the time to review those individual backgrounds, assist them in trying to find out what the circumstance was, do an investigation, and get it over with. And the reality is those standards have already been suggested as part of the Coast Guard program, and I think they are pretty good standards.

Senator CARPER. OK. Any other comments from anyone, please, on this?

Mr. CALDWELL. There are two things. First, it is a statutory criteria as to what crimes disqualify them. Second, there is an appeals process. But what I am not sure about is whether the appeals process will allow them to take somebody who committed one of those crimes 20 years ago and allow him to still have the TWIC card.

Senator CARPER. I believe there is a process—we call it a "waiver process"—where people can seek a waiver, and I think in some cases, a person could seek and receive a waiver even if the offense was one of these that are stipulated in the guidelines.

Mr. Lloyd, do you want to add anything? If not, I have another TWIC-related question.

Mr. LLOYD. Senator, I would just say briefly that one of the things that we do at Project SeaHawk is almost on a continuous basis with all of the task force agencies that we have there is go through and check and make sure that those individuals who are working at the port and on the docks in particular do meet those statutory requirements. Occasionally, you do find individuals with ties to ongoing criminal activity, and that is what we see as much of a threat to port security as the terrorists. If our port is vulnerable to that kind of ongoing criminal activity, then we feel like it is vulnerable to potential terrorist intrusion at that point.

Senator CARPER. Alright. Good. One other question. Again, it is TWIC-related. But maybe, Mr. Caldwell, you would be best at this. When we first conceived of this idea and said we want to put together a program and increase our port security, do you recall when we said we wanted to get it underway? Was there an early target date?

Mr. CALDWELL. It was included in the Maritime Transportation Security Act, and I believe that was passed in November 2002. But I do not know if it had an implementation milestone associated with it.

Senator CARPER. Anybody recall? Captain Monroe.

Captain MONROE. Yes. When Congress first talked about the TWIC program, they were looking at that point as a broad-based transportation worker program across all aspects. And this came through right after September 11, 2001, because it was one of the first things that people recognized needed to be addressed. And what happened is, come 2002, 2003, it began to go off in different directions.

Senator CARPER. Alright. Given the long run-up to actually being able to launch the program today in one port, and some other ports are in line next, when do you think we can reasonably expect to have the program pretty well up and running, not just in a handful of ports but throughout the country?

Captain MONROE. Well, right now the Coast Guard has a program that they are rolling out, so we are looking at some very definitive deadlines. So within the next year to 18 months, the TWIC program, as currently envisioned, should be fairly well in place in most places. And I have to credit the port of Wilmington because they did a lot of good work as part of the pilot program. We had a chance to meet with them and talk with them, and I think they

did a great job looking at a lot of uncertainties and sort of reining it in for us a little bit. But I think within 18 months we will see a pretty substantive accomplishment there.

Senator CARPER. Well, good. I was at the port not long ago, and they said, "Who is Jeff Monroe?" [Laughter.]

I said, "I think he is from Portland, Oregon." No, I did not say that. I am sure he is from Maine. Thank you all very much.

Chairman LIEBERMAN. Thanks, Senator Carper.

Attorney Lloyd, Mr. Caldwell, Captain Monroe, thanks very much for being here, for what you are doing every day to improve our homeland security, and for the testimony that you have given today. We appreciate it very much.

The record of the hearing will be held open for the customary 15 days for Members to submit additional questions to you or for you to add to your testimony. But please know that you have our thanks.

The hearing is adjourned.

[Whereupon, at 12:09 p.m., the Committee was adjourned.]

APPENDIX

Statement of
Stewart Baker

Assistant Secretary, Policy
Department of Homeland Security

Introduction

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee, I would like to thank you for the opportunity to speak today about the progress we have made improving port and maritime cargo security since the passage of the Security and Accountability For Every Port Act (SAFE Port Act).

This hearing, coming only a few days after the one-year anniversary of the enactment of the SAFE Port Act, provides an opportunity to discuss not only the Department of Homeland Security's (DHS) implementation of the Act's requirements, but also to reflect on the reasons behind our continued efforts.

As many Members of this committee are aware, approximately 32,000 seagoing containers arrive and are off- loaded at United States seaports each day. In fiscal year 2006, that equated to 11.6 million cargo containers.

To put this in a visual context, the National Mall – from the steps of the Capitol to the Washington Monument - could hold a single layer of just 13,068 containers (twenty foot equivalent units). If you wanted to put all the containers that arrive in the United States annually on the National Mall, you would have 13,068 stacks that were each 888 containers high.

These figures illustrate the incredible volume of maritime containerized cargo transiting the global supply chain. Because so much of the world's trade converges in the maritime supply chain, it is uniquely vulnerable to terrorist exploitation. An efficient maritime transportation system is vital to the global economy, but it can also be used to move dangerous cargo to our ports and cities. Simply put, we are talking about a vital global supply chain that serves a vibrant, interdependent global economy – and the importance of protecting it.

The SAFE Port Act displays a broad, strategic vision, covering more than 75 different sections, and touching on all aspects of the existing maritime security architecture -- from securing the containers that transit the supply chain, to defending the vessels and ports that connect it, to ensuring the protection and accountability of the people that work within it.

This noteworthy legislation, with its broad support, reflects the close collaboration between DHS and both the House and the Senate during its development. The SAFE Port Act recognizes the importance of balancing the security of America's borders with the necessity of facilitating legitimate trade and travel. The Act recognizes that any disruptions to this maritime transportation system will have immediate and lasting consequences for our economy and the world at large.

The DHS approach to SAFE Port Act

DHS commends the work of this Committee in addressing the vulnerabilities of containerized cargo through this legislation and through the continued dialogue we have had as we work to implement the Act's many provisions. We appreciate the Committee's

recognition of a number of notable DHS successes through the codification of initiatives and programs that DHS undertook immediately after the 9/11 terrorist attacks and has been implementing successfully ever since.

The SAFE Port Act directs DHS to complete more than 100 specific tasks – an ambitious undertaking. We have completed over 50 to-date and are on track for the remaining provisions. Simply put, the overwhelming majority of requirements mandated by the SAFE Port Act have either been completed or are on schedule to be completed within the required timeframe.

One of the Department's most ambitious achievements over the last year has been the fulfillment of the Act's foreign scanning pilot program requirement, under the Secure Freight Initiative (SFI). SFI became fully operational on October 13th in three foreign ports: Qasim (Pakistan), Cortes (Honduras), and Southampton (United Kingdom). All maritime containerized cargo destined for the U.S. from these locations is currently being scanned and that information is being analyzed by U.S. Customs and Border Protection (CBP) officials stationed in-country and domestically and is available to the host nation government.

Other significant SAFE Port Act accomplishments include:

- On October 3 of this year, USCG published the proposed rule for the Long Range Identification and Tracking (LRIT), which will facilitate the Government's use of the full range of classified and unclassified vessel tracking information available.
- USGC has increased the pace of foreign port assessments, is on track to complete an initial assessment of all of our trading partners by March 2008, and anticipates conducting assessments on a two year cycle thereafter.
- The final Transportation Worker Identification Credential (TWIC) joint rule was published on time by the Transportation Security Administration (TSA) and the USCG. The rule establishes standards and procedures for gaining unescorted access to the Nation's ports and vessels.
- The International Strategy to Enhance Supply Chain Security was also released on time and received input from both the National Maritime Security Advisory Council (NMSAC) and the Commercial Operations Advisory Committee (COAC).
- The Cargo, Maritime, and Trade Office (CMT) was established within the Policy Directorate to coordinate all cargo security programs among the various agencies and departments, as well as effectively engage all relevant stakeholders, including the private sector, in the development of policies and regulations.
- CBP is on track to screen approximately 98 percent of all sea-borne containerized cargo entering the United States for illicit radiological/nuclear materials with radiation portal monitors by the end of December 31, 2007.

Overall, DHS has been working aggressively, and often within constrained timeframes, toward the full implementation of the Act's requirements. While much has been accomplished, there remain a few mandates we have yet to achieve. The remaining requirements are either very close to completion or face outstanding technological

challenges, which have required DHS to seek alternative solutions, and in some cases, reach out to our international and industry partners.

In reflecting on the not yet completed mandates, two themes emerge that often explain the limits we face as we work to translate written words in the Act into meaningful and successful programs. The first theme is that programs built on new technology need to proceed carefully and meticulously. The second theme is that because the supply chain extends across the entire globe, securing it requires close cooperation and partnerships with our foreign counterparts. Neither technological development nor diplomacy reacts well to being rushed. Small delays early on pay dividends and result in stronger, more effective programs in the long run.

The Pace of Technology

I would like to expand on the first theme – the tension between the pace of technology development and how it shapes the rate of policy implementation. The right technological advancements can augment security dramatically: technology can act as a force multiplier, a tool for organizing and sifting through mammoth amounts of data, and can expand the speed and breadth of communications. However energized we are about achieving the benefits of technology now, the brutal reality is that sometimes the pace of technological development does not accord with the policy deadlines we seek to achieve.

The SAFE Port Act addresses many cases in which new technological tools have the potential to greatly increase security. Sometimes, these technologies are ready for use and can provide immediate benefits. This is the case with the non-intrusive inspection (NII) technologies that we deploy at domestic ports of entry to obtain images of the contents of containers. These NII technologies help our Customs and Border Protection officers every day to identify threats, contraband and other anomalies as goods enter our ports.

However, often, the process of transitioning technology from the factory where it is designed or the laboratory where it is tested, into the operational realm can be challenging. We face this challenge as we seek to implement: 1) the Transportation Worker Identification Credential program, 2) the overseas radiological and nuclear scanning pilot, and 3) as we consider means to secure containers using new technologies.

Transportation Worker Identification Credential (TWIC)
The Transportation Worker Identification Credential program offers an example of new technology that will quickly confirm a port worker's identity. TWIC is one of the world's most advanced, interoperable biometric credentialing programs. When it is ready, the new card reader technology that can verify an encrypted biometric will augment the security of our nation's ports.

In order to successfully achieve this vision, the TWIC program is moving towards its objectives, making decisions focused on enhancing port security through a reasoned, phased-in implementation.

TSA is also moving forward on the pilot program called for in the Act to test the TWIC biometric card readers and has identified the Port Authorities of Los Angeles; Long Beach; Brownsville, Texas; and New York and New Jersey; as well as Watermark Cruises of Annapolis, Maryland as pilot participants.

While it has unfortunately proved impossible to meet every SAFE Port Act deadline for TWIC, I am confident that the hard work and time the Department is putting into technology and requirements development, incorporating Congressional and industry input, and developing a careful deployment approach will result in a stronger, healthier and more efficient TWIC program that will protect our country's ports into the future.

Secure Freight – Overseas Scanning Pilot
As I mentioned earlier, the overseas scanning pilot called for in the Act is now operational in three foreign ports, meeting the SAFE Port deadline. This pilot is the first part of our Secure Freight Initiative. Under SFI, DHS and our partner, the Department of Energy, have deployed non-intrusive imaging, radiation detection equipment, and optical character recognition technology abroad to provide an integrated scan of U.S.-bound container cargo. Information from this technology, combined with our normal analysis of manifest data, will provide a comprehensive, real-time approach to assessing the risk of every container bound for the United States.

The process has not been simple; integrating radiation portal monitors, non-intrusive inspection equipment, and optical character readers into each port has presented serious challenges. For instance, successfully deploying the container scanning equipment has required re-configuring certain port layouts to accommodate the equipment without adversely affecting port efficiency. Additionally, some equipment functions differently in extreme weather conditions. Different countries have varying degrees of existing information technology (IT) infrastructure, and the costs of transferring the data back to the United States (to the National Targeting Center) in real-time can be very high. However, in Port Qasim (Pakistan), Puerto Cortes (Honduras), and the Port of Southampton (United Kingdom), we continue to work successfully with our partners at the Department of Energy, our international allies, and industry to address these issues daily.

The department's next step is to expand the program, in a limited capacity, to four more ports in Hong Kong, Salalah (Oman), Port Busan (South Korea), and Singapore. DHS chose to partner with these ports because they pose different challenges and provide diverse environments in which to evaluate various technology options. Hong Kong, Busan and Singapore are three of the world's largest ports and different space constraints and speed of traffic in each present challenges that must be overcome for scanning to work effectively. Salalah has a very high rate of transshipped traffic that enters the port via ship and does not travel through the port's gates, where the scanning equipment is traditionally placed. Each of these ports will offer vital lessons and evidence on how this

integrated suite of scanning technology can meld smoothly into the logistics, operations, and flow of commerce at different ports.

The Department will prepare and submit a report to Congress in April 2008, as mandated in the SAFE Port Act, detailing the progress made in these first seven Secure Freight Initiative ports. The report will outline the successes and challenges we have faced while implementing scanning in foreign locations, including: the availability, capabilities and efficiency of technology and equipment; the process of negotiations with our host nation counterparts as well as their input and feedback on the scanning in their ports; the impact on the movement of cargo through ports and across the global supply chain; the staffing and human capital requirements that will be necessary both abroad and domestically and additional considerations.

While I believe in the benefits of the scanning technology and the importance of addressing radiation and nuclear threats to containers, this serves as another example of the pace of technology development differing from the rate of policy implementation. The lessons we are learning from this initial seven port deployment indicate a lot of promise for these technologies, but at the same time have allowed us to develop a more realistic vision of the challenges inherent in scanning the 11.6 million shipping containers that come to the United States from over 700 ports each year. As technologies mature, policies must be adapted to take full advantage of their benefits. Based on what we learn through these initial pilots, we will consider a full range of policy options that will allow the Department to best use the technologies to enhance security.

Securing Containers Through New Technology

The SAFE Port Act addresses the issue of container security standards and procedures. While DHS, as required by the Act, issued a letter on May 18, 2007 explaining that we will not be using the rule-making authority at this time, we strongly support and are continuing to seek opportunities to enhance supply chain security efforts, including enhancements to the security of the container. The potential use of Container Security Devices (CSDs) is a third area where the tension is evident between technology readiness and policy needs.

CSDs have the potential to increase the security of a container if they are able to accurately indicate whether a container has been opened by unauthorized personnel seeking to introduce dangerous and illicit materials or to remove the container's contents illegally.

However, when we discuss CSDs, we must recognize that there are also limits to the benefits: the financial and logistical costs of the devices and the significant infrastructure beyond the device itself that could be costly and challenging to deploy, as well as possible delays and other operational implications associated with response protocols.

We are developing a path forward that would explore the efficiency of these technologies and the degree to which they might enhance container security in very specific trade lanes. I look forward to sharing our strategy with this committee when it is finalized.

Partnerships and Collaborations

Before I discuss some of the specific provisions, I will offer a brief word on a second theme in the Department's overall approach to effectively implementing the SAFE Port Act: Partnerships and Collaborations. The Department's maritime and supply chain security doctrine is grounded on a commitment to deploy a strong, layered system. By deploying multiple, mutually-reinforcing security layers and tools, we diminish the risk associated with failure at a single point. To do this successfully, DHS must have equally strong partnerships with the trade and foreign governments who own and control most of the international supply chain.

The theme of partnership and collaboration, between DHS and other federal entities as well as between DHS, industry and the international community, is central to a number of programs and initiatives required by the Act. I would like to highlight some of the significant achievements within these partnership programs, touching upon international partnership such as the Container Security Initiative (CSI) and the Secure Freight Initiative (SFI), partnerships with domestic industry such as the Customs Trade Partnership Against Terrorism (C-TPAT), and the collaborative efforts between the Domestic Nuclear Detection Office (DNDO), other DHS offices, as well as other state, local, and federal entities.

Container Security Initiative (CSI)
The Container Security Initiative (CSI) and the Secure Freight Initiative (SFI) are true examples of successful bilateral and multilateral solutions to supply chain security. In both cases, DHS receives indispensable cooperation and support from foreign governments that has allowed us to establish a framework that will greatly aid our future efforts abroad.

Under CSI, we are partnering with foreign governments to identify and inspect high-risk cargo containers at foreign ports before they are shipped to our seaports and pose a threat to the United States and to global trade. We continue to make excellent progress in ports around the world. This fiscal year CSI expanded to 8 additional ports, and reached a milestone of 58 ports worldwide covering 85% of the container traffic destined to the United States.

Secure Freight Initiative (SFI)
As we continue to move forward on the next generation of CSI—the Secure Freight Initiative – I want to point out that this expands the CSI partnership to include, multiple foreign governments, the trade community, vendors of leading-edge technology, and vital U.S. government agencies, in particular the Department of Energy (DOE), who provides the Radiation Portal Monitors under their Megaports Program. I mentioned the Secure Freight Initiative previously, but I want to highlight here the fact that this initiative is the

culmination of healthy and vigorous cooperation at each of these levels: among U.S. Government agencies, between multiple foreign governments, and with the trade community and vendors of leading-edge technology.

Advance Security Filing Initiative ("10+2")
DHS fully appreciates the need to develop close partnerships with the private sector and industry as these groups own the assets and are responsible for the movement of goods throughout the global supply chain. Our efforts with the Advanced Security Filing Initiative as well as the Customs-Trade Partnership Against Terrorism (C-TPAT) program exemplify this collaborative approach.

As you know, the Safe Port Act required DHS to collect more detailed information on maritime cargo destined for importation into the United States. Working actively with the trade through trade advisory groups, such as the Departmental Advisory Committee on Commercial Operations (COAC) and through the trade community in general, DHS has developed the Advanced Security Filing (better known as the "10+2" data elements). The Advanced Security Filing will provide additional advanced cargo information that will enhance our ability to perform risk-based assessments prior to cargo being laden on a vessel overseas. A Notice of Proposed Rulemaking is currently under review but I want to assure you that DHS is committed to expediting this process to the extent possible.

Customs Trade Partnership Against Terrorism (C-TPAT)
CBP's Customs-Trade Partnership Against Terrorism (C-TPAT) is an integral part of the DHS multi-layered strategy. CBP works with the trade community to ensure that our partners adopt stronger supply chain security measures across their international supply chains. Significantly, the program has enabled CBP to leverage supply chain security overseas where the U.S. government has no regulatory authority.

C-TPAT is an example of one of the successful programs supported by Congress through codification in the SAFE Port Act. The SAFE Port Act not only legislatively recognized C-TPAT, but also added greater accountability by mandating specific time frames for activities and greater program oversight. Again, I am pleased to report that DHS will meet all C-TPAT Safe Port Act requirements: CBP will validate all new partners within one year of certification, revalidate Tier 2 and Tier 3 members once every three years, and conduct yearly revalidations on some of the highest risk enrollment sectors such as the U.S./Mexico highway carriers.

Additionally, CBP has implemented a pilot program using third parties to validate supply chains where we currently lack full access. In May 2007, CBP selected 11 firms to act as validators in China because Chinese government continues to deny CBP personnel access to conduct supply chain security validations. I will note that interest in the pilot program has thus far been minimal. Of the more than three hundred (300) C-TPAT importers that were invited to participate in this voluntary pilot in June, less than a dozen importers have opted to do so to date. The primary concerns expressed by C-TPAT members involve sharing proprietary business and security data with a third party and the costs associated

with the validation, which, as outlined in the SAFE Port Act, must be incurred by the C-TPAT member.

Domestic Nuclear Detection Office (DNDO)
Since the authorization of the Domestic Nuclear Detection Office (DNDO) by the SAFE Port Act one year ago, DNDO has continued to strengthen its role within DHS. DNDO has successfully developed strong working relationships with CBP and USCG and is meeting the requirements outlined in the SAFE Port Act. Individuals from across the various government agencies have brought their knowledge and expertise to the table to help DHS create a robust program focused on the tools needed to detect and interdict nuclear or radiological material.

DNDO's comprehensive strategy for the deployment of radiological and nuclear detection equipment, submitted to Congress this year, provides an overview of some of DNDO's key activities, and I would like to touch on a few notable achievements.

Working closely with other DHS components, DNDO has made excellent progress in deploying radiation detection technology at our busiest ports resulting in the radiation scanning of just over 94 percent of all incoming seaborne cargo into the United States. By the end of this calendar year, 98 percent of all containerized sea cargo entering the United States at the 22 busiest ports will be scanned for radiological and nuclear threats.

Furthermore, DNDO is currently testing the next generation of radiation detection equipment, known as Advanced Spectroscopic Portals, at eight locations nationwide – at Piers A and J in Long Beach, at the APM and PNCT Terminals in Newark, at the Colombia and World Trade bridges in Laredo, at the Blue Water Bridge in Port Huron, and at the Fort Street crossing in Detroit. Future deployments of ASPs, pending Secretarial certification, will allow CBP to quickly differentiate between real threats and benign materials, such as kitty litter or granite.

The SAFE Port Act also required DNDO to establish an Intermodal Rail Radiation Detection Test Center. This was a forward-thinking requirement and one that DNDO strongly supports. The Port of Tacoma was selected as the location of the Rail Test Center because more than 70 percent of its total import cargo volume is handled by rail at multiple intermodal rail terminals. DNDO is working diligently with CBP and the Port of Tacoma to begin testing the operational needs, as well as evaluating innovative technical solutions, to fit the unique radiological and nuclear detection requirements of intermodal rail terminals.

DNDO also recently announced the West Coast Maritime pilot program, which is beginning in the Puget Sound region of Washington State and will expand into San Diego, California. The three-year pilot will provide maritime radiation detection capabilities for State and local authorities with the goal of reducing the risk of radiological and nuclear threats that could be illicitly transported on recreational or small commercial vessels. This effort is another example of the close coordination between DNDO and other DHS components including CBP and USGC.

Path Forward

Let me conclude with a few comments related to the Department's path forward. Our focus on risk management and security is driven by Congressional mandates and media interest but also by informed judgments about other areas of potential risks.

Over the last several years, the focus on threats from large commercial vessels and containerized cargo has been significant. As we continue to discuss the risks and threats to maritime container security, the department is also focusing on other threats to our ports, such as the kind demonstrated by the attack on the U.S.S. Cole or the French tanker, The Limburg. The USCG and CBP are working closely to expand our efforts to secure small maritime crafts. Although the overwhelming majority of small craft owners and operators are upstanding citizens and law-abiding mariners, various small vessels operate with great autonomy and anonymity in close proximity to critical maritime infrastructure and key resources, creating a potential for terrorist exploitation.

DHS believes that preventive, but reasonable, measures are necessary to address potential small vessel threats, ranging from smuggling Weapons of Mass Destruction (WMDs) across our borders, to their use as a water-borne improvised explosive device or as platforms for attacks against our nation's critical infrastructure. We are currently developing a National Strategy to address these risks by: (1) Implementing a layered approach; (2) leveraging a strong partnership with the small vessel community and public and private sectors to enhance maritime domain awareness; (3) leveraging technology to enhance our ability to detect, determine intent, and interdict small vessels when necessary; and (4) enhancing coordination, cooperation, and communication among various stakeholders, including Federal, state, local, tribal, and territorial agencies, as well as international partners.

The Department is working closely with other government departments and agencies, with industry, and the international community to establish workable solutions to improve supply chain security.

We recognize the importance of having a realistic schedule for technological development and the importance of establishing strong international and public-private partnerships. We applaud the ambitious goals established in the SAFE Port Act and continue to work energetically to implement them. I would like to thank the Senate Committee on Homeland Security and Governmental Affairs again for this opportunity to discuss our efforts within the context of the SAFE Port Act.

This completes my prepared statement. I would be happy to answer to any questions you may have.

Department of Justice

STATEMENT

OF

REGINALD I. LLOYD
UNITED STATES ATTORNEY
FOR THE DISTRICT OF SOUTH CAROLINA

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

CONCERNING

"ONE YEAR LATER: A PROGRESS REPORT ON THE SAFE PORT ACT"

PRESENTED ON

OCTOBER 16, 2007

STATEMENT OF REGINALD I. LLOYD
United States Attorney
District of South Carolina
Before the
Committee on Homeland Security and Governmental Affairs
United States Senate

October 16, 2007

Mr. Chairman, members of the Committee, I am Reginald Lloyd, the United States Attorney for the District of South Carolina. It is an honor to appear before you today to talk about a Port and Intermodal Security Initiative in Charleston, South Carolina called "Project SeaHawk". Some of you may be familiar with Project SeaHawk, but for those of you who are not, I would like to take a few minutes this morning to share with you what I believe is a truly successful example of federal, state, and local agencies working together very effectively to secure the Ports of South Carolina and to serve as a national model of innovation to enhance our nation's intermodal security.

SeaHawk's Mission

Project SeaHawk was established in March of 2003 as a congressionally-funded pilot project to enhance maritime and intermodal transportation security for Charleston and the South Carolina Ports. SeaHawk is currently operated under the direction and authority of the United States Attorney's Office in the District of South Carolina and serves as one of the District's counterterrorism/critical infrastructure initiatives through its Anti-Terrorism Advisory Council. The Project has four primary goals: First, to enhance the security of the intermodal environment in the Port of Charleston and other South Carolina Ports; second, to operate a unified Law Enforcement Task Force coordinating federal, state, and local resources; third, to develop a streamlined process to target illicit intermodal activity; and, finally, to serve as a national model and test-bed for innovative ideas.

The protection of our nation's maritime borders is a shared responsibility crossing multiple jurisdictional boundaries. While each federal agency responsible for maritime border security has a core mission at the Port, no national standard exists to facilitate coordination of resources, operations, or information and intelligence exchange with federal agencies or with state and local jurisdictions. This leads to potential gaps that may be exploitable by criminals or extremists thus increasing the vulnerability of the Ports and intermodal transportation. Since its inception, SeaHawk has sought to seal the seams between port and maritime security activities. SeaHawk does not replace the good work of the federal agencies who conduct their mission at the Port; rather it seeks to integrate those missions through co-location of federal, state, and local agencies; unity of effort; innovative development and deployment of technology; and information-sharing -- all of which can be exported to assist other U.S. Ports at the end of the pilot project. As a result, SeaHawk has been called a model for port and intermodal security throughout the nation.

SeaHawk Achievements

Since its establishment in March of 2003, Project SeaHawk has already achieved many of its envisioned goals and objectives as follows:

- Establishment of a full-time, multi-agency, co-located task force of federal, state, and local law enforcement personnel using a unified command structure to eliminate interagency rivalries, promote cooperation, and enhance information-sharing and investigative resources;
- Creation of a shared information environment for increased situational awareness of intermodal activity in the port by providing full and complete access of collected information to task force members;
- Development of an interagency intelligence section to provide direct support to law enforcement operations and investigations;
- Creation of a joint operations command center providing intermodal and maritime domain situational awareness and resource coordination;
- Development of an integrated and linked radiological detection and monitoring architecture; and
- Operation of a proactive maritime and intermodal security strategy to deter criminal or extremist-related illicit activities in South Carolina.

SeaHawk Partnerships

None of the SeaHawk objectives would have been accomplished without the strong partnerships established among the core agencies that have primary jurisdiction in securing our nation's maritime borders. Full-time personnel commitments to SeaHawk from the U.S. Coast Guard (USCG), Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), Defense Criminal Investigative Service (DCIS), South Carolina Law Enforcement Division (SLED), Charleston County Sheriff's Department, Mt. Pleasant Police Department, Charleston Police Department, North Charleston Police Department, Charleston Area Marine Law Enforcement Unit, and the South Carolina Ports Authority Police Department have ensured that SeaHawk's mission is truly integrated to serve and benefit the Port of Charleston. SeaHawk's mission is also enhanced by its co-location and strong working relationship with the FBI's Joint Terrorism Task Force (JTTF). In addition, SeaHawk is directly integrated with the South Carolina State Fusion Center and, as a result, shares and receives information providing situational awareness of criminal activity in and around the Port. SeaHawk has also begun discussions with other Ports in the region such as Savannah, Wilmington, and Norfolk with regard to how lessons learned at SeaHawk can assist them.

SeaHawk Structure and Staffing

SeaHawk operates through a Unified Command structure comprised of liaison officers from the USCG, CBP, ICE, and SLED and chaired by the Director of Project SeaHawk, an Assistant United States Attorney from the District of South Carolina. The

United States Attorney's Office has also provided the staff support functions for SeaHawk which includes Administrative, Intelligence, Plans, and Information Technology. DOJ also coordinates the State and Local Law Enforcement assets at SeaHawk. Each member of the Unified Command brings agency-unique resources that support SeaHawk's operations.

A SeaHawk Executive Steering Committee meets quarterly to receive information about the status of Project SeaHawk and provide input on long-term strategic and operational goals. The Steering Committee includes the United States Attorney, the Captain of the Port, the CBP Port Director, the Chief of the South Carolina Law Enforcement Division who also serves as the Director for Homeland Security for the District of South Carolina, the FBI Special-Agent-In-Charge (SAC) for South Carolina, the Resident-Agent-In-Charge for ICE, the Transportation Security Administration (TSA) Federal Security Director, and all sheriffs and police chiefs for the state and local law enforcement agencies who have personnel dedicated to SeaHawk. The use of the Unified Command to make daily and short-term decisions for SeaHawk operations and the SeaHawk Executive Steering Committee to provide input on long-term strategy and operations ensures that all agencies are all on the same page with regard to SeaHawk's goals and objectives.

Maritime Screening and Assessment Portal

One of the biggest challenges in establishing SeaHawk was the creation of a process and a security screening logic that would support the collective decision-making and security resource allocation of SeaHawk's Unified Command. This is being addressed through the development of an information and data-capture process in which multi-source information collected as part of the maritime and intermodal screening process is filtered through a data-logic model comprised of a variety of indicators of suspect activity. All activity identified as suspect in this process is subjected to a thorough review process, the results of which are provided to the Unified Command who meet daily and focus on reviewing a 96-hour window of pending activity within the Port. Issues identified in the Maritime Screening and Assessment Portal are individually discussed and addressed through the application of SeaHawk resources. The combined agencies represent a significant capability to investigate or address security issues that may arise. SeaHawk's Maritime Screening and Assessment Portal has proven to be effective as an information portal that operationalizes a comprehensive approach to conducting maritime and intermodal security.

SeaHawk Task Force Officers

At SeaHawk, the federal officers, special agents, and inspectors charged with securing our nation's maritime borders are augmented with task force officers from all of the surrounding local municipalities. Each of these local law enforcement officers are sworn special deputy U.S. Marshals who have received training to conduct searches and inspections. The real value of SeaHawk is the ability to pool limited resources and then apply them against a risk-based ranking of all identified security issues. In other words, the sum of the combined parts of SeaHawk is greater than the strengths or capabilities of

any one agency. Further, the combined group has a wider scope of jurisdictional authority than any one agency or activity. Every day, SeaHawk Task Force Officers are involved in a broad range of preventive security actions from conducting ship boardings to inspecting trucks and terminal yards. The SeaHawk Task Force Officers are clearly a force multiplier that enhance the security of the Port and send a clear message to all visiting foreign vessels about the thoroughness of Charleston's maritime security program. We believe that this proactive, preventive policing is a national model that achieves the unified approach that Congress and the public are looking for to protect critical infrastructures such as the Port.

Interagency Intelligence Program

Seahawk was established with the intent of using an intelligence effort to lead policing and prevention operations. The Seahawk intelligence team is a unique resource for the maritime security effort in South Carolina as no other Captain of the Port or Sector Commander in the USCG, nor Port Director in CBP, nor SAC in ICE has a similarly-sized or capable resource. The Seahawk intelligence team, which includes the USCG's field intelligence elements, conducts the review of all vessels and crew bound to the Port of Charleston and provides the results of that screening to the Unified Command on a daily basis so that they can plan mitigation actions. The intelligence team also provides situational awareness information to SeaHawk with regard to the global war on terrorism and its specific implications for South Carolina, including terrorism-related advisories pertaining to the intermodal environment in the U.S. and unique insights into the international maritime shipping community that includes suspect operating, management, crewing or business practices of a shipping enterprise that may operate a vessel bound to a Port in South Carolina.

SeaHawk Interagency Operations Center

Seahawk's Operations Center is the central hub of all maritime and intermodal security operations within the South Carolina complex. The Center was designed to enhance and facilitate information-sharing and joint operations. A variety of sensor and other information is received and displayed in the command center to enhance situational awareness of all intermodal activity occurring in the Ports. Ships can be followed with radar and video as they enter and leave the harbor area, special sensors monitor the environment for radiological materials and various information streams or intelligence feeds keep SeaHawk Task Force Officers and intelligence analysts apprised of ongoing events that may affect the security and continued safe operation of the Port of Charleston.

SeaHawk Technology

Seahawk has used its resources to improve maritime security and intermodal law enforcement and security capabilities across four broad areas. These areas include voice and data communications, law enforcement investigative and intelligence tools, information technology infrastructure, security and national security access, and a variety of sensor programs. One of the cutting-edge programs undertaken by Seahawk has been

a mobile radiological detection program that was designed to complement the fixed-array radiological detection program operated by CBP at the Port terminals and the USCG's smaller radiological sensor program used during ship boardings. The Seahawk mobile capability deploys a sensitive radiological sensor in a vehicle and a small boat. These mobile sensors can be used for patrols within the port, across all intersecting waterways, or location where there is a reported radiological threat. Radiological alerts identified by the mobile sensors are provided back to the Seahawk Operations Center for analysis. Seahawk has partnered with DHS' Domestic Nuclear Detection Office (DNDO) and TSA to develop and field this capability.

SeaHawk Budget

Total funding appropriated to DOJ for Project SeaHawk since fiscal year 2003 is $46.4 million dollars, and $41.4 million is available until expended. As of October 9, 2007, SeaHawk has expended and/or obligated approximately $38.5 million of the Project funds with the remaining approximately $7.7 million dollars budgeted, but not yet obligated. Based on its current budget, DOJ anticipates having funds to operate SeaHawk through September 2009. The fiscal year 2008 President's Budget proposes no additional funding and no rescission of unobligated balances for Project SeaHawk.

The most tangible SeaHawk legacy to South Carolina's maritime security is qualitative improvement to security infrastructure. In that regard, by the end of the pilot project, approximately 67% of the SeaHawk budget will have been expended to acquire or improve fixed assets at a cost of $31.1 million. These fixed assets are spread across the following broad areas and include the SeaHawk Operations Center; SeaHawk Maritime Screening and Assessment portal; SeaHawk information-sharing sources; state and local law enforcement equipment including vehicles and boats; radiological architecture; and the task force communications.

SeaHawk Upcoming Projects

In the remaining two years of the pilot project, SeaHawk has obligated funds for and is scheduled to complete a number of additional projects that will continue to integrate federal, state, and local law enforcement activities at the South Carolina Ports. These projects include a facility build-out to co-locate the USCG's Sector Command Center (SCC) with the SeaHawk Operations Center. We believe that SeaHawk's integration of the SCC, which is currently located in downtown Charleston, will enhance USCG's interoperability with all entities involved in the intermodal security of South Carolina Ports and will result in the development of a model interagency operations center as described in the Safe Port Act of October 2006.

In addition, we also plan to renovate an existing facility located adjacent to the Project SeaHawk Operations Center and relocate the SeaHawk Marine Law Enforcement Unit to that new facility. The Marine Unit is comprised of maritime law enforcement assets from multiple local jurisdictions who support and augment all maritime security operations now conducted by USCG, ICE, and CBP. The SeaHawk plan is to provide an upgraded facility to the Marine Unit that will allow the Marine Unit

to become a sustained law enforcement presence on the Port thereby greatly benefiting federal, state, and local law enforcement efforts.

SeaHawk Transition

Because Project SeaHawk was established prior to the full standup of DHS and funded by means of a congressional earmark to DOJ, it is not clear who will fund and sponsor SeaHawk when the pilot project ends. Based on an analysis of projected annual operating cost, SeaHawk could operate as it currently exists at a yearly cost of approximately $2.7M - $4.5M. Those projected costs include facility expenses; administration, training, and travel; information technology; and personnel costs. The Safe Port Act of October 2006 directed the Secretary of the DHS to establish interagency operation centers for port security at all high-priority ports not later than 3 years from the enactment of the Act and, we believe that, by the end of the pilot project, Project SeaHawk will have all of the necessary elements to serve as a national model for the "interagency operation centers" described in the Act. The DOJ and the United States Attorney's Office in the District of South Carolina remain focused on transitioning Project SeaHawk in a way that maximizes its return on the congressional investment entrusted to it in 2003.

I thank you very much for inviting me here and giving me the opportunity to talk to you about a project that is a true example of federal, state, and local governments working together at their best. I am very proud to be associated with Project SeaHawk, and I am happy to respond to any questions you may have.

GAO

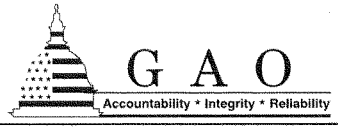
Testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, October 16, 2007

MARITIME SECURITY

One Year Later: A Progress Report on the SAFE Port Act

Statement of Stephen L. Caldwell, Director
Homeland Security and Justice Issues



GAO-08-171T

October 16, 2007

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-08-171T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

MARITIME SECURITY

One Year Later: A Progress Report on the SAFE Port Act

Why GAO Did This Study

Because the safety and economic security of the United States depend in substantial part on the security of its 361 seaports, the United States has a vital national interest in maritime security. The Security and Accountability for Every Port Act (SAFE Port Act), modified existing legislation and created and codified new programs related to maritime security. The Department of Homeland Security (DHS) and its U.S. Coast Guard, Transportation Security Agency, and U.S. Customs and Border Protection have key maritime security responsibilities. This testimony synthesizes the results of GAO's completed work and preliminary observations from GAO's ongoing work related to the SAFE Port Act pertaining to (1) overall port security, (2) security at individual facilities, and (3) cargo container security. To perform this work GAO visited domestic and overseas ports; reviewed agency program documents, port security plans, and post-exercise reports; and interviewed officials from the federal, state, local, private, and international sectors.

What GAO Recommends

GAO has made recommendations to DHS to develop strategic plans, better plan the use of its human capital, establish performance measures, and otherwise improve program operations. DHS has generally concurred with our recommendations and is making progress implementing them. We provided a draft of this information to DHS agencies and incorporated technical comments as appropriate.

To view the full product, including the scope and methodology, click on GAO-08-171T. For more information, contact Stephen Caldwell (202) 512- 9610 or caldwells@gao.gov.

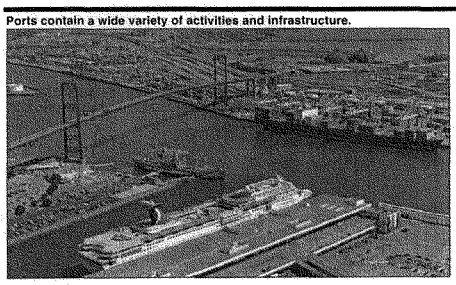
What GAO Found

Federal agencies have improved overall port security efforts by establishing committees to share information with local port stakeholders, taking steps to establish interagency operations centers to monitor port activities, conducting operations such as harbor patrols and vessel escorts, writing port-level plans to prevent and respond to terrorist attacks, testing such plans through exercises, and assessing the security at foreign ports. However, these agencies face resource constraints and other challenges trying to meet the SAFE Port Act's requirements to expand these activities. For example, the Coast Guard faces budget constraints in trying to expand its current command centers and include other agencies at the centers.

Similarly, private facilities and federal agencies have taken action to improve security at about 3,000 individual facilities by writing facility-specific security plans, inspecting facilities to ensure they are complying with their plans, and developing special identification cards for workers to prevent terrorists from getting access to secure areas. Federal agencies face challenges trying to meet the act's requirements to expand the scope or speed the implementation of such activities. For example, the Transportation Security Agency missed the act's July 2007 deadline to implement the identification card program at 10 selected ports because of delays in testing equipment and procedures.

Federal programs related to the security of cargo containers have also improved as agencies are enhancing systems to identify high-risk cargo, expanding partnerships with other countries to screen containers before they depart for the United States, and working with international organizations to develop a global framework for container security. Federal agencies face challenges implementing container security aspects of the SAFE Port Act and other legislation. For example, Customs and Border Protection must test and implement a new program to screen 100 percent of all incoming containers overseas—a departure from its existing risk-based programs.

Ports contain a wide variety of activities and infrastructure.



Source: United States Coast Guard.

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss port and cargo security functions related to provisions of the Security and Accountability for Every Port Act (SAFE Port Act).[1] The nation's 361 seaports are the gateway for more than 80 percent of our foreign trade. Worldwide, some 30 large ports, spread across North America, Asia, and Europe constitute the world's primary, interdependent trading web. Much of this trade—particularly high-value cargo—enters and leaves in cargo containers.

In our post 9/11 environment, however, the potential security weaknesses presented by these economic gateways have become apparent. Sprawling, easily accessible by water and land, often close to urban areas, and containing facilities that represent opportunities for inflicting significant damage as well as causing economic mayhem, ports present potential terrorist targets. Further, they are potential conduits for weapons prepared elsewhere and concealed in cargo designed to move quickly to many locations beyond the ports themselves.

Since the 9/11 attacks, Congress has established a new port security framework—much of which was set in place by the Maritime Transportation Security Act (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 major 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; (3) developing the Transportation Worker Identification Credential (TWIC), a biometric identification card to help restrict access to secure areas to only authorized personnel; and (4) establishing of a process to assess foreign ports, from which vessels depart on voyages to the United States. The Department of Homeland Security (DHS)—itself a creation of the new security environment brought on by the 9/11 attacks—administers much of this framework, which also attempts to balance security priorities with the need to facilitate legitimate trade.

[1]Pub. L. No. 109-347, 120 Stat. 1884 (2006).

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

The SAFE Port Act, which was enacted in October 2006, is one of the latest additions to this port security framework. The act made a number of adjustments to programs within this framework, creating additional programs or lines of effort and altering others. The SAFE Port Act created and codified new programs and initiatives, and amended some of the original provisions of MTSA. The SAFE Port Act included provisions that (1) codified the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT), two programs administered by U.S. Customs and Border Protection (CBP) to help reduce threats associated with cargo shipped in containers, as well as established the Domestic Nuclear Detection Office (DNDO), which is responsible for conducting research, development, testing, and evaluation of radiation detection equipment; (2) required interagency operational centers where agencies organize to fit the security needs of the port area at selected ports; (3) set an implementation schedule and fee restrictions for TWIC; (4) required that all containers entering high volume U.S. ports be scanned for radiation sources by December 31, 2007; and (5) required additional data be made available to CBP for targeting cargo containers for inspection.[3] This statement summarizes our recently completed and ongoing work.

Over the past several years, we have examined and reported on many of the programs in this new port security framework. This statement is designed both to provide an overview of what we have earlier reported about these programs and to describe, with the preliminary information available, what DHS is doing as a result of the SAFE Port Act requirements and the challenges the agency faces in doing so. This statement discusses three key areas and 19 programs, as shown in table 1.

[3]The Implementing Recommendations of the 9/11 Commission Act of 2007 amended a SAFE Port Act provision on scanning all United States bound containers at foreign ports. See Pub. L. No. 110-53, §1701(a), 121 Stat. 266, 489-90. This amendment is discussed later in this testimony.

Table 1: **Summary of Three Key Areas and 19 Programs in This Statement**

Program	Description
Overall port security	
Area Maritime Security Committees	Committees consisting of key port stakeholders who share information and develop port security plans.
Interagency Operational Centers	Command centers where agencies share information, coordinate their activities, and coordinate joint efforts.
Port security operations	Activities to maintain security and deter attacks, such as boat patrols and vessel escorts.
Area Maritime Security Plans	Plan laying out local port vulnerabilities, responsibilities, and some response actions.
Port security exercises	Exercises among various port stakeholders to test the effectiveness of port security plans.
Evaluations of security at foreign ports	Coast Guard program where officers visit and assess security conditions at foreign ports.
Port facility security	
Port facility security plans	Plans that include, among other things, operational and physical security measures and procedures for responding to security threats.
Port facility security compliance monitoring	Coast Guard review of port facility security plans and compliance with such plans.
Transportation Worker Identification Credential	Biometric identification cards to be issued to port workers to help secure access to areas of ports.
Background checks	DHS requirements for persons who enter secure or restricted areas or transport hazardous cargo.
Container security	
Automated Targeting System	Risk-based decision system to determine cargo shipped in containers requiring inspection.
Customs In-Bond System	The in-bond system allows goods to transit the United States without officially entering U.S. commerce.
Container Security Initiative	Stationing CBP officers at foreign ports to help identify and inspect high-risk cargo to be shipped in containers destined for the United States.
Customs-Trade Partnership Against Terrorism	Partnership between private companies and CBP to improve international supply chain security.
Promoting Global Standards	Efforts to work with members of the customs and trade community on approaches to standardizing supply chain security.
Domestic Nuclear Detection Office	Research, development, testing and evaluation of radiation detection equipment to prevent nuclear or radiological materials from entering the United States.
Megaports Initiative	Radiation detection technology at foreign ports to stop the proliferation of weapons of mass destruction.
Secure Freight Initiative	Combines Container Security Initiative scanning with Megaports Initiative radiation detection at foreign ports.
100 Percent Container Scanning at Foreign Ports	Scanning by nonintrusive imaging and radiation detection equipment of all cargo containers at foreign ports inbound to the United States by 2012.

Source: GAO.

This statement is organized into three main areas, as follows:

- programs related to overall port security, such as those for coordinating among stakeholders, conducting security operations, developing security plans, and conducting exercises to test security procedures;
- programs related specifically to security at individual facilities, such as examining security measures and ensuring that only properly cleared individuals have access to port areas; and,
- programs related specifically to cargo container security, such as screening containers at ports both here and abroad and forming partnerships with the private sector.

This statement is based primarily on a body of work we completed in response to congressional requests and mandates for analysis of maritime, port, and cargo security efforts of the federal government.[4] In some cases, we provide preliminary observations from our ongoing work. Thus, the timeliness of the data that were the basis for our prior reporting varies depending on when our products were issued and the preliminary observations are subject to change as we complete our work.

We conducted all of our work in accordance with generally accepted government auditing standards. To perform both our completed and ongoing work we visited several domestic and overseas ports; reviewed agency program documents, port security plans, and post-exercise reports, and other documents; and interviewed officials from the federal, state, local, private, and international sectors. The officials were from a wide variety of port stakeholders to include Coast Guard, CBP, TSA, port authorities, terminal operators, vessel operators, foreign governments, and international organizations. While this body of work does not cover all the provisions of the SAFE Port Act, it does cover a wide range of these provisions as shown in Table 1.

We provided a draft of the information in this testimony to DHS. DHS provided technical comments, which we incorporated as appropriate.

[4]A list of related GAO products may be found at the end of this testimony.

Summary

Regarding overall security at U.S. ports, federal agencies have taken a number of steps to improve maritime security and implement many aspects of MTSA. The Coast Guard has established Area Maritime Security Committees (AMSCs) to coordinate activities and share information among the various stakeholders at specific ports. The Coast Guard also has local operations centers where it coordinates its activities. The SAFE Port Act requires that all high-priority ports have interagency operational centers no later than 3 years after the act's enactment.[5] Given the capabilities and organization of its existing centers, the Coast Guard estimates it will cost $260 million to meet this requirement and has begun evaluating ways to expand current centers to meet the act's requirements. The Coast Guard also conducts a number of operations at U.S. ports to deter and prevent terrorist attacks, such as harbor patrols or vessel escorts. While the Coast Guard has set specific requirements for the level of these activities, they are not always able to complete them at some ports due to resource constraints. The Coast Guard, in collaboration with the MTSA-required AMSCs, has written port-specific security plans to deter and respond to terrorist attacks—but these plans do not fully address recovery issues (e.g., how to reopen a port after an attack) and natural disasters (e.g., hurricanes or earthquakes). The Coast Guard, again in collaboration with the AMSCs, has sponsored exercises to test the port security plans. But the Coast Guard will face challenges, such as including recovery scenarios, expanding the program in line with SAFE Port Act requirements to include new scenarios and improve the communication of lessons learned during exercises. Finally, security in our own ports is dependent on security in foreign ports where vessels depart for the United States. The Coast Guard has implemented a MTSA-required program to work with foreign countries to inspect and strengthen security at their ports, but will likely face challenges in hiring and training sufficient staff to meet SAFE Port Act requirements to increase the frequency of such inspections. A related challenge is that many of the foreign countries that the Coast Guard has visited—to include several countries in the Caribbean Basin—are poor and lack the resources to make major improvements on their own.

Regarding security at approximately 3,000 individual facilities, federal agencies and the facilities themselves have taken positive steps. In line

[5]The SAFE Port Act did not define "high-priority ports," but the Coast Guard identified a number of factors that it used in determining which ports are high-priority, including risk assessment data, port criticality ratings, and existing investments in facilities.

with MTSA, facilities have written and implemented security plans and the Coast Guard has generally inspected such facilities to verify compliance and take enforcement actions where necessary. The SAFE Port Act increased requirements for the scope and frequency of these activities, doubling the frequency of Coast Guard inspections of facilities and requiring unannounced inspections. The Coast Guard has issued guidance on how the new requirements are to be met, but the impact on resource needs remains uncertain. To control access to individual facilities at ports, MTSA required a program to develop secure and biometric transportation worker identification credentials (TWIC). Under the program, transportation workers would have to undergo background checks to receive TWIC cards. The SAFE Port Act established a July 1, 2007 milestone for the implementation of the TWIC program at the 10 highest risk ports. The Transportation Security Administration (TSA), the agency responsible for implementing TWIC, did not meet the July deadline, citing the need to conduct additional testing of the systems and technologies that will be used to enroll the estimated 770,000 workers that are required to obtain a TWIC card. Finally, while DHS has created the Screening Coordination Office (SCO) to better coordinate TWIC with other programs that require background checks, it will be challenged to fully coordinate all the DHS screening programs, ensuring that the cost and benefits of potentially eliminating or keeping different screening programs are properly considered, and coordinating with other federal screening programs outside DHS.

Regarding the security of cargo containers—which carry a large volume of the world's commerce through our ports—CBP has developed a layered security strategy to identify and inspect containers that may contain terrorist weapons of mass destruction (WMD). CBP has refined its Automated Targeting System (ATS) to better analyze shipping information and identify suspicious containers. However, it does not have the most up to date information for certain containers—those that transit beyond the ports as part of the in-bond system, which allows goods to transit the United States without officially entering U.S. commerce. CBP has expanded and improved the management of its Container Security Initiative (CSI) where the agency places U.S. customs officials in foreign ports to help target and inspect suspicious containers. Similarly, CBP has expanded and improved the management of its Customs-Trade Partnership Against Terrorism (C-TPAT) where private companies agree to improve the security of their supply chains in exchange for reduced scrutiny over their shipments. The SAFE Port Act codified these two programs into law and required enhanced management and oversight of these programs. CBP is working to meet these new requirements, but our

prior and ongoing work suggests that it may face challenges setting equipment standards and conducting validations of company practices. Furthermore, our work has shown that the Domestic Nuclear Detection Office (DNDO) needs to take additional action to ensure adequate testing of radiation detection equipment that CBP uses at domestic ports to scan containers for radiation. The Department of Energy (DOE) is expanding its Megaports program that complements CSI by providing foreign nations with radiation detection equipment to scan containers moving through their ports. The SAFE Port Act also required pilot programs to test new technologies or combine existing technologies to test the feasibility of scanning all U.S.-bound containers overseas. More recent legislation required that all containers bound for the United States be scanned overseas by 2012 with possible extensions for individual ports. Our preliminary observations suggest this requirement potentially creates new challenges for CBP in terms of integrating this with existing programs, working with foreign governments, overcoming logistical barriers, testing new technology, determining resource requirements and responsibilities, and other issues.

We have reviewed many of the MTSA and SAFE Port Act related programs and made prior recommendations to the appropriate agencies to develop strategic plans, better plan their use of human capital, establish performance measures, and otherwise improve the operations of these programs. In general, these agencies have concurred with our recommendations and are making progress implementing them.

Prior Actions Have Improved Port Security, but Issues Remain

Port security overall has improved because of the development of organizations and programs such as AMSCs, Area Maritime Security Plans (AMSPs), maritime security exercises, and the International Port Security Program, but challenges to successful implementation of these efforts remain. Additionally, agencies may face challenges addressing the additional requirements directed by the SAFE Port Act, such as a provision that DHS establish interagency operational centers at all high-priority ports. AMSCs and the Coast Guard's sector command centers have improved information sharing, but the types and ways information is

shared varies.[6] AMSPs, limited to security incidents, could benefit from unified planning to include an all-hazards approach. Maritime security exercises would benefit from timely and complete after action reports, increased collaboration across federal agencies, and broader port level coordination. The Coast Guard's International Port Security Program is currently evaluating the antiterrorism measures maintained at foreign seaports.

Area Maritime Security Committees Share Information and Coast Guard Plans to Expand Interagency Operational Centers

Two main types of forums have developed for agencies to coordinate and share information about port security: area committees and Coast Guard sector command centers. AMSCs serve as a forum for port stakeholders, facilitating the dissemination of information through regularly scheduled meetings, issuance of electronic bulletins, and sharing key documents. MTSA provided the Coast Guard with the authority to create AMSCs—composed of federal, state, local, and industry members—that help to develop the AMSP for the port. As of August 2007, the Coast Guard had organized 46 AMSCs. Each has flexibility to assemble and operate in a way that reflects the needs of its port area, resulting in variations in the number of participants, the types of state and local organizations involved, and the way in which information is shared. Some examples of information shared includes assessments of vulnerabilities at specific port locations, information about potential threats or suspicious activities, and Coast Guard strategies intended for use in protecting key infrastructure. As part of an ongoing effort to improve its awareness of the maritime domain, the Coast Guard developed 35 sector command centers, four of which operate in partnership with the U.S. Navy.[7]

[6]The Coast Guard has implemented a new field command structure that is designed to unify previously disparate Coast Guard units, such as air stations and marine safety offices, into 35 different integrated commands, called sectors. At each of these sectors, the Coast Guard has placed management and operational control of these units and their associated resources under the same commanding officer.

[7]The Coast Guard shares some responsibilities with the U.S. Navy at four of these locations. These centers are located in Hampton Roads, Virginia; Jacksonville, Florida; San Diego, California; and Seattle, Washington.

We have previously reported that both of these types of forums have helped foster cooperation and information-sharing.[8] We further reported that AMSCs provided a structure to improve the timeliness, completeness, and usefulness of information sharing between federal and nonfederal stakeholders. These committees improved upon previous information-sharing efforts because they established a formal structure and new procedures for sharing information. In contrast to AMSCs, the Coast Guard's sector command centers can provide continuous information about maritime activities and involve various agencies directly in operational decisions using this information. We have reported that these centers have improved information sharing, and the types of information and the way information is shared varies at these centers depending on their purpose and mission, leadership and organization, membership, technology, and resources.

The SAFE Port Act called for establishment of interagency operational centers, directing the Secretary of DHS to establish such centers at all high-priority ports no later than 3 years after the Act's enactment. The act required that the centers include a wide range of agencies and stakeholders and carry out specified maritime security functions. In addition to authorizing the appropriation of funds and requiring DHS to provide the Congress a proposed budget and cost-sharing analysis for establishing the centers, the act directed the new interagency operational centers to utilize the same compositional and operational characteristics of existing sector command centers. According to the Coast Guard, none of the 35 centers meets the requirements set forth in the SAFE Port Act. Nevertheless, the four centers the Coast Guard operates in partnership with the Navy are a significant step in meeting these requirements, according to a senior Coast Guard official. The Coast Guard is currently piloting various aspects of future interagency operational centers at existing centers and is also working with multiple interagency partners to

[8]See GAO, *Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention*, GAO-05-394 (Washington, D.C.: Apr. 15, 2005); *Maritime Security: Enhancements Made, but Implementation and Sustainability Remain Key Challenges*, GAO-05-448T (Washington, D.C.: May 17, 2005); and *Maritime Security: Information-Sharing Efforts Are Improving*, GAO-06-933T (Washington, D.C.: Jul. 10, 2006).

further develop this project.[9] DHS has submitted the required budget and cost-sharing analysis proposal, which outlines a 5-year plan for upgrading its centers into future interagency operations centers to continue to foster information sharing and coordination in the maritime domain. The Coast Guard estimates the total acquisition cost of upgrading 24 sectors that encompass the nation's high priority ports into interagency operations centers will be approximately $260 million, to include investments in information system, sensor network, facilities upgrades and expansions. According to the Coast Guard, future interagency operations centers will allow the Coast Guard and its partners to use port surveillance with joined tactical and intelligence information, and share this data with port partners working side-by-side in expanded facilities.

In our April 2007 testimony, we reported on various challenges the Coast Guard faces in its information sharing efforts.[10] These challenges include obtaining security clearances for port security stakeholders and creating effective working relationships with clearly defined roles and responsibilities. In our past work, we found the lack of federal security clearances among area committee members had been routinely cited as a barrier to information sharing.[11] In turn, this inability to share classified information may limit the ability to deter, prevent, and respond to a potential terrorist attack. The Coast Guard, having lead responsibility in coordinating maritime information, has made improvements to its program for granting clearances to area committee members and additional clearances have been granted to members with a need to know.[12] In addition, the SAFE Port Act includes a specific provision requiring DHS to sponsor and expedite security clearances for participants in interagency operational centers. However, the extent to which these

[9]According to the Coast Guard, these multiple interagency partners include Customs and Border Protection, Immigration and Customs Enforcement, Department of Defense, the Secure Border Initiative Network (SBInet) Program Office, and State and local partners. A pilot interagency operational center located in Charleston, South Carolina, known as Project Seahawk, is managed by the Department of Justice. It was created through an appropriation in the fiscal year 2003 Consolidated Appropriations Resolution (Pub. L. No. 108-7, 117 Stat. 11, 53 (2003.)).

[10]See GAO, *Maritime Security: Observations on Selected Aspects of the SAFE Port Act.* GAO-07-754T. (Washington, D.C.: Apr. 26, 2007).

[11]See GAO-06-933T and GAO-05-394.

[12]In July 2007, the Coast Guard reported having granted security clearances to 212 area committee members with a need to know, which is an improvement from July 2006, when we reported 188 out of 467 members had received a security clearance to date.

efforts will ultimately improve information sharing is not yet known. As the Coast Guard expands its relationships with multiple interagency partners, collaborating and sharing information effectively under new structures and procedures will be important. While some of the existing centers achieved results with existing interagency relationships, other high-priority ports might face challenges establishing new working relationships among port stakeholders and implementing their own interagency operational centers. Finally, addressing potential overlapping responsibilities —such as leadership roles for the Coast Guard and its interagency partners—will be important to ensure that actions across the various agencies are clear and coordinated.

Operations to Provide Overall Port Security Face Resource Constraints

As part of its operations, the Coast Guard has also imposed additional activities to provide overall port security. The Coast Guard's operations order, Operation Neptune Shield, first released in 2003, specifies the level of security activities to be conducted. The order sets specific activities for each port; however, the amount of each activity is established based on the port's specific security concerns. Some examples of security activities include conducting waterborne security patrols, boarding high-interest vessels, escorting vessels into ports, and enforcing fixed security zones. When a port security level increases, the amount of activity the Coast Guard must conduct also increases.[13] The Coast Guard uses monthly field unit reports to indicate how many of its security activities it is able to perform. Our review of these field unit reports indicates that many ports are having difficulty meeting their port security responsibilities, with resource constraints being a major factor. In an effort to meet more of its security requirements, the Coast Guard uses a strategy that includes partnering with other government agencies, adjusting its activity requirements, and acquiring resources. Despite these efforts, many ports are still having difficulty meeting their port security requirements. The Coast Guard is currently studying what resources are needed to meet certain aspects of its port security program, but to enhance the effectiveness of its port security operations, a more comprehensive study to determine all additional resources and changes to strategy to meet minimum security requirements may be needed.

[13]The Coast Guard uses a three-tiered system of Maritime Security (MARSEC) levels consistent with DHS's Homeland Security Advisory System (HSAS). MARSEC levels are designed to provide a means to easily communicate pre-planned scalable responses to increased threat levels.

Area Maritime Security Plans Are in Place but Need to Address Recovery and Natural Disasters

Implementing regulations for MTSA specified that AMSPs include, among other things, operational and physical security measures in place at the port under different security levels, details of the security incident command and response structure, procedures for responding to security threats including provisions for maintaining operations in the port, and procedures to facilitate the recovery of the marine transportation system after a security incident. A Coast Guard Navigation and Vessel Inspection Circular (NVIC) provided a common template for AMSPs and specified the responsibilities of port stakeholders under them.[14] As of September 2007, 46 AMSPs are in place at ports around the country. The Coast Guard approved the plans by June 1, 2004, and MTSA requires that they be updated at least every 5 years.

The SAFE Port Act added a requirement to AMSPs, which specified that they include recovery issues by identifying salvage equipment able to restore operational trade capacity. This requirement was established to ensure that the waterways are cleared and the flow of commerce through United States ports is reestablished as efficiently and quickly as possible after a security incident. While the Coast Guard sets out the general priorities for recovery operations in its guidelines for the development of AMSPs, we have found that this guidance offers limited instruction and assistance for developing procedures to address recovery situations.

The Maritime Infrastructure Recovery Plan (MIRP) recognizes the limited nature of the Coast Guard's guidance and notes the need to further develop recovery aspects of the AMSPs.[15] The MIRP provides specific recommendations for developing the recovery sections of the AMSPs. The AMSPs that we reviewed often lacked recovery specifics and none had been updated to reflect the recommendations made in the MIRP. The Coast Guard is currently updating the guidance for the AMSPs and aims to complete the updates by the end of calendar year 2007 so that the guidance will be ready for the mandatory 5-year re-approval of the AMSPs in 2009. Coast Guard officials commented that any changes to the recovery section would need to be consistent with the national protocols developed

[14]NVICs provide detailed guidance about enforcement or compliance with certain Coast Guard safety regulations and programs. NVIC 9-02, most recently revised on October 27, 2005, detailed requirements for AMSPs.

[15]The MIRP, one of the eight supporting plans of the National Strategy for Maritime Security, is intended to facilitate the restoration of maritime commerce after a terrorist attack or natural disaster.

for the SAFE Port Act.[16] Additionally, related to recovery planning, the Coast Guard and CBP have developed specific interagency actions focused on response and recovery. This should provide the Coast Guard and CBP with immediate security options for the recovery of ports and commerce.

Further, AMSPs generally do not address natural disasters (i.e., they do not have an all-hazards approach).[17] In a March 2007 report examining how ports are dealing with planning for natural disasters such as hurricanes and earthquakes, we noted that AMSPs cover security issues but not other issues that could have a major impact on a port's ability to support maritime commerce.[18] As currently written, AMSPs are concerned with deterring and, to a lesser extent, responding to security incidents. We found, however, that unified consideration of all risks—natural and man-made—faced by a port may be beneficial. Because of the similarities between the consequences of terrorist attacks and natural or accidental disasters, much of the planning for protection, response, and recovery capabilities is similar across all emergency events. Combining terrorism and other threats can thus enhance the efficiency of port planning efforts. This approach also allows port stakeholders to estimate the relative value of different mitigation alternatives. The exclusion of certain risks from consideration, or the separate consideration of a particular type of risk, raises the possibility that risks will not be accurately assessed or compared, and that too many or too few resources will be allocated toward mitigation of a particular risk.

As ports continue to revise and improve their planning efforts, available evidence indicates that by taking a systemwide approach and thinking strategically about using resources to mitigate and recover from all forms of disaster, ports will be able to achieve the most effective results. AMSPs provide a useful foundation for establishing an all-hazards approach. While the SAFE Port Act does not call for expanding AMSPs in this manner, it does contain a requirement that natural disasters and other emergencies

[16]DHS released the Strategy to Enhance the International Supply Chain in July 2007. This strategy contains a plan to speed the resumption of trade in the event of a terrorist on our ports or waterways as required in the SAFE Port Act.

[17]All hazards emergency preparedness efforts seek to prepare all sectors of American society—business, industry and non profit; territorial, local, and tribal governments, and the general public—for all hazards the nation may face, i.e., any large-scale emergency event, including terrorist attacks and natural or accidental disasters.

[18]See GAO, *Port Risk Management: Additional Federal Guidance Would Aid Ports in Disaster Planning and Recovery*, GAO-07-412 (Washington, D.C.: Mar. 28, 2007).

be included in the scenarios to be tested in the Port Security Exercise Program. On the basis of our prior work, we found there are challenges in using AMSCs and AMSPs as the basis for broader all-hazards planning. These challenges include determining the extent that security plans can serve all-hazards purposes. We recommended that DHS encourage port stakeholders to use the AMSCs and MTSA-required AMSPs to discuss all-hazards planning. DHS concurred with this recommendation.

Maritime Security Exercises Require a Broader Scope and Participation

The Coast Guard Captain of the Port and the AMSC are required by MTSA regulations to conduct or participate in exercises to test the effectiveness of AMSPs annually, with no more than 18 months between exercises. These exercises—which have been conducted for the past several years—are designed to continuously improve preparedness by validating information and procedures in the area plan, identifying weaknesses and strengths, and practicing command and control within an incident command/unified command framework. In August 2005, the Coast Guard and the TSA initiated the Port Security Training Exercise Program (PortSTEP)—an exercise program designed to involve the entire port community, including public governmental agencies and private industry, and intended to improve connectivity of various surface transportation modes and enhance AMSPs. Between August 2005 and October 2007, the Coast Guard expected to conduct PortSTEP exercises for 40 area committees and other port stakeholders. Additionally, the Coast Guard initiated its own Area Maritime Security Training and Exercise Program (AMStep) in October 2005. This program was also designed to involve the entire port community in the implementation of the AMSP. Between the two programs, PortSTEP and AMStep, all AMSCs have received a port security exercise each year since inception.

The SAFE Port Act included several new requirements related to security exercises, such as establishing a Port Security Exercise Program to test and evaluate the capabilities of governments and port stakeholders to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism, natural disasters, and other emergencies at facilities that MTSA regulates. The act also required the establishment of a port security exercise improvement plan process that would identify, disseminate, and monitor the implementation of lessons learned and best practices from port security exercises.

Though we have not specifically examined compliance with these new requirements, our work in examining past exercises suggests that implementing a successful exercise program faces several challenges.[10] These challenges include setting the scope of the program to determine how exercise requirements in the SAFE Port Act differ from area committee exercises that are currently performed. This is especially true for incorporating recovery scenarios into exercises. In this past work, we also found that Coast Guard terrorism exercises frequently focused on prevention and awareness, but often did not include recovery activities. According to the Coast Guard, with the recent emphasis on planning for recovery operations, it has held several exercises over the past year that have included in part, or solely, recovery activities. It will be important that future exercises also focus on recovery operations so public and private stakeholders can cover gaps that might hinder commerce after a port incident. Other long-standing challenges include completing after-action reports in a timely and thorough manner and ensuring that all relevant agencies participate. According to the Coast Guard, as the primary sponsor of these programs, it faces a continuing challenge in getting comprehensive participation in these exercises.

The Coast Guard Is Evaluating the Security of Foreign Ports, but Faces Resource Challenges

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 develop a program to assess security measures in foreign ports and, among other things, recommend steps necessary to improve security measures in those ports. The Coast Guard established this 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

[10]See GAO, *Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention*, GAO-05-170 (Washington, D.C.: Jan. 14, 2005); and GAO-07-412.

Security (ISPS) Code.[20] 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. The conditions of these visits, such as timing and locations, are negotiated between the Coast Guard and the host nation. Coast Guard officials also make annual visits to the countries to obtain additional observations on the implementation of security measures and ensure deficiencies found during the country visits are addressed.[21]

Both the SAFE Port Act and other congressional directions have called for the Coast Guard to increase the pace of its visits to foreign countries. Although MTSA did not set a time frame for completion of these visits, the Coast Guard initially set a goal to visit the approximately 140 countries that conduct maritime trade with the United States by December 2008. In September 2006, the conference report accompanying the fiscal year 2007 DHS Appropriations Act directed the Coast Guard to "double the amount" at which it was conducting its visits.[22] Subsequently, in October 2006, the SAFE Port Act required the Coast Guard to reassess security measures at the foreign ports every 3 years. Coast Guard officials said they will comply with the more stringent requirements and will reassess countries on a 2-year cycle. With the expedited pace, the Coast Guard now expects to assess all countries by March 2008, after which reassessments will begin.

We are currently conducting a review of the Coast Guard's International Port Security Program that evaluates the Coast Guard's implementation of international enforcement programs. The report, expected to be issued in early 2008, will cover issues related to the program, such as the extent to

[20]The International Port Security Program uses the ISPS Code as the benchmark by which it measures the effectiveness of a country's anti-terrorism measures in a port. The code was developed after the 9/11 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.

[21]In addition to the Coast Guard visiting the ports of foreign countries under this program, countries can also make reciprocal visits to U.S. ports to observe U.S. implementation of the ISPS Code, obtaining ideas for implementation of the code in their ports and sharing best practices for security.

[22]See H.R. Conf. Rep. No. 109-699, at 142 (2006).

which the program is using a risk-based approach in carrying out its work, what challenges the program faces as it moves forward, and the extent to which the observations collected during the country visits are used by other programs such as the Coast Guard's port state control inspections and high interest vessel boarding programs.

As of September 2007, the Coast Guard reported that it has visited 109 countries under this program and plans to visit another 29 more by March 2008.[23] For the countries for which the Coast Guard has issued a final report, the Coast Guard reported that most had "substantially implemented the security code," while a few countries were found to have not yet implemented the ISPS Code and will be subject to a reassessment or other sanctions. The Coast Guard also found several facilities needing improvements in areas such as access controls, communication devices, fencing, and lighting.

While our review is still preliminary, Coast Guard officials told us that to plan and prepare for the next cycle of reassessments that are to begin next year, they are considering modifying their current visit methodology to incorporate a risk-based approach to prioritize the order and intensity of the next round of country visits. To do this, they have consulted with a contractor to develop an updated country risk prioritization model. Under the previous model, the priority assigned to a country for a visit was weighted heavily towards the volume of U.S. trade with that country. The new model being considered is to incorporate other factors, such as corruption and terrorist activity levels within the countries. Program officials told us that the details of this revised approach have yet to be finalized.

Coast Guard officials told us that as they complete the first round of visits and move into the next phase of revisits, challenges still exist in implementing the program. One challenge identified was that the faster rate at which foreign ports will now be reassessed will require hiring and training new staff—a challenge the officials expect will be made more difficult because experienced personnel who have been with the program since its inception are being transferred to other positions as part of the Coast Guard's rotational policy. These officials will need to be replaced with newly assigned personnel.

[23]There are approximately 140 countries that are maritime trading partners with the United States.

Reluctance by some countries to allow the Coast Guard to visit their ports due to concerns over sovereignty was another challenge cited by program officials in completing the first round of 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 they begin to revisit countries as part of the program's next phase, program officials stated that sovereignty concerns may still be an issue. Some countries may be reluctant to host a comprehensive country visit on a recurring basis because they believe the frequency—once every 2 to 3 years—is too high. Sovereignty also affects the conditions of the visits, such as timing and locations, because such visits are negotiated between the Coast Guard and the host nation. Thus the Coast Guard team making the visit could be precluded from seeing locations that are not in compliance.

Another challenge program officials cite is having limited ability to help countries build on or enhance their capacity to implement the ISPS Code requirements. For example, the SAFE Port Act required that GAO report on various aspects of port security in the Caribbean Basin. We earlier reported that although the Coast Guard found that most of the countries had substantially implemented the ISPS Code, some facilities needed to make improvements or take additional measures.[24] In addition, our discussions with facility operators and government officials in the region indicated that assistance—such as additional training—would help enhance their port security. 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 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

[24]See GAO, *Information on Port Security in the Caribbean Basin*, GAO-07-804R, (Washington, D.C.: Jun. 29, 2007).

Dominican Republic and the Bahamas). Program officials indicated that as part of reexamining the approach for the program's next phase, they will also consider possibilities to improve the program's ability to provide training and capacity building to countries when a need is identified.

Port Facility Security Efforts Continue, but Additional Evaluation is Needed

To improve the security at individual facilities at ports, many long-standing programs are underway. However, new challenges to their successful implementation have emerged. The Coast Guard is required to conduct assessments of security plans and facility compliance inspections, but faces challenges in staffing and training to meet the SAFE Port Act's additional requirements such as the sufficiency of trained personnel and guidance to conduct facility inspections. TSA's TWIC program has addressed some of its initial program challenges, but will continue to face additional challenges as the program rollout continues. Many steps have been taken to ensure that transportation workers are properly screened, but redundancies in various background checks have decreased efficiency and highlighted the need for increased coordination.

The Coast Guard's Compliance Monitoring of Maritime Facilities Identifies Deficiencies, but Program Effectiveness Overall Has Not Been Evaluated

MTSA and its implementing regulations required owners and operators of certain maritime facilities (e.g., power stations, chemical manufacturing facilities, and refineries that are located on waterways and receive foreign vessels) to conduct assessments of their security vulnerabilities, develop security plans to mitigate these vulnerabilities, and implement measures called for in the security plans by July 1, 2004. Under the Coast Guard regulations, these plans are to include items such as measures for access control, responses to security threats, and drills and exercises to train staff and test the plan.[25] The plans are "performance-based," meaning that the Coast Guard has specified the outcomes it is seeking to achieve and has given facilities responsibility for identifying and delivering the measures needed to achieve these outcomes.

Under MTSA, Coast Guard guidance calls for the Coast Guard to conduct one on-site facility inspection annually to verify continued compliance with the plan. The SAFE Port Act, enacted in 2006, required the Coast Guard to conduct at least two inspections—one of which was to be unannounced—of each facility annually. We currently have ongoing work that reviews the Coast Guard's oversight strategy under MTSA and SAFE Port Act requirements. The report, expected later this year, will cover,

[25]Requirements for security plans for facilities are found in 33 C.F.R. Part 105, Subpart D.

among other things, the extent to which the Coast Guard has met its inspection requirements and found facilities to be in compliance with its security plans, the sufficiency of trained inspectors and guidance to conduct facility inspections, and aspects of the Coast Guard's overall management of its MTSA facility oversight program, particularly documenting compliance activities.

Our work is preliminary. However, according to our analysis of Coast Guard records and statements from officials, the Coast Guard seems to have conducted facility compliance exams annually at most—but not all—facilities. Redirection of staff to a higher-priority mission, such as Hurricane Katrina emergency operations, may have accounted for some facilities not having received an annual exam. The Coast Guard also conducted a number of unannounced inspections—about 4,500 in 2006, concentrated in around 1,200 facilities—prior to the SAFE Port Act's passage. According to officials we spoke with, the Coast Guard selected facilities for unannounced inspection based on perceived risk and inspection convenience (e.g., if inspectors were already at the facility for another purpose). The Coast Guard has identified facility plan compliance deficiencies in about one-third of facilities inspected each year, and the deficiencies identified are concentrated in a small number of categories (e.g., failure to follow the approved plan for ensuring facility access control, record keeping, or meeting facility security officer requirements). We are still in the process of reviewing the data Coast Guard uses to document compliance activities and will have additional information in our forthcoming report.

Sectors we visited generally reported having adequate guidance and staff for conducting consistent compliance exams, but until recently, little guidance on conducting unannounced inspections, which are often incorporated into work while performing other mission tasks. Lacking guidance on unannounced inspections, the process for conducting one varied considerably in the sectors we visited. For example, inspectors in one sector found the use of a telescope effective in remotely observing facility control measures (such as security guard activities), but these inspectors primarily conduct unannounced inspections as part of vehicle patrols. Inspectors in another sector conduct unannounced inspections at night, going up to the security gate and querying personnel about their security knowledge (e.g., knowledge of high-security level procedures). As we completed our fieldwork, the Coast Guard issued a Commandant message with guidance on conducting unannounced inspections. This message may provide more consistency, but how the guidance will be applied and its impact on resource needs remain uncertain. Coast Guard

officials said they plan to revise their primary circular on facility oversight by February 2008. They are also planning to revise MTSA regulations to conform to SAFE Port Act requirements in 2009 (in time for the reapproval of facility security plans) but are behind schedule.

We recommended in June 2004 that the Coast Guard evaluate its compliance inspection efforts taken during the initial 6-month period after July 1, 2004, and use the results to strengthen its long-term strategy for ensuring compliance.[26] The Coast Guard agreed with this recommendation. Nevertheless, based on our ongoing work, it appears that the Coast Guard has not conducted a comprehensive evaluation of its oversight program to identify strengths or target areas for improvement after 3 years of program implementation. Our prior work across a wide range of public and private-sector organizations shows that high-performing organizations continuously assess their performance with information about results based on their activities.[27] For decision makers to assess program strategies, guidance, and resources, they need accurate and complete data reflecting program activities. We are currently reviewing the accuracy and completeness of Coast Guard compliance data and will report on this issue later this year.

TSA Has Made Progress in Implementing the TWIC Program, but Key Deadline Has Been Missed as TSA Evaluates Test Program

To control access to secure areas of port facilities and vessels, the Secretary of DHS was required by MTSA to, among other things, issue a transportation worker identification card that uses biometrics, such as fingerprints.. TSA had already initiated a program to create an identification credential that could be used by workers in all modes of transportation when MTSA was enacted. This program, called the TWIC program, is designed to collect personal and biometric information to validate workers' identities, conduct background checks on transportation workers to ensure they do not pose a threat to security, issue tamper-resistant biometric credentials that cannot be counterfeited, verify these credentials using biometric access control systems before a worker is granted unescorted access to a secure area, and revoke credentials if disqualifying information is discovered, or if a card is lost, damaged, or

[26]See GAO, *Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security*, GAO-04-838 (Washington, D.C.: Jun. 2004).

[27]See GAO, *Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making*, GAO-05-97 (Washington, D.C.: Sep. 2005).

stolen. TSA, in partnership with the Coast Guard, is focusing initial implementation on maritime facilities.

We have previously reported on the status of this program and the challenges that it faces.[28] Most recently, we reported that TSA has made progress in implementing the TWIC program and addressing problems we previously identified regarding contract planning and oversight and coordination with stakeholders.[29] For example, TSA reported that it added staff with program and contract management expertise to help oversee the contract and developed plans for conducting public outreach and education efforts.

The SAFE Port Act required TSA to implement TWIC at the 10 highest-risk ports by July 1, 2007, conduct a pilot program to test TWIC access control technologies in the maritime environment; issue regulations requiring TWIC card readers based on the findings of the pilot; and periodically report to Congress on the status of the program. However, TSA did not meet the July 1 deadline, citing the need to conduct additional testing of the systems and technologies that will be used to enroll the estimated 770,000 workers that will be required to obtain a TWIC card. According to TSA officials, the agency plans to complete this testing and begin enrolling workers at the Port of Wilmington on October 16, 2007, and begin enrolling workers at additional ports in November 2007.[30] TSA is also in the process of conducting a pilot program to test TWIC access control technologies in the maritime environment that will include a variety of maritime facilities and vessels in multiple geographic locations. According to TSA, the results of the pilot program will help the agency issue future regulations that will require the installation of access control systems necessary to read the TWIC cards.

[28]See GAO, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program*, GAO-05-106 (Washington, D.C.: December 2004); and *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program*, GAO-06-982 (Washington, D.C.: Sep. 2006).

[29]See GAO, *Transportation Security: TSA Has Made Progress in Implementing the Transportation Worker Identification Credential Program, but Challenges Remain*, GAO-07-681T (Washington, D.C.: Apr. 12, 2007).

[30] These additional ports include Corpus Christi, TX; Baton Rouge, LA; Beaumont, TX; Honolulu, HI; Oakland, CA; Tacoma, WA; Chicago/Calumet, IL; Houston, TX; Port Arthur, TX; Providence, RI; and Savannah, GA.

It is important that TSA establish clear and reasonable time frames for implementing TWIC as the agency begins enrolling workers and issuing TWIC cards in October. TSA could face additional challenges as the TWIC implementation progresses; these include monitoring the effectiveness of contract planning and oversight. TSA has developed a quality assurance surveillance plan with performance metrics that the enrollment contractor must meet to receive payment. The agency has also taken steps to strengthen government oversight of the TWIC contract by adding staff with program and contract management expertise. However, the effectiveness of these steps will not be clear until implementation of the TWIC program begins. Ensuring a successful enrollment process for the program presents another challenge. According to TSA, the agency has made communication and coordination top priorities by taking actions such as establishing a TWIC stakeholder communication committee and requiring the enrollment contractor to establish a plan for coordinating and communicating with all stakeholders who will be involved in the program. Finally, TSA will have to address access control technologies to ensure that the program is implemented effectively. It will be important that TSA's TWIC access control technology pilot ensure that these technologies work effectively in the maritime environment before facilities and vessels will be required to implement them.

DHS Working to Coordinate Multiple Background Check Programs for Transportation Workers

Since the 9/11 attacks, the federal government has taken steps to ensure that transportation workers, many of whom transport hazardous materials or have access to secure areas in locations such as port facilities, are properly screened to ensure they do not pose a security risk. Concerns have been raised, however, that transportation workers may face a variety of background checks, each with different standards. In July 2004, the 9/11 Commission reported that having too many different biometric standards, travel facilitation systems, credentialing systems, and screening requirements hampers the development of information crucial for stopping terrorists from entering the country, is expensive, and is inefficient.[31] The commission recommended that a coordinating body raise standards, facilitate information-sharing, and survey systems for potential problems. In August 2004, Homeland Security Presidential Directive - 11 announced a new U.S. policy to "implement a coordinated and

[31]The National Commission On Terrorist Attacks Upon the United States, *Final Report of the National Commission On Terrorist Attacks Upon the United States*, Washington, D.C.: Jul. 22, 2004).

comprehensive approach to terrorist-related screening—in immigration, law enforcement, intelligence, counterintelligence, and protection of the border, transportation systems, and critical infrastructure—that supports homeland security, at home and abroad."

DHS components have begun a number of their own background check initiatives. For example, in January 2007, TSA determined that the background checks required for three other DHS programs satisfied the background check requirement for the TWIC program.[32] That is, an applicant who has already undergone a background check in association with any of these three programs does not have to undergo an additional background check and pays a reduced fee to obtain a TWIC card. Similarly, the Coast Guard plans to consolidate four credentials and require that all pertinent information previously submitted by an applicant at a Coast Guard Regional Examination Center will be forwarded by the center to TSA through the TWIC enrollment process.

In April 2007, we completed a study of DHS background check programs as part of a SAFE Port Act requirement to do so.[33] We found that the six programs we reviewed were conducted independently of one another, collected similar information, and used similar background check processes. Further, each program operated separate enrollment facilities to collect background information and did not share it with the other programs. We also found that DHS did not track the number of workers who, needing multiple credentials, were subjected to multiple background check programs. Because DHS is responsible for a large number of background check programs, we recommended that DHS ensure that its coordination plan includes implementation steps, time frames, and budget requirements; discusses potential costs/benefits of program

[32]TSA determined that the background checks required for the hazardous materials endorsement (an endorsement that authorizes an individual to transport hazardous materials for commerce) and the Free and Secure Trade card (a voluntary CBP program that allows commercial drivers to receive expedited border processing) satisfy the background check requirements for TWIC. TSA also determined that an individual issued a Merchant Mariner Document (issued between February 3, 2003, and March 26, 2007) was not subject to an additional background check for TWIC.

[33]The SAFE Port Act required that GAO conduct a study of the background records checks carried out for DHS that are similar to the one required of truck drivers to obtain a hazardous material endorsement. Pub. L. No. 109-347, §105 120 Stat. 1884, 1891 (2006). See GAO, *Transportation Security: Efforts to Eliminate Redundant Background Check Investigations*, GAO-07-756 (Washington, D.C.: Apr. 26, 2007).

standardization; and explores options for coordinating and aligning background checks within DHS and other federal agencies.

DHS concurred with our recommendations and continues to take steps—both at the department level and within its various agencies—to consolidate, coordinate, and harmonize such background check programs.[34] At the department level, DHS created SCO in July 2006 to coordinate DHS background check programs. SCO is in the early stages of developing its plans for this coordination. In December 2006, SCO issued a report identifying common problems, challenges, and needed improvements in the credentialing programs and processes across the department. The office awarded a contract in April 2007 that will provide the methodology and support for developing an implementation plan to include common design and comparability standards and related milestones to coordinate DHS screening and credentialing programs. Since April 2007, DHS and SCO signed a contract to produce three deliverables to align its screening and credentialing activities, set a method and time frame for applying a common set of design and comparability standards, and eliminate redundancy through harmonization. These three deliverables are as follows:

- **Credentialing framework**: A framework completed in July 2007 that describes a credentialing life-cycle of registration and enrollment, eligibility vetting and risk assessment, issuance, expiration and revocation, and redress. This framework was to incorporate risk-based levels or criteria, and an assessment of the legal, privacy, policy, operational, and technical challenges.

- **Technical review**: An assessment scheduled for completion in October 2007 is to be completed by the contractor in conjunction with the DHS Office of the Chief Information Officer. This is to include a review of the issues present in the current technical environment and the proposed future technical environment needed to address those issues, and provide recommendations for targeted investment reuse and key target technologies.

- **Transition plan**: A plan scheduled to be completed in November 2007 is to outline the projects needed to actualize the framework, including

[34]The term "harmonize" is used to describe efforts to increase efficiency and reduce redundancies by aligning the background check requirements to make the programs more consistent.

identification of major activities, milestones, and associated timeline and costs.

Stakeholders in this effort include multiple components of DHS and the Departments of State and Justice.

In addition, the DHS Office of the Chief Information Officer (CIO) and the director of SCO issued a memo in May 2007 to promote standardization across screening and credentialing programs. In this memo, DHS indicated that (1) programs requiring the collection and use of fingerprints to vet individuals will use the Automated Biometric Identification System (IDENT); (2) these programs are to reuse existing or currently planned and funded infrastructure for the intake of identity information to the greatest extent possible; (3) its CIO is to establish a procurement plan to ensure that the department can handle a large volume of automated vetting from programs currently in the planning phase; and (4) to support the sharing of databases and potential consolidation of duplicative applications, the Enterprise Data Management Office is currently developing an inventory of biographic data assets that DHS maintains to support identity management and screening processes.

While continuing to consolidate, coordinate, and harmonize background check programs, DHS will likely face additional challenges, such as ensuring that its plans are sufficiently complete without being overly restrictive, and lack of information regarding the potential costs and benefits associated with the number of redundant background checks. SCO will be challenged to coordinate DHS's background check programs in such a way that any common set of standards developed to eliminate redundant checks meets the varied needs of all the programs without being so strict that it unduly limits the applicant pool or so intrusive that potential applicants are unwilling to take part. Without knowing the potential costs and benefits associated with the number of redundant background checks that harmonization would eliminate, DHS lacks the performance information that would allow its program managers to compare their program results with goals. Thus, DHS cannot be certain where to target program resources to improve performance. As we recommended, DHS could benefit from a plan that includes, at a minimum, a discussion of the potential costs and benefits associated with the number of redundant background checks that would be eliminated through harmonization.

Container Security Programs Continue to Expand and Mature, but New Challenges Emerge

Through the development of strategic plans, human capital strategies, and performance measures, several container security programs have been established and matured. However, these programs continue to face technical and management challenges in implementation. As part of its layered security strategy, CBP developed the Automated Targeting System as a decision support tool to assess the risks of individual cargo containers. ATS is a complex mathematical model that uses weighted rules that assign a risk score to each arriving shipment based on shipping information (e.g., manifests, bills of lading, and entry data). Although the program has faced quality assurance challenges from its inception, CBP has made significant progress in addressing these challenges. CBP's in-bond program does not collect detailed information at the U.S. port of arrival that could aid in identifying cargo posing a security risk and promote the effective use of inspection resources. In the past, CSI has lacked sufficient staff to meet program requirements. C-TPAT has faced challenges with validation quality and management in the past, in part due to its rapid growth. The Department of Energy's (DOE) Megaports Initiative faces ongoing operational and technical challenges in the installation and maintenance of radiation detection equipment at ports. In addition, implementing the Secure Freight Initiative and the 9/11 Commission Act of 2007 presents additional challenges for the scanning of cargo containers inbound to the United States.

Management of the Automated Targeting System Has Improved

CBP is responsible for preventing terrorists and WMD from entering the United States. As part of this responsibility, CBP addresses the potential threat posed by the movement of oceangoing cargo containers. To perform this mission, CBP officers at seaports utilize officer knowledge and CBP automated systems to assist in determining which containers entering the country will undergo inspections, and then perform the necessary level of inspection of each container based upon risk. To assist in determining which containers are to be subjected to inspection, CBP uses a layered security strategy that attempts to focus resources on potentially risky cargo shipped in containers while allowing other ocean going containers to proceed without disrupting commerce. ATS is one key element of this strategy. CBP uses ATS as a decision support tool to review documentation, including electronic manifest information submitted by the ocean carriers on all arriving shipments, and entry data submitted by brokers to develop risk scores that help identify containers for additional inspection.[35] CBP requires the carriers to submit manifest information 24

[35]Cargo manifests are prepared by the ocean carrier to describe the contents of a container.

hours prior to a United States-bound sea container being loaded onto a vessel in a foreign port. CBP officers use these scores to help them make decisions on the extent of documentary review or additional inspection as required.

We have conducted several reviews of ATS and made recommendations for its improvement.[36] Consistent with these recommendations, CBP has implemented a number of important internal controls for the administration and implementation of ATS.[37] For example, CBP (1) has established performance metrics for ATS, (2) is manually comparing the results of randomly conducted inspections with the results of inspections resulting from ATS analysis of the shipment data, and (3) has developed and implemented a testing and simulation environment to conduct computer-generated tests of ATS. Since our last report on ATS, the SAFE Port Act required that the CBP Commissioner take additional actions to improve ATS. These requirements included steps such as (1) having an independent panel review the effectiveness and capabilities of ATS; (2) considering future iterations of ATS that would incorporate smart features;[38] (3) ensuring that ATS has the capability to electronically compare manifest and other available data to detect any significant anomalies and facilitate their resolution; (4) ensuring that ATS has the capability to electronically identify, compile, and compare select data elements following a maritime transportation security incident; and (5) developing a schedule to address recommendations made by GAO and the Inspectors General of the Department of the Treasury and DHS.

CBP's Management of the In-Bond Cargo System Impedes Efforts to Manage Security Risks

CBP's in-bond system—which allows goods to transit the United States without officially entering U.S. commerce—must balance the competing goals of providing port security, facilitating trade, and collecting trade revenues. However, we have earlier reported that CBP's management of the system has impeded efforts to manage security risks. Specifically, CBP

[36]For a summary of these reviews, 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).

[37]The Comptroller General's internal control standards state that internal control activities help ensure that management's directives are carried out. Further, they state that the control objectives should be effective and efficient in accomplishing the agency's control objectives. GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1, 11 (Washington, D.C.: Nov. 1999).

[38]Smart features include more complex algorithms and real-time intelligence.

does not collect detailed information on in-bond cargo at the U.S. port of arrival that could aid in identifying cargo posing a security risk and promote effective use of inspection resources.[39]

The in-bond system is designed to facilitate the flow of trade throughout the United States and is estimated to be widely used. The U.S. customs system allows cargo to move from the U.S. arrival port, without appraisal or payment of duties to another U.S. port for official entry into U.S. commerce or for exportation.[40] In-bond regulations currently permit bonded carriers from 15 to 60 days, depending on the mode of shipment, to reach their final destination and allow them to change a shipment's final destination without notifying CBP. The in-bond system allows the trade community to avoid congestion and delays at U.S. seaports whose infrastructure has not kept pace with the dramatic growth in trade volume. In-bond facilitates trade by allowing importers and shipping agents the flexibility to move cargo more efficiently. Using the number of in-bond transactions reported by CBP for the 6-month period of October 2004 to March 2005, we found over 6.5 million in-bond transactions were initiated nationwide. Some CBP port officials have estimated that in-bond shipments represent from 30 percent to 60 percent of goods received at their ports.[41]

As discussed earlier in this testimony, CBP uses manifest information it receives on all cargo arriving at U.S. ports (including in-bond cargo) as input for ATS scoring to aid in identifying security risks and setting inspection priorities. For regular cargo, the ATS score is updated with more detailed information as the cargo makes official entry at the arrival port. For in-bond cargo, the ATS scores generally are not updated until these goods move from the port of arrival to the destination port for official entry into United States commerce, or not updated at all for cargo

[39]See GAO, *International Trade: Persistent Weaknesses in the In-Bond Cargo System Impede Customs and Border Protection's Ability to Address Revenue, Trade, and Security Concerns*, GAO-07-561, (Washington, D.C.: Apr. 17, 2007).

[40]In-bond goods must be transported by a carrier covered by a CBP-approved bond that allows goods that have not yet entered U.S. commerce to move through the United States. The bond is a contract given to ensure performance of obligations imposed by law or regulation and guarantees payment to CBP if these obligations are not performed.

[41]CBP cannot assess the extent of the program because it does not collect accurate information on the value and volume of in-bond cargo, and its analysis of existing data is limited to the number of in-bond transactions.

that is intended to be exported.[42] As a result, in-bond goods might transit the United States without having the most accurate ATS risk score.

Entry information frequently changes the ATS score for in-bond goods.[43] For example, CBP provided data for four major ports comparing the ATS score assigned to in-bond cargo at the port of arrival based on the manifest to the ATS score given after goods made official entry at the destination port.[44] These data show that for the four ports, the ATS score based on the manifest information stayed the same an average of 30 percent of the time after being updated with entry information, ATS scores increased an average of 23 percent of the time and decreased an average of 47 percent of the time. A higher ATS score can result in higher priority being given to cargo for inspection than otherwise would be given based solely on the manifest information. A lower ATS score can result in cargo being given a lower priority for inspection and potentially shift inspection resources to cargo deemed a higher security risk. Without having the most accurate ATS score, in-bond goods transiting the United States pose a potential security threat because higher-risk cargo may not be identified for inspection at the port of arrival. In addition, scarce inspection resources may be misdirected to in-bond goods that a security score based on better information might have shown did not warrant inspection.

We earlier recommended that the Commissioner of CBP take action in three areas to improve the management of the in-bond program, which included collecting and using improved information on in-bond shipments to update the ATS score for in-bond movements at the arrival port and enable better informed decisions affecting security, trade and revenue collection.[45] DHS agreed with most of our recommendations. According to CBP, they are in the process of developing an in-bond weight set to be utilized to further identify cargo posing a security risk. The weight set is being developed based on expert knowledge, analysis of previous in-bond seizures, and creation of rules based on in-bond concepts.

[42]Although an in-bond form is required for in-bond movement, it does not have the same level of detail contained in entry documents, and data from the form are not used to update ATS scores.

[43]Entry information is documentation to declare items arriving in the United States. Entry information allows CBP to determine what is included in a shipment, and provides more detail on a container's contents than manifest information.

[44]These four ports were Los Angeles, Long Beach, Newark, and New York.

[45]GAO-07-561.

The SAFE Port Act of 2006 contains provisions related to securing the international cargo supply chain, including provisions related to the movement of in-bond cargo. Specifically, it requires that CBP submit a report to several congressional committees on the in-bond system that includes an assessment of whether ports of arrival should require additional information for in-bond cargo, a plan for tracking in-bond cargo in CBP's Automated Commercial Environment information system, and assessment of the personnel required to ensure reconciliation of in-bond cargo between arrival port and destination port. The report must also contain an assessment of the feasibility of reducing transit time while traveling in-bond, and an evaluation of the criteria for targeting and examining in-bond cargo. Although the report was due June 30, 2007, CBP has not yet finalized the report and released it to Congress.

The CSI Program Continues to Mature, but Addressing SAFE Port Act Requirements Adds New Challenges

CPB initiated its CSI program to detect and deter terrorists from smuggling WMD via cargo containers before they reach domestic seaports in January 2002. The SAFE Port Act formalized the CSI program into law. Under CSI, foreign governments sign a bilateral agreement with CBP to allow teams of U.S. customs officials to be stationed at foreign seaports to identify cargo container shipments at risk of containing WMD. CBP personnel use automated risk assessment information and intelligence to target to identify those at risk containing WMD. When a shipment is determined to be high risk, CBP officials refer it to host government officials who determine whether to examine the shipment before it leaves their seaport for the United States. In most cases, host government officials honor the U.S. request by examining the referred shipments with nonintrusive inspection equipment and, if they deem necessary, by opening the cargo containers to physically search the contents inside.[16] CBP planned to have a total of 58 seaports by the end of fiscal year 2007.

[16]A core element of CSI is the use of technology to scan—to capture data including images of cargo container contents—high-risk containers to ensure that examinations can be done rapidly without slowing down the movement of trade. This technology can include equipment such as large scale X-ray and gamma ray machines and radiation detection devices.

Our 2003 and 2005 reports on the CSI program found both successes and challenges faced by CBP in implementing the program.[47] Since our last CSI report in 2005, CBP has addressed some of the challenges we identified and has taken steps to improve the CSI program. Specifically, CBP contributed to the Strategy to Enhance International Supply Chain Security that DHS issued in July 2007, which addressed a SAFE Port Act requirement and filled an important gap—between broad national strategies and program-specific strategies, such as for CSI—in the strategic framework for maritime security that has evolved since 9/11. In addition, in 2006 CBP issued a revised CSI strategic plan for 2006 to 2011, which added three critical elements that we had identified in our April 2005 report as missing from the plan's previous iteration. In the revised plan, CBP described how performance goals and measures are related to CSI objectives, how CBP evaluates CSI program operations, and what external factors beyond CBP's control could affect program operations and outcomes. Also, by expanding CSI operations to 58 seaports by the end of September 2007, CBP would have met its objective of expanding CSI locations and program activities. CBP projected that at the end of fiscal year 2007 between 85 and 87 percent of all U.S. bound shipments in containers will pass through CSI ports where the risk level of the container cargo is assessed and the contents are examined as deemed necessary.

Although CBP's goal is to review information about all U.S.-bound containers at CSI seaports for high-risk contents before the containers depart for the United States, we reported in 2005 that the agency has not been able to place enough staff at some CSI ports to do so.[48] Also, the SAFE Port Act required DHS to develop a human capital management plan to determine adequate staffing levels in U.S. and CSI ports. CBP has developed a human capital plan, increased the number of staff at CSI ports, and provided additional support to the deployed CSI staff by using staff in the United States to screen containers for various risk factors and potential inspection. With these additional resources, CBP reports that manifest data for all US-bound container cargo are reviewed using ATS to

[47]See GAO, *Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts*, GAO-05-557 (Washington, D.C.: Apr. 26, 2005) and *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*, GAO-03-770 (Washington, D.C.: Jul. 2003).

[48]See GAO-05-557.

determine whether the container is at high risk of containing WMD. However, the agency faces challenges in ensuring that optimal numbers of staff are assigned to CSI ports due in part to its reliance on placing staff overseas at CSI ports without systematically determining which functions could be performed overseas and which could be performed domestically.

Also, in 2006 CBP improved its methods for conducting onsite evaluations of CSI ports, in part by requiring CSI teams at the seaports to demonstrate their proficiency at conducting program activities and by employing electronic tools designed to assist in the efficient and systematic collection and analysis of data to help in evaluating the CSI team's proficiency. In addition, CBP continued to refine the performance measures it uses to track the effectiveness of the CSI program by streamlining the number of measures it uses to six, modifying how one measure is calculated to address an issue we identified in our April 2005 report; and developing performance targets for the measures. We are continuing to review these assessment practices as part of our ongoing review of the CSI program, and expect to report on the results of this effort shortly.

Similar to our recommendation in a previous CSI report, the SAFE Port Act called upon DHS to establish minimum technical criteria for the use of nonintrusive inspection equipment in conjunction with CSI. The act also directs DHS to require that seaports receiving CSI designation operate such equipment in accordance with these criteria and with standard operating procedures developed by DHS. CBP officials stated that their agency faces challenges in implementing this requirement due to sovereignty issues and the fact that the agency is not a standard setting organization, either for equipment or for inspections processes or practices. However, CBP has developed minimum technical standards for equipment used at domestic ports and the World Customs Organization (WCO)[49] had described issues—not standards—to consider when procuring inspection equipment. Our work suggests that CBP may face continued challenges establishing equipment standards and monitoring host government operations, which we are also examining in our ongoing review of the CSI program.

[49]The WCO is an international organization aimed at enhancing the effectiveness and efficiency of customs administrations.

C-TPAT Continues to Expand and Mature, but Management Challenges Remain

CBP initiated C-TPAT in November 2001 to complement other maritime security programs as part of the agency's layered security strategy. In October 2006, the SAFE Port Act formalized C-TPAT into law. C-TPAT is a voluntary program that enables CBP officials to work in partnership with private companies to review the security of their international supply chains and improve the security of their shipments to the United States. In return for committing to improve the security of their shipments by joining the program, C-TPAT members receive benefits that result in the likelihood of reduced scrutiny of their shipments, such as a reduced number of inspections or shorter wait times for their shipments. CBP uses information about C-TPAT membership to adjust risk-based targeting of these members shipments in ATS. As of July 2007, CBP had certified more than 7,000 companies that import goods via cargo containers through U.S. seaports—which accounted for approximately 45 percent of all U.S. imports—and validated the security practices of 78 percent of these certified participants.

We reported on the progress of the C-TPAT program in 2003 and 2005 and recommended that CBP develop a strategic plan and performance measures to track the program's status in meeting its strategic goals.[50] DHS concurred with these recommendations. The SAFE Port Act also mandated that CBP develop and implement a 5-year strategic plan with outcome-based goals and performance measures for C-TPAT. CBP officials stated that they are in the process of updating their strategic plan for C-TPAT, which was issued in November 2004, for 2007 to 2012. This updated plan is being reviewed within CBP, but a time frame for issuing the plan has not been established. We recommended in our March 2005 report that CBP establish performance measures to track its progress in meeting the goals and objectives established as part of the strategic planning process.[51] Although CBP has since put additional performance measures in place, CBP's efforts have focused on measures regarding program participation and facilitating trade and travel. CBP has not yet developed performance measures for C-TPAT's efforts aimed at ensuring improved supply chain security, which is the program's purpose.

[50]See GAO, *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security*, GAO-05-404 (Washington, D.C.: Mar. 2005); and GAO-03-770.

[51]See GAO-05-405.

In our previous work, we acknowledged that the C-TPAT program holds promise as part of a layered maritime security strategy. However, we also raised a number of concerns about the overall management of the program. Since our past reports, the C-TPAT program has continued to mature. The SAFE Port Act mandated that actions—similar to ones we had recommended in our March 2005 report—be taken to strengthen the management of the program. For example, the act included a new goal that CBP make a certification determination within 90 days of CBP's receipt of a C-TPAT application, validate C-TPAT members' security measures and supply chain security practices within 1 year of their certification, and revalidate those members no less than once in every 4 years. As we recommended in our March 2005 report, CBP has developed a human capital plan and implemented a records management system for documenting key program decisions. CBP has addressed C-TPAT staffing challenges by increasing the number of supply chain security specialists from 41 in 2005 to 156 in 2007.

In February 2007, CBP updated its resource needs to reflect SAFE Port Act requirements, including that certification, validation, and revalidation processes be conducted within specified time frames. CBP believes that C-TPAT's current staff of 156 supply chain security specialists will allow it to meet the act's initial validation and revalidation goals for 2007 and 2008. If an additional 50 specialists authorized by the act are made available by late 2008, CBP expects to be able to stay within compliance of the act's time frame requirements through 2009. In addition, CBP developed and implemented a centralized electronic records management system to facilitate information storage and sharing and communication with C-TPAT partners. This system—known as the C-TPAT Portal—enables CBP to track and ascertain the status of C-TPAT applicants and partners to ensure that they are certified, validated, and revalidated within required time frames. As part of our ongoing work, we are reviewing the data captured in Portal, including data needed by CBP management to assess the efficiency of C-TPAT operations and to determine compliance with its program requirements. These actions—dedicating resources to carry out certification and validation reviews and putting a system in place to track the timeliness of these reviews—should help CBP meet several of the mandates of the SAFE Port Act. We expect to issue a final report early next year.

Our 2005 report raised concerns about CBP granting benefits prematurely—before CBP had validated company practices. Instead of granting new members full benefits without actual verification of their supply chain security, CBP implemented three tiers to grant companies

graduated benefits based on CBP's certification and validation of their security practices. Related to this, the SAFE Port Act codified CBP's policy of granting graduated benefits to C-TPAT members. Tier 1 benefits—a limited reduction in the score assigned in ATS—are granted to companies upon certification that their written description of their security profile meets minimum security criteria. Companies whose security practices CBP validates in an on-site assessment receive Tier 2 benefits that may include reduced scores in ATS, reduced cargo examinations, and priority searches of cargo. If CBP's validation shows sustained commitment by a company to security practices beyond what is expected, the company receives Tier 3 benefits. Tier 3 benefits may include expedited cargo release at U.S. ports at all threat levels, further reduction in cargo examinations, priority examinations, and participation in joint incident management exercises.

Our 2005 report also raised concerns about whether the validation process was rigorous enough. Similarly, the SAFE Port Act mandates that the validation process be strengthened, including setting a year time frame for completing validations. CBP initially set a goal of validating all companies within their first 3 years as C-TPAT members, but the program's rapid growth in membership made the goal unachievable. CBP then moved to a risk-based approach to selecting members for validation, considering factors such as a company's having foreign supply chain operations in a known terrorist area or involving multiple foreign suppliers. CBP further modified its approach to selecting companies for validation to achieve greater efficiency by conducting "blitz" operations to validate foreign elements of multiple members' supply chains in a single trip. Blitz operations focus on factors such as C-TPAT members within a certain industry, supply chains within a certain geographic area, or foreign suppliers to multiple C-TPAT members. Risks remain a consideration, according to CBP, but the blitz strategy drives the decision of when a member company will be validated. In addition to taking these actions to efficiently conduct validations, CBP has periodically updated the minimum security requirements that companies must meet to be validated and is conducting a pilot program of using third-party contractors to conduct validation assessments. As part of our ongoing work, we are reviewing these actions, which are required as part of the SAFE Port Act, and other CBP efforts to enhance its C-TPAT validation process.

CBP Has Played a Key Role in Promoting Global Customs Security Standards and Initiatives, but Progress with These Efforts Presents New Challenges for CSI and C-TPAT

The CSI and C-TPAT programs have provided a model for global customs security standards, but as other countries adopt the core principles of CSI and programs similar to C-TPAT, CBP may face new challenges. Foreign officials within the WCO and elsewhere have observed the CSI and C-TPAT programs as potential models for enhancing supply chain security. Also, CBP has taken a lead role in working with members of the domestic and international customs and trade community on approaches to standardizing supply chain security worldwide. As CBP has recognized, and we have previously reported, in security matters the United States is not self-contained, in either its problems or its solutions. The growing interdependence of nations requires policymakers to recognize the need to work in partnerships across international boundaries to achieve vital national goals.

For this reason, CBP has committed through its strategic planning process to develop and promote an international framework of standards governing customs-to-customs relationships and customs-to-business relationships in a manner similar to CSI and C-TPAT, respectively. To achieve this, CBP has worked with foreign customs administrations through the WCO to establish a framework creating international standards that provide increased security of the global supply chain while facilitating international trade. The member countries of the WCO, including the United States, adopted such a framework, known as the WCO Framework of Standards to Secure and Facilitate Global Trade and commonly referred to as the SAFE Framework, in June 2005. The SAFE Framework internationalizes the core principles of CSI in creating global standards for customs security practices and promotes international customs-to-business partnership programs, such as C-TPAT. As of September 11, 2007, 148 WCO member countries had signed letters of intent to implement the SAFE Framework. CBP, along with the customs administrations of other countries and through the WCO, provides technical assistance and training to those countries that want to implement the SAFE Framework, but do not yet have the capacity to do so.

The SAFE Framework enhances the CSI program by promoting the implementation of CSI-like customs security practices, including the use of electronic advance information requirements and risk-based targeting, in both CSI and non-CSI ports worldwide. The framework also lays the foundation for mutual recognition, an arrangement whereby one country can attain a certain level of assurance about the customs security standards and practices and business partnership programs of another country. In June 2007, CBP entered into the first mutual recognition

arrangement of a business-to-customs partnership program with the New Zealand Customs Service. This arrangement stipulates that members of one country's business-to-customs program be recognized and receive similar benefits from the customs service of the other country. CBP is pursuing similar arrangements with Jordan and Japan, and is conducting a pilot program with the European Commission to test approaches to achieving mutual recognition and address differences in their respective programs. However, the specific details of how the participating counties' customs officials will implement the mutual recognition arrangement—such as what benefits, if any, should be allotted to members of other countries' C-TPAT like programs—have yet to be determined. As CBP goes forward, it may face challenges in defining the future of its CSI and C-TPAT programs and, more specifically, in managing the implementation of mutual recognition arrangements, including articulating and agreeing to the criteria for accepting another country's program; the specific arrangements for implementation, including the sharing of information; and the actions for verification, enforcement; and, if necessary, termination of the arrangement.

DNDO Faces Challenges Testing Radiation Detection Equipment

DHS also has container security programs to develop and test equipment to scan containers for radiation. Its DNDO was originally created in April 2005 by presidential directive; but the office was formally established in October 2006 by Section 501 of the SAFE Port Act. DNDO has lead responsibility for conducting the research, development, testing, and evaluation of radiation detection equipment that can be used to prevent nuclear or radiological materials from entering the United States. DNDO is charged with devising the layered system of radiation detection equipment and operating procedures—known as the "global architecture"—designed to prevent nuclear smuggling at foreign ports, the nation's borders, and inside the United States.

Much of DNDO's work on radiation detection equipment to date has focused on the development and use of radiation detection portal monitors, which are larger-scale equipment that can screen vehicles, people, and cargo entering the United States. Current portal monitors detect the presence of radiation but cannot distinguish between benign, naturally occurring radiological materials such as ceramic tile, and dangerous materials such as highly enriched uranium. Since 2005, DNDO has been testing, developing, and planning to deploy the next generation of portal monitors, known as "Advanced Spectroscopic Portals" (ASPs), which can not only detect but also identify radiological and nuclear materials within a shipping container. In July 2006, DNDO announced that

it had awarded contracts to three vendors to develop and purchase $1.2 billion worth of ASPs over 5 years for deployment at U.S. points of entry.

We have reported a number of times to Congress concerning DNDO's execution of the ASP program.[52] To ensure that DHS' substantial investment in radiation detection technology yields the greatest possible level of detection capability at the lowest possible cost, in March 2006 we recommended that once the costs and capabilities of ASPs were well understood, and before any of the new equipment was purchased for deployment, the Secretary of DHS work with the Director of DNDO to analyze the costs and benefits of deploying ASPs.[53] Further, we recommended that this analysis focus on determining whether any additional detection capability provided by the ASPs was worth the considerable additional costs. In response to our recommendation, DNDO issued its cost-benefit analysis in May 2006 and an updated, revised version in June 2006.[54] According to senior agency officials, DNDO believes that the basic conclusions of its cost-benefit analysis showed that the new ASP monitors are a sound investment for the U.S. government.

However, in October 2006, we concluded that DNDO's cost benefit analysis did not provide a sound basis for DNDO's decision to purchase and deploy ASP technology because it relied on assumptions of the anticipated performance level of ASPs instead of actual test data and that it did not justify DHS' planned $1.2 billion expenditure.[55] We also reported that DNDO did not assess the likelihood that ASPs would either misidentify or fail to detect nuclear or radiological material. Rather, it

[52] See GAO, *Combating Nuclear Smuggling: Additional Actions Needed to Ensure Adequate Testing of Next Generation Radiation Detection Equipment*, GAO-07-1247T (Washington, D.C.: Sep 18, 2007);*Combating Nuclear Smuggling: DNDO Has Not Yet Collected Most of the National Laboratories' Test Results on Radiation Portal Monitors in Support of DNDO's Testing and Development Program*, GAO-07-347R (Washington, D.C.: Mar. 9, 2007); *Combating Nuclear Smuggling: DHS's Cost-Benefit Analysis to Support the Purchase of New Radiation Detection Portal Monitors Was Not Based on Available Performance Data and Did Not Fully Evaluate All the Monitors' Cost and Benefits*, GAO-07-133R (Washington, D.C.: Oct. 17, 2006); *Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports of Entry, but Concerns Remain*, GAO-06-389 (Washington, D.C.: Mar. 22, 2006).

[53] See GAO-06-389.

[54] DNDO, *Cost Benefit Analysis for Next Generation Passive Radiation Detection of Cargo at the Nation's Border Crossings*, May 30, 2006.

[55] See GAO-07-133R.

focused its analysis on reducing the time necessary to screen traffic at border check points and reduce the impact of any delays on commerce. We recommended that DNDO conduct further testing of ASPs and the currently deployed portal monitors before spending additional funds to purchase ASPs. DNDO conducted this testing of ASPs at the Nevada Test site during February and March 2007.

In September 2007, we testified on these tests, stating that, in our view, DNDO used biased test methods that enhanced the performance of the ASPs.[56] In particular, DNDO conducted preliminary runs of almost all the materials and combination of materials that it used in the formal tests and then allowed ASP contractors to collect test data and adjust their systems to identify these materials. In addition, DNDO did not attempt in its tests to identify the limitations of ASPs—a critical oversight in its test plan. Specifically, the materials that DNDO included in its test plan did not emit enough radiation to hide or mask the presence of nuclear materials located within a shipping container. Finally, in its tests of the existing radiation detection system, DNDO did not include a critical standard operating procedure that officers with CBP use to improve the system's effectiveness.

It is important to note that, during the course of our work, CBP, DOE, and national laboratory officials we spoke to voiced concern about their lack of involvement in the planning and execution of the Nevada Test Site tests. For example, DOE officials told us that they informed DNDO in November 2006 of their concerns that the materials DNDO planned to use in its tests were too weak to effectively mask the presence of nuclear materials in a container. DNDO officials rejected DOE officials' suggestion to use stronger materials in the tests because, according to DNDO, there would be insufficient time to obtain these materials and still obtain the DHS Secretary's approval for full-scale production of ASPs by DNDO's self-imposed deadline of June 26, 2007. Although DNDO has agreed to perform computer simulations to address this issue, the DNDO Director would not commit at the September testimony to delaying full-scale ASP production until all the test results were in.

[56] See GAO-07-1247T.

DOE Continues to Expand Its Megaports Program

The Megaports Initiative, initiated by DOE's National Nuclear Security Administration in 2003, represents another component in the efforts to prevent terrorists from smuggling WMD in cargo containers from overseas locations. The goal of this initiative is to enable foreign government personnel at key foreign seaports to use radiation detection equipment to screen 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 or its allies. DOE installs radiation detection equipment, such as radiation portal monitors and handheld radioactive isotope identification devices, at foreign seaports that is then operated by foreign government officials and port personnel working at these ports.

Through August 2007, DOE had completed installation of radiation detection equipment at eight ports: Rotterdam, the Netherlands; Piraeus, Greece; Colombo, Sri Lanka; Algeciras, Spain; Singapore; Freeport, Bahamas; Manila, Philippines; and Antwerp, Belgium (Phase I). Operational testing is under way at four additional ports: Antwerp, Belgium (Phase II); Puerto Cortes, Honduras; Qasim, Pakistan; and Laem Chabang, Thailand. Additionally, DOE has signed agreements to begin work and is in various stages of implementation at ports in 12 other countries, including the United Kingdom, United Arab Emirates/Dubai, Oman, Israel, South Korea, China, Egypt, Jamaica, the Dominican Republic, Colombia, Panama, and Mexico, as well as Taiwan and Hong Kong. Several of these ports are also part of the Secure Freight Initiative, discussed in the next section. Further, in an effort to expand cooperation, DOE is engaged in negotiations with approximately 20 additional countries in Europe, Asia, the Middle East, and Latin America.

DOE had made limited progress in gaining agreements to install radiation detection equipment at the highest priority seaports when we reported on this program in March 2005.[57] Then, the agency had completed work at only two ports and signed agreements to initiate work at five others. We also noted that DOE's cost projections for the program were uncertain, in part because they were based on DOE's $15 million estimate for the average cost per port. This per port cost estimate may not be accurate because it was based primarily on DOE's radiation detection assistance

[57]For additional information, see GAO, *Preventing Nuclear Smuggling: DOE Has Made Limited Progress in Installing Radiation Detection Equipment at Highest Priority Foreign Seaports*, GAO-05-375 (Washington, D.C.: Mar. 31, 2005).

work at Russian land borders, airports, and seaports and did not account for the fact that the costs of installing equipment at individual ports vary and are influenced by factors such as a port's size, physical layout, and existing infrastructure. Since our review, DOE has developed a strategic plan for the Megaports Initiative and revised it's per port estimates to reflect port size, with per port estimates ranging from $2.6 million to $30.4 million.

As we earlier reported, DOE faces several operational and technical challenges specific to installing and maintaining radiation detection equipment at foreign ports as the agency continues to implement its Megaports Initiative. These challenges include ensuring the ability to detect radioactive material, overcoming the physical layout of ports and cargo-stacking configurations, and sustaining equipment in port environments with high winds and sea spray.

Secure Freight Initiative Testing Feasibility of Combining Scanning Technologies

The SAFE Port Act required that a pilot program—known as the Secure Freight Initiative (SFI)—be conducted to determine the feasibility of 100 percent scanning of U.S. bound containers. To fulfill this requirement, CBP and DOE jointly announced the formation of SFI in December 2006, as an effort to build upon existing port security measures by enhancing the U.S. government's ability to scan containers for nuclear and radiological materials overseas and better assess the risk of inbound containers. In essence, SFI builds upon the CSI and Megaports programs. The SAFE Port Act specified that new integrated scanning systems that couple nonintrusive imaging equipment and radiation detection equipment must be pilot-tested. It also required that, once fully implemented, the pilot integrated scanning system scan 100 percent of containers destined for the United States that are loaded at pilot program ports.

According to agency officials, the initial phase of the initiative will involve the deployment of a combination of existing container scanning technology—such as X-ray and gamma ray scanners used by host nations at CSI ports to locate high-density objects that could be used to shield nuclear materials, inside containers—and radiation detection equipment. The ports chosen to receive this integrated technology are: Port Qasim in Pakistan, Puerto Cortes in Honduras, and Southampton in the United Kingdom. Four other ports located in Hong Kong, Singapore, the Republic of Korea, and Oman will receive more limited deployment of these technologies as part of the pilot program. According to CBP, containers from these ports will be scanned for radiation and other risk factors before they are allowed to depart for the United States. If the scanning

systems indicate that there is a concern, both CSI personnel and host country officials will simultaneously receive an alert and the specific container will be inspected before that container continues to the United States. CBP officials will determine which containers are inspected, either on the scene locally or at CBP's National Targeting Center.

Per the SAFE Port Act, CBP is to report by April 2008 on, among other things, the lessons learned from the SFI pilot ports and the need for and the feasibility of expanding the system to other CSI ports. Every 6 months thereafter, CBP is to report on the status of full-scale deployment of the integrated scanning systems to scan all containers bound for the United States before their arrival.

New Requirement for 100 Percent Scanning Introduces New Challenges

Recent legislative actions have updated U.S. maritime security requirements and may affect overall international maritime security strategy. In particular, the recently enacted Implementing Recommendations of the 9/11 Commission Act (9/11 Act) requires, by 2012, 100 percent scanning of U.S.-bound cargo containers using nonintrusive imaging equipment and radiation detection equipment at foreign seaports. The act also specifies conditions for potential extensions beyond 2012 if a seaport cannot meet that deadline. Additionally, it requires the Secretary of DHS to develop technological and operational standards for scanning systems used to conduct 100 percent scanning at foreign seaports. The Secretary also is required to ensure that actions taken under the act do not violate international trade obligations and are consistent with the WCO SAFE Framework. The 9/11 Act provision replaces the requirement of the SAFE Port Act that called for 100 percent scanning of cargo containers before their arrival in the United States, but required implementation as soon as possible rather than specifying a deadline. While we have not yet reviewed the implementation of the 100 percent scanning requirement, we have a number of preliminary observations based on field visits of foreign ports regarding potential challenges CBP may face in implementing this requirement:

- **CBP may face challenges balancing new requirement with current international risk management approach.** CBP may have difficulty requiring 100 percent scanning while also maintaining a risk-based security approach that has been developed with many of its international partners. Currently, under the CSI program, CBP uses automated targeting tools to identify containers that pose a risk for terrorism for further inspection before being placed on vessels bound for the United States. As we have previously reported, using risk

management allows for reduction of risk against possible terrorist attack to the nation given resources allocated and is an approach that has been accepted governmentwide. Furthermore, many U.S. and international customs officials we have spoken to, including officials from the World Customs Organization, have stated that the 100 percent scanning requirement is contrary to the SAFE Framework developed and implemented by the international customs community, including CBP. The SAFE Framework, based on CSI and C-TPAT, calls for a risk management approach, whereas the 9/11 Act calls for the scanning of all containers regardless of risk.

- **United States may not be able to reciprocate if other countries request it.** The CSI program, whereby CBP officers are placed at foreign seaports to target cargo bound for the United States, is based on a series of bilateral, reciprocal agreements with foreign governments. These reciprocal agreements also allow foreign governments the opportunity to place customs officials at U.S. seaports and request inspection of cargo containers departing from the United States and bound for their home country. Currently, customs officials from certain countries are stationed at domestic seaports and agency officials have told us that CBP has inspected 100 percent of containers that these officials have requested for inspection. According to CBP officials, the SFI pilot, as an extension of the CSI program, allows foreign officials to ask the United States to reciprocate and scan 100 percent of cargo containers bound for those countries. Although the act establishing the 100 percent scanning requirement does not mention reciprocity, CBP officials have told us that the agency does not have the capacity to reciprocate should it be requested to do so, as other government officials have indicated they might when this provision of the 9/11 Act is in place.

- **Logistical feasibility is unknown and may vary by port.** Many ports may lack the space necessary to install additional equipment needed to comply with the requirement to scan 100 percent of U.S. bound containers. Additionally, we observed that scanning equipment at some seaports is located several miles away from where cargo containers are stored, which may make it time consuming and costly to transport these containers for scanning. Similarly, some seaports are configured in such a way that there are no natural bottlenecks that would allow for equipment to be placed such that all outgoing containers can be scanned and the potential to allow containers to slip by without scanning may be possible. Transshipment cargo containers—containers moved from one vessel to another—are only available for scanning for a short period of time and may be difficult to

access. Similarly, it may be difficult to scan cargo containers that remain on board a vessel as it passes through a foreign seaport. CBP officials told us that currently containers such as these that are designated as high-risk at CSI ports are not scanned unless specific threat information is available regarding the cargo in that particular container.

- **Technological maturity is unknown.** Integrated scanning technologies to test the feasibility of scanning 100 percent of U.S. bound cargo containers are not yet operational at all seaports participating in the pilot program, known as SFI. The SAFE Port Act requires CBP to produce a report regarding the program, which will include an evaluation of the effectiveness of scanning equipment at the SFI ports. However, this report will not be due until April 2008. Moreover, agency officials have stated that the amount of bandwidth necessary to transmit scanning equipment outputs to CBP officers for review exceeds what is currently feasible and that the electronic infrastructure necessary to transmit these outputs may be limited at some foreign seaports. Additionally, there are currently no international standards for the technical capabilities of inspection equipment. Agency officials have stated that CBP is not a standard setting organization and has limited authority to implement standards for sovereign foreign governments.

- **Resource responsibilities have not been determined.** The 9/11 Act does not specify who would pay for additional scanning equipment, personnel, computer systems, or infrastructure necessary to establish 100 percent scanning of U.S. bound cargo containers at foreign ports. According to the Congressional Budget Office (CBO) in its analysis of estimates for implementing this requirement, this provision would neither require nor prohibit the U.S. federal government from bearing the cost of conducting scans. For the purposes of its analysis, CBO assumed that the cost of acquiring, installing, and maintaining systems necessary to comply with the 100 percent scanning requirement would be borne by foreign ports to maintain trade with the United States. However, foreign government officials we have spoken to expressed concerns regarding the cost of equipment. They also stated that the process for procuring scanning equipment may take years and can be difficult when trying to comply with changing U.S. requirements. These officials also expressed concern regarding the cost of additional personnel necessary to: (1) operate new scanning equipment; (2) view scanned images and transmit them to the United States; and (3) resolve false alarms. An official from one country with whom we met told us that, while his country does not scan 100 percent of exports,

modernizing its customs service to focus more on exports required a 50 percent increase in personnel, and other countries trying to implement the 100 percent scanning requirement would likely have to increase the size of their customs administrations by at least as much.

- **Use and ownership of data have not been determined.** The 9/11 Act does not specify who will be responsible for managing the data collected through 100 percent scanning of U.S.-bound containers at foreign seaports. However, the SAFE Port Act specifies that scanning equipment outputs from SFI will be available for review by U.S. government officials either at the foreign seaport or in the United States. It is not clear who would be responsible for collecting, maintaining, disseminating, viewing or analyzing scanning equipment outputs under the new requirement. Other questions to be resolved include ownership of data, how proprietary information would be treated, and how privacy concerns would be addressed.

CBP officials have indicated they are aware that challenges exist. They also stated that the SFI will allow the agency to determine whether these challenges can be overcome. According to senior officials from CBP and international organizations we contacted, 100 percent scanning of containers may divert resources, causing containers that are truly high risk to not receive adequate scrutiny due to the sheer volume of scanning outputs that must be analyzed. These officials also expressed concerns that 100 percent scanning of U.S.-bound containers could hinder trade, leading to long lines and burdens on staff responsible for viewing images. However, given that the SFI pilot program has only recently begun, it is too soon to determine how the 100 percent scanning requirement will be implemented and its overall impact on security.

Agency Comments

We provided a draft of the information in this testimony to DHS. DHS provided technical comments, which we incorporated as appropriate.

Mr. Chairman and members of the Committee, this completes my prepared statement. I will be happy to respond to any questions that you or other members of the committee have at this time.

GAO Contact and Staff Acknowledgments

For information about this testimony, please contact Stephen L. Caldwell, Director, Homeland Security and Justice Issues, at (202) 512-9610, or caldwells@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this testimony include Richard Ascarate, Jonathan Bachman, Jason Bair, Fredrick Berry, Christine Broderick, Stockton Butler, Steven Calvo, Frances Cook, Christopher Currie, Anthony DeFrank, Wayne Ekblad, Christine Fossett, Nkenge Gibson, Geoffrey Hamilton, Christopher Hatscher, Valerie Kasindi, Monica Kelly, Ryan Lambert, Nicholas Larson, Daniel Klabunde, Matthew Lee, Gary Malavenda, Robert Rivas, Leslie Sarapu, James Shafer, Kate Siggerud, and April Thompson.

TESTIMONY ON THE PROGRESS ON THE SAFE PORT ACT BEFORE THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS

October 16, 2007

Captain Jeffrey W. Monroe MM, MS

Good Morning. My name is Captain Jeffrey Monroe, Director of Ports and Transportation for the City of Portland, Maine. Thank you for your invitation to speak on the progress of the Safe Port Act. Today, I will be commenting on three areas of port security that can be summarized as global, national and local.

Everyday some 75,000 Twenty-Foot Equivalent Unit (TEU) containers move in and out of ports in the United States alone. This poses a significant threat to ports and communities throughout the nation. Since 9/11, with the increasing focus on maritime security, we have reduced the threats to the United States through several programs including the Customs-Trade partnership Against Terrorism (C-TPAT), the Container Security initiative (CSI), The Smart Box program, and the Advanced Trade Data Initiative. The programs are designed to supply much needed information about supply chain partners and shipments and to protect a complicated supply chain.

While these programs are of critical value, their implementation is advancing much too slowly. Although the industry recognizes the value of securing the nation's supply chain, the requirement to secure cargo with C-TPAT specified seals is meeting resistance from shippers. The concern is that the costs of implementing an electronic seal program are high and standards for these devices have yet to be completed. The industry does not want to invest in expensive experimental technology until a proven and cost effective federal standard has been set for container security devices.

Another key concept that ties in with new technology is the Greenlane concept, which is being touted as an incentive to shippers to add these new devices. However, this program is also off to a slow start as Greenlanes in seaports do not exist at this point and there is no real movement for their establishment.

While Customs tracking has improved, inspections increased, shippers recruited for pre-clearance programs and reporting of manifests have been made more efficient, new initiatives designed to improve cargo security continue to move at a very slow pace. However, it is apparent that although cargo security is one of the nation's most significant threat issues, multi-agency coordination and effective policy development remains a minor function of the Department of Homeland Security.

The current Office of Cargo Policy at DHS needs to be elevated in the DHS structure and must be more active in its outreach to industry. Further, this office must have a far reaching view of cargo security as part of a transportation system that includes maritime, aviation and surface. Recovery from attack or natural disaster requires a systematic

approach. It will make little difference if a port is able to open without the landside infrastructure ready to deliver and accept cargo. For too many years, our national transportation system has suffered from a modal approach as opposed to a systematic approach. It would be a major mistake for us to mirror this ineffective model in Homeland Security.

Cargo and the policies that impact the movement of goods related to security must have significant attention within DHS. We cannot continue to think myopically, focused on some small segment of security without looking at the entire picture. For example, this lack of a coordinated approach is currently providing us with a TWIC system that does not meet the original goals of the Transportation Worker Identification Credential. Instead of the one system as originally envisioned, it appears that there will be separate standards for maritime and aviation. The aviation system was able to credential and clear hundreds of thousands of workers in a relatively short period of time. Yet, some six years after 9-11, we are still in the process of implementing the TWIC standard for the maritime world, which is different from the system already in use. Additionally, to date, nothing has been done to address TWIC in regard to surface transportation.

As a professional merchant mariner, seaport director, airport director and member of the DHS National Maritime Security Committee, I had to go through four separate background checks, each with differing standards. This amazes me that one single and effective approach cannot be designed and implemented in a shorter period of time. That same issue will exist with cargo security, which will also cause significant delays. Although we are currently focused on containers, there is a wide range of cargo movements that seldom get addressed. Project cargo, bulk and neo-bulk cargoes, and other specialized activities all have their own element of security risk. A high level policy office could address not just one type of cargo, but all logistical movements.

Such an office could also reach out to a broad segment of the industry. I believe we have reached a point where a government/business summit should be held and reasonable target dates for specifications and implementation of cargo security programs must be established and implemented.

The formation of a high level policy office for cargo security was proposed in legislation by Senator Collins last year. It was a good idea then and it is an even more essential idea now. I would encourage this committee to address this in the near future.

We cannot afford to continue to work with obscure standards and poorly coordinated programs. We feel the lack of progress in our ports. For example, The Port of Portland includes activities in both of the cities of Portland and South Portland. In 2006, the Port was the 26th largest port in the United States in gross tonnage. We are the largest oil port on the east coast, the largest tonnage port in New England and the largest foreign inbound transit port in the United States (Source-US Army Corps of Engineers). Though geographically small in size the port continues to be a microcosm of all port activities, with growing container and break bulk businesses, international ferry and domestic ferries serving and commercial and recreational boating interests. Our transportation

system alone, in a City of 65,000 and a region of 350,000, handled some 6.5 million passengers in our system and nearly 30 million tons of cargo.

The Port is the home of a mix of public and private stakeholders committed to ensuring that the letter and the spirit of the Maritime Transportation Security Act (MTSA) are always an integral part of any port planning initiative. To that end, our success to date in becoming a model of interoperability would not have been possible without the cooperation of professionals and public officials and the funding we have received through the port security grants program.

Through seven rounds of funding of approximately $6MM, we have been able to meet the requirements of the MTSA. These funds have allowed us to purchase the fences, lighting and screening technology required to date and we are ready for the next steps in TWIC development. But we have gone further.

Portland has developed an all-hazard approach to planning. We have examined each of our security requirement solutions for attributes beyond prevention. All Homeland Security funding now flows through one center to ensure that systems are interoperable and to avoid redundancy. We coordinate our programs with our neighboring cities and meet often with public and private stakeholders. Besides our close working relationship with the United States Coast Guard, we also maintain ongoing coordination with the TSA, US Customs and Border Protection, and federal, State and local law enforcement. We have done this out of necessity, utilizing available funds to the maximum advantage.

However, we view transportation security as a partnership between maritime, aviation and surface transportation agencies and providers and share resources and information across the wide spectrum of activities. We also recognize our important place in the community and understand that we are not only protecting the traveling public but our citizens as well.

Lessons learned from a number of natural disasters have also taught us that this all-hazard approach is necessary not only for deterrence of terrorist attacks but for the recovery of commerce and continuity of government programs and services. Only the close monitoring of all-hazard programs will identify fault lines in our approach. Only communication with our neighbors will allow us the resiliency required to protect our citizens. We do not understand why this same model cannot work in Washinton.

As we continue to hear that resources should be directed to only "bigger ports", we realize that to allocate funding to ports based on simple quantitative analysis does not sufficiently consider the enormous impact a disruption in port commerce would have on the entire region. It does not consider our status as an international border crossing and it does not reflect recent history. The reasons that two of the 9/11 hijackers chose to begin their assault on the US from Portland have never been fully explained.

We recognize that Portland is of a size that makes participation among all parties somewhat easier than a more highly urbanized area. But the commitment to an all-hazard

approach and the integration of all stakeholders is possible through the leadership of the communities and a desire to put the good of the entire system ahead of individual interests.

The equipment and training that we have been able to acquire through the Seaport Security Grant Program allows us this practice for disaster and to insure we share the best intelligence available. We know that we are far better prepared than we were in 2001 or even 2005. We know that we are still learning the best ways to achieve a totally integrated security and response package. And we know that it will take more funding, more commitment of our time and continuing leadership. We are prepared to continue our work.

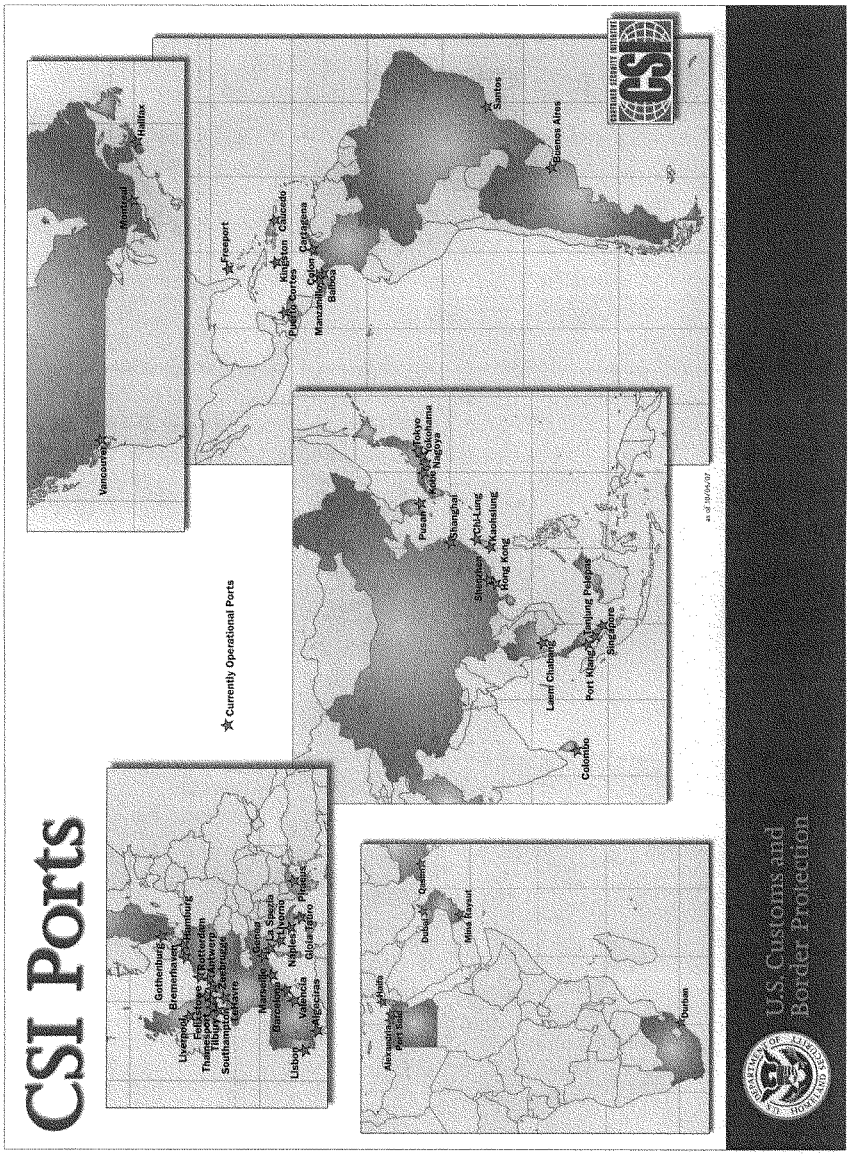
Above all however, the Department of Homeland Security must get its arms around the critical issue of port and supply security. The leadership must begin in Washington and work its way throughout DHS, to the State level and ultimately to the communities dealing with these issues. We simply must do a better job in looking at the entire picture and while the various key pieces of legislation related to port and cargo security have moved us ahead; our national bureaucracy remains an impediment to effective implementation of that legislation.

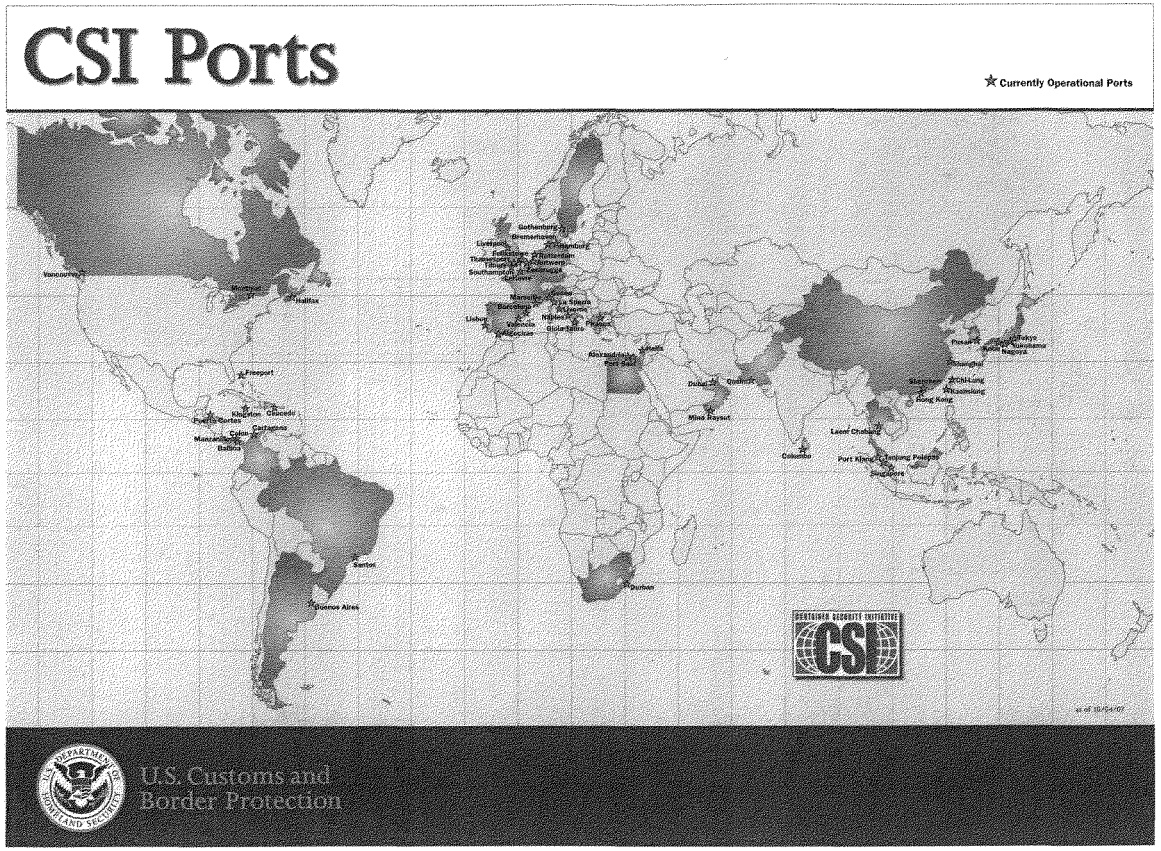
In speaking to you from the trenches, I hope that the intentions of this Committee, Congress and our Administration are to dramatically increase the effectiveness of cargo and Homeland security. To that end, I hope that we will put as strong an emphasis on cargo security as we have on other elements of Homeland Security and that we will remove the bureaucratic boundaries that inhibit making our entire system as secure as humanly possible.

Thank you.

U.S. Customs & Border Protection
WORKSPACE
CONTAINER INFO
MESSENGER
ALARMS
G N I S
TAR:
LSS:
Comments:
Submit
Port Monitor

Implementing the SAFE Port Act
8%
Outstanding Provisions
(In Progress)
44%
Completed
Requirements
48%
On Schedule
DHS is on track with over 92% of the requirements.
Homeland Security


CSI Ports
Currently Operational Ports
Gothenburg
Bremerhaven
Hamburg
Rotterdam
Zeebrugge
Antwerp
Le Havre
Fos
Genoa
La Spezia
Livorno
Naples
Gioia Tauro
Piraeus
Barcelona
Valencia
Algeciras
Lisbon
Marseille
Felixstowe
Thamesport
Tilbury
Southampton
Sheerness
Vancouver
Montreal
Halifax
Freeport
Kingston
Caucedo
Puerto Cortes
Cartagena
Colon
Manzanillo
Balboa
Santos
Buenos Aires
Tokyo
Kobe
Yokohama
Nagoya
Pusan
Shanghai
Chi-Lung
Kaohsiung
Hong Kong
Shenzhen
Laem Chabang
Tanjung Pelepas
Port Klang
Singapore
Colombo
Dubai
Qasim
Mina Faysal
Aqaba
Alexandria
Port Said
Durban
U.S. Customs and Border Protection


CSI Ports
★ Currently Operational Ports
Vancouver
Montreal
Halifax
Freeport
Kingston
Cruzeiro
Puerto Cortes
Colon
Cartagena
Manzanillo
Balboa
Santos
Buenos Aires
Gothenburg
Bremerhaven
Hamburg
Le Havre
Rotterdam
Antwerp
Felixstowe
Thamesport
Tilbury
Southampton
Zeebrugge
Genoa
La Spezia
Marseilles
Barcelona
Valencia
Algeciras
Lisbon
Naples
Gioia Tauro
Piraeus
Durban
Dubai
Colombo
Mina Rayasi
Laem Chabang
Port Klang
Tanjung Pelepas
Singapore
Yantian
Shanghai
Shekou
Ningbo
Nansha
Xiamen
Hong Kong
Pusan
Kwangyang
Kaohsiung
CONTAINER SECURITY INITIATIVE
CSI
as of 10/24/07
U.S. Customs and
Border Protection

CSI Ports

☆ Operational Ports (58)

EUROPE

Algeciras, Spain
Antwerp, Belgium
Barcelona, Spain
Bremerhaven, Germany
Felixstowe, UK
Genoa, Italy
Gioia Tauro, Italy
Gothenburg, Sweden
Hamburg, Germany
La Spezia, Italy
Le Havre, France
Lisbon, Portugal
Liverpool, UK
Livorno, Italy
Marseille, France
Naples, Italy
Piraeus, Greece
Rotterdam, Netherlands
Southampton, UK
Thamesport, UK
Tilbury, UK
Valencia, Spain
Zeebrugge, Belgium

ASIA

Chi-Lung, Taiwan
Colombo, Sri Lanka
Dubai, United Arab Emirates
Hong Kong
Kaohsiung, Taiwan
Kobe, Japan
Laem Chabang, Thailand
Nagoya, Japan
Port Klang, Malaysia
Pusan, Korea
Qasim, Pakistan
Shanghai, People's Republic of China
Shenzhen, People's Republic of China
Singapore, Singapore
Tanjung Pelepas, Malaysia
Tokyo, Japan
Yokohama, Japan

AFRICA

Alexandria, Egypt
Durban, South Africa
Port Said, Egypt

MIDDLE EAST

Haifa, Israel
Mina Raysut, Oman

NORTH AMERICA

Halifax, Canada
Montreal, Canada
Vancouver, Canada

CENTRAL AMERICA/ CARIBBEAN

Balboa, Panama
Caucedo, Dominican Republic
Colon, Panama
Freeport, Bahamas
Kingston, Jamaica
Manzanillo, Panama
Puerto Cortes, Honduras

SOUTH AMERICA

Buenos Aires, Argentina
Cartagena, Columbia
Santos, Brazil

☐ Planned Expansion Ports

CONTAINER SECURITY INITIATIVE
CSI

as of 10/04/07

U.S. Customs and Border Protection

October 1, 2007

Dear Senator Lieberman,

With the enactment of the "Implementing Recommendations of the 9/11 Commission Act of 2007", I would like to reaffirm the Japanese Government's commitment to fighting terrorism hand in hand with the United States. However, I would like to express my concern about Section 1701 of the Act, which requires 100 percent scanning of containers bound for the United States at foreign ports before they are loaded onto vessels. This provision, if it were to be implemented as such, would severely disrupt international trade and cause tremendous damage to the economies of both Japan and the United States.

I would also like to express my concern about Section 1602 of the Act, which mandates the Secretary of Homeland Security to establish a system to screen 100 percent of cargo on passenger aircraft. Rules that need to be made to implement this provision could hinder efficient air transportation from foreign countries to the United States.

While I fully understand the importance of enhancing the security of global supply chains, I would like to emphasize that it is essential to implement security measures in a way that does not undermine the smooth flow of goods. Simply scanning all containers would only provide marginal improvements in security, while it would significantly disrupt global trade. At the last summit meeting in April, Prime Minister Abe and President Bush endorsed bilateral efforts to make trade flows more secure and more efficient. Based on this endorsement by the two leaders, the Governments of Japan and the United States have established the Study Group on Secure and Efficient Trade Coordination, through which we have been maintaining close contact with each other. Additionally, our two governments have been successfully cooperating on the Container Security Initiative and have been conducting meaningful discussions on mutual recognition of Authorized Economic Operators (AEOs). I firmly believe that ongoing efforts such as these between the two governments are more effective and practical ways of achieving the twin goals of improving security while facilitating legitimate trade.

I would also like to address that the requirement of 100 percent scanning mentioned in Section 1701 of the Act would be inconsistent with the Framework of Standards adopted by the World Customs Organization (WCO). To address security threats, the Framework of Standards espouses the risk management approach, which aims to identify and target high-risk cargoes rather than conducting indiscriminate inspections.

As members of the WCO, our two governments share the basic principle of this widely-accepted risk-based approach.

I would appreciate it if you could give further consideration to these particular issues for the mutual benefit of our two countries.

I look forward to continuing constructive dialogue with your government on how we can cooperate to further secure and facilitate global trade.

Sincerely,

Ryozo Kato
Ambassador of Japan

Questions for the Hearing Record
For Reginald I. Lloyd
United States Attorney
For the District of South Carolina

From the October 16, 2007 hearing on
"One Year Later: A Progress Report on the Safe Port Act"

From Chairman Joseph I. Lieberman

Question: Is the U.S. Attorney's office planning to continue its participation in Project Seahawk following the transition of the Center from the Department of Justice to the Department of Homeland Security?

Response: The United States Attorney's Office for the District of South Carolina ("USAO") is committed to continuing participation at Project Seahawk after Seahawk is transitioned to the Department of Homeland Security. Its participation will obviously include continuing to prosecute cases of federal interest that arise in and around the Ports of South Carolina. Additionally, the USAO will continue to use its influence and leadership in the District of South Carolina to encourage, facilitate, and engage in proactive law enforcement operations at the Ports as part of the District of South Carolina's anti-terrorism initiatives. One of the primary objectives of the Anti-Terrorism Advisory Council ("ATAC" -- United States Attorney led councils set up in every district in the nation) is to focus on prevention and disruption of terrorist acts by identifying and implementing anti-terrorism initiatives in the district based upon the particular vulnerabilities of each district. Protection of the Ports of South Carolina will remain one of the District of South Carolina's highest ATAC initiatives, and that Office will continue to work with all agencies at the Port and throughout South Carolina to determine proactive operations and strategies in order to bring prosecutions, as well as prevent and disrupt threats to the Ports and the nation. The USAO for the District of South Carolina will assign an Assistant United States Attorney to assist with coordinating interagency operations and strategies at Seahawk and review matters on a routine basis for possible prosecution.

Post-Hearing Questions for the Record
Submitted to Stephen L. Caldwell
From Senator Joseph I. Lieberman

"One Year Later: A Progress Report on the SAFE Port Act"
October 16, 2007

1. The Secure Freight Initiative pilot program seems to be based on a similar model to the Container Security Initiative, with foreign customs organizations agreeing to scan cargo prior to its being shipped to the United States. A few private companies, shippers and terminal operators have discussed implementing a 100% scanning system, perhaps voluntarily if they were able to receive sufficient incentives, like a GreenLane.

   - Do you see any benefit or drawback to allowing private companies to implement a 100% scanning system?

   - Whether scans are done by foreign governments or by the private sector, what types of checks should be in place to ensure these operations are secure?

Answer:

GAO has not examined the issues associated with private companies doing the scanning to meet the requirements of the 9/11 Act. However, in our preliminary work, we identified several potential challenges, such as resource constraints and integration with existing risk based security initiatives, that would remain regardless of who conducts these scans. These challenges are listed in detail in our written statement. Nonetheless, no matter who conducts these scans, CBP should ensure that the overall examination system, which includes scanning, can reliably detect and identify WMD in container cargo bound for the United States. To do this, CBP should systematically collect information on the examining entity's examination system—including equipment, people, and processes—and compare these with established guidelines and technical criteria that will provide CBP with a basis for determining the reliability of examinations of 100% of container cargo bound for the United States. This is of particular concern since most high risk container cargo that has already been examined at a foreign seaport is generally not reexamined once it arrives at a U.S. seaport.

Post-Hearing Questions for the Record
Submitted to Captain Jeffrey W. Monroe
From Senator Susan M. Collins

"One Year Later: A Progress Report on the SAFE Port Act"
October 16, 2007

1. The critical infrastructure at the ports is almost entirely in the hands of the private sector, and therefore the private sector must play a central role in the resumption of trade after an incident. How should DHS' resumption of trade planning evolve to appropriately include private sector involvement?

Response:

DHS needs to approach the restoration of trade in the same manner as the private sector. Logistic planners are able to maintain an inventory of available facilities including their road and rail connections. Planners know distances, transit times, and available infrastructure at most facilities where their vessels call and maintain a backup list of facilities where in case of weather or other diversions, a market can still be served.

This is the approach DHS needs to take. To look at it methodically:

1. DHS needs to insure it looks beyond the water and the piers understanding that port facilities are only one portion of the logistics chain.

2. DHS should compile a database that is updated annually which contains information about ocean distances, port distances, water depths, facility availability, type of facility equipment, market areas served, land distances, road capacity, rail capacity, availability of personnel, availability of equipment, average facility costs and discharge/load points inland. This paints the full picture of the logistics chain and allows DHS to coordinate a rapid restoration of commodity and personnel movement.

3. As part of the inventory process, DHS maintains a current list of contacts and management personnel that handle each segment of the logistic chain, most of whom are in the private sector.

4. DHS can present a planning program that involves all of the private sector entities who are more than willing to open their facilities to alternate uses during national emergency. To formalize this, DHS can execute formal letters of agreement for every facility inventoried in the program.

DHS needs to look at the entire nation and the entire transportation network as part of a comprehensive system and the private sector would be more than willing to participate as they did after 9-11.

Note: During Katrina, logistics planners in the private sector, working with port authorities and industry personnel, were able to predict interruptions in the supply chair through New Orleans and diverted cargo and commodities well in advance of the storm to other ports and surface networks that were not affected.

This is the most effective way for DHS to approach the issue.

Question#:	1
Topic:	SFI
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Post-Hearing Questions for the Record Submitted to
Hon. Stewart A. Baker, Assistant Secretary for Policy,
Department of Homeland Security

Question: The 9/11 Commission implementation legislation enacted by Congress this summer includes a provision requiring 100% of all cargo containers be scanned by 2012, though it gives the Secretary some authority to extend the deadline. The lessons learned from the Secure Freight Initiative (SFI) will steer the Department toward the goal of 100% scanning.

Has DHS developed a formal evaluation plan for SFI? If so, please provide a copy to the Committee.

What metrics will DHS use to determine if such systems significantly impact trade capacity and the flow of cargo at foreign or U.S. ports, one of the key criteria required in the Act for the evaluation of the pilot program?

Answer:
Proper metrics for the SFI pilots are critical to ensure the accuracy and operational relevancy of the data yielded from each port. In preparing the report to Congress required by the SAFE Port Act, DHS is currently developing and refining the metrics to evaluate the successes and challenges of SFI. The report will be submitted in April 2008.

With particular focus on the impact on trade capacity, DHS will continue to work with its terminal/port operator counterparts to determine if SFI deployments are impacting trade and the flow of cargo at foreign ports. DHS routinely meets with SFI partners to discuss SFI deployments and their effect on the flow of cargo. Some examples of possible metrics include: the maximum throughput in SFI queues, container processing time, alarm rates, and domestic re-inspection rates. As discussions with stakeholders continue, these metrics will be expanded, readjusted, and supplemented.

Question#:	2
Topic:	SFI pilot program
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The three main ports in the pilot program, Southampton Container Terminal in the U.K., Port Qasim in Pakistan, and Port Cortez in Honduras, are moderately sized ports and process little trans-shipped cargo. DHS has also reached agreements to test the Secure Freight Initiative in a more limited capacity at four additional ports, including the large ports of Singapore and Hong Kong.

Answer:
What may work at one moderately sized port may not work, or may require considerable adaptation, at a larger port like Singapore or Hong Kong. DHS has categorized the participation of Singapore and Hong Kong in SFI as limited, but how will the pilot program work in those large ports, to evaluate the balance needed between security and commerce? How will foreign ports and DHS work to test the both the scanning equipment and the flow of commerce to their limits at such high volume ports?

The pilot is limited in Singapore and Hong Kong in that we are deploying to only one terminal for the aforementioned ports. This limited capacity deployment goes above and beyond what is required under the SAFE Ports act.

It is essential that these systems be tested at high-volume ports by scanning a volume of containers that reveals an accurate representation of the challenges in a high-volume port. Hong Kong and Singapore represent nearly 20 percent of the total shipments to the United States, 14.32 percent and 3.89 percent respectively.

Additionally, there are other measures that are important in these "limited" capacity test ports. The pilots in Hong Kong, Singapore, Salalah and Busan will also test the challenges of scanning 100 percent of containers destined for the U.S. in a high transshipment rate port and using the scanning systems in high-volume ports with a relatively small footprint.

As DHS moves forward with SFI, we will continue to work with our host-government and terminal operator counterparts to evaluate deployed technology and evaluate the requirements that are needed at high-volume ports in order to determine that both the flow of commerce and security needs are met.

Question#:	3
Topic:	TWIC enrollment
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The Transportation Worker Identification Credential, or TWIC, program is long overdue and been plagued by problems. As a result Congress was forced to revise the program, and the SAFE Port Act required DHS implement TWIC at 50 "top priority" ports before the end of 2007. On October 3rd, DHS announced it will finally begin enrollment for TWIC, beginning with the Port of Wilmington, DE. Though DHS is finally prepared to begin vetting and enrolling port and transportation workers, it does appear to once again have fallen behind schedule.

Not only will DHS apparently not be capable of deploying TWIC to 50 ports by January 1, 2008, but the first dozen ports receiving enrollment centers do not appear to be based on any type of understandable priority system. The nation's two largest ports, Los Angeles-Long Beach and New York-New Jersey, are not on the initial list. How did DHS choose the initial dozen ports it did?

The Department has set its own informal deadline of September 2008 for vetting and enrolling approximately 750,000 individuals with unescorted access to U.S. ports. In addition to establishing 146 fixed enrollment centers, mobile enrollment centers will also be deployed as necessary. Is it realistic to expect DHS will be able to enroll ¾ of a million people in less than one year, and what capacity does the Department and its contractor have to surge resources and equipment to larger ports to try to meet the September 2008 deadline?

Answer:

The Department of Homeland Security considers all ports to be important for security and commercial reasons. Implementation was prioritized based on port location, volume and type of cargo handled, population, and program risk. The enrollment schedule focuses on initially phasing in both small and large ports to ensure the smooth implementation of the program. The ports of Los Angeles and Long Beach, as well as New York and New Jersey are currently targeted to be deployed by late December 2007. (Note: In NY/NJ, there will be a total of 3 sites; the first is targeted to open in December, with the other two opening within a month of the first one.)

DHS' intention is to implement the program in 39 ports by January 1, 2008, and in all ports by September 2008. We structured our cost model and contract with our enrollment provider to be flexible in order to assign resources as required to address large volumes of applicants over the life of the contract. Overall, the cost model provides incentives to the contractor to enroll workers as quickly as possible because the contractor's revenue is earned directly from the number of enrollments processed.

Question#:	4
Topic:	TWIC readers
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: In response to concerns that card readers had not been adequately tested in the initial TWIC pilot program, the SAFE Port Act bifurcated TWIC, requiring DHS to begin vetting workers and issuing TWIC cards in 2007, but retest TWIC card readers, setting a separate April 11, 2009 deadline for final regulations for those readers.

What progress has DHS made in developing and testing TWIC card readers in the year since the passage of the SAFE Port Act, and do you expect DHS will be able to meet the April 2009 deadline for card reader regulations? When will DHS begin testing TWIC card readers?

Without card readers, TWIC cards will serve as little more than regular ID cards for entry into a U.S. port. Who will be responsible for checking to see if individuals have valid, authentic TWIC cards when they enter a port, from the time the cards are issued, until readers are deployed?

If TWIC needs more time to pilot its program, will this information be used to make other background check programs more efficient? Is this part of the plan? Is DHS coordinating with other departments on this?

Answer:

Since the passage of the Security and Accountability For Every Port (SAFE Port) Act of 2006, steady progress has been made toward planning and facilitating the required TWIC reader pilot tests. To date, the ports of New York/New Jersey, Brownsville, TX, Long Beach, CA/Los Angeles, CA, and a small passenger vessel operator from Annapolis, MD have volunteered to participate in the pilot tests. In addition, an initial draft of the Test and Evaluation Master Plan (TEMP) has been developed and is currently under review by both TSA and the Coast Guard. Physical testing of TWIC readers in the maritime environment will begin shortly after they have been manufactured by vendors. Section 104 of The SAFE Ports Act requires DHS to issue a final rule implementing reader requirements no later than two years after commencement of the pilot programs required under this Act. Although, as discussed above, DHS intends to commence the pilot programs in January 2008, the Department is working to have final rules implementing reader requirements that take into consideration the results of the pilot programs as soon as possible.

After the compliance date comes into effect for a given Coast Guard Captain of the Port zone, owners and operators of MTSA-regulated facilities will be required by regulation to ensure individuals possess a TWIC before being granted unescorted access to secure areas. The TWIC Final Rule, which was published on January 25th, 2007, and became effective on March 26th, 2007, also requires review of each TWIC for tampering, and validation of expiration date, photograph and other security features. Moreover, the Coast Guard will be conducting both random and routine inspections of TWICs using hand-held electronic readers in addition to confirming employer and employee compliance with the existing requirements.

Question#:	5
Topic:	C-TPAT
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The SAFE Port Act made a number of important changes to the Customs-Trade Partnership Against Terrorism, or C-T-PAT, program to improve port security. Those changes, in conjunction with the Container Security Initiative teams working at overseas ports are supposed to help create an expedited review process for containers once they arrive in the U.S. Senators Murray, Collins, Coleman and myself called it a "GreenLane" in our original legislation.

Has DHS developed a third tier, or GreenLane, for C-TPAT membership? If so, how many C-TPAT members have been designated as Tier 3 members, and what additional requirements and benefits has CBP identified for those members?

Since the passage of the SAFE Port Act, CBP has implemented a pilot program to use third parties to validate C-TPAT members operating in China. How many C-TPAT members have elected to participate in the third party validation pilot program in the past year, and what has DHS or CBP learned from the pilot program? Does the Department plan to expand the program beyond China?

Answer:
C-TPAT has established a 3 tiered system to provide benefits to its Importer partners. Tier III importers meet Tier I and II requirements and exceed the minimum-security criteria as outlined in the C-TPAT best practices catalog, allowing them to receive the highest Automated Targeting Score reduction. C-TPAT members also receive other benefits including reduction in the number of compliance measurement exams and certain front-of-line privileges. As of November 16, 2007 there are 230 C-TPAT importers receiving TIER III benefits.

With respect to the second part of the question, C-TPAT identified 304 importer partners that have 75 percent or more of their supply chain in China and which are in Tier 1 status, individually inviting them to participate in C-TPAT's third party validation pilot program. To date, only nine importer partners have elected to participate in the pilot. At the conclusion of the pilot on May 1, 2008, C-TPAT will prepare a report for Congress which will include lessons learned. Currently there are no plans to expand the pilot program beyond China.

Question#:	6
Topic:	Project Seahawk
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The SAFE Port Act gives DHS until October 2009 to establish interagency operations centers at all high priority ports. These centers are designed to improve the collection and sharing of maritime security information at local ports, as well as the coordination of operations among federal, state and local entities at the ports.

What steps has DHS taken to begin establishing interagency operations centers at other ports? Has DHS established a timeline for rolling out these centers, or identified which port or ports will be the next to receive such a center?

Project Seahawk was originally funded through the Department of Justice, and the work there has been coordinated through the U.S. Attorney's Office for the District of South Carolina. The Administration plans to transition Seahawk from DoJ's control to DHS. What is the timeframe for this transition? Does DHS plan to maintain the U.S. Attorney's office role with Seahawk after the transition?

Participation of state and local law enforcement agencies has been key to the success of Seahawk. Some of those agencies have expressed concern that they may not be able to continue their participation without financial assistance from the federal government. Does DHS anticipate providing any assistance to state and local governments in order to ensure their continued participation at Seahawk? What will DHS do at other interagency operations centers as they are established?

Answer:
Interagency Operations Centers:
In the last three years the Coast Guard has established four Sector Command Center-Joint (SCC-J) which are Sector Command Centers with interagency representation from other agencies such as Customs and Border Protection (CBP) and the United States Navy (USN). SCC-Js are located in San Diego, CA, Seattle, WA, Hampton Roads, VA, and Jacksonville, FL. The SCC-J in Seattle is located in a new facility that hosts the Navy, CBP and other port partners from the Puget Sound area.

The Coast Guard's proposed acquisition project to support interagency operations centers at the 24 high-priority Coast Guard Sectors is called Command 21. Command 21 provides sensor and information integration and sharing capability that will establish the maritime domain awareness necessary to support port-level, interagency operations. Working with our interagency partners, including CBP, Immigration and Customs Enforcement (ICE),

Question#:	6
Topic:	Project Seahawk
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Department of Defense, the Secure Boarder Initiative Network (SBInet) Program Office, and state and local port partners, the Coast Guard is refining the project requirements and applying lessons learned from the SCC pilot project in Sector Miami, FL and from Project Seahawk in Chaleston, SC. The planned Command 21 deployment schedule for the 24 high-priority Coast Guard Sectors follows:

FY09:
Charleston — Hampton Roads — New York
San Diego — Seattle

FY10:
Boston — Corpus Christi — Key West
Long Island Sound — Miami — Detroit
Jacksonville — New Orleans

FY11:
Baltimore — Honolulu — Mobile

FY12:
LA/Long Beach — Buffalo — Delaware Bay
St. Petersburg — San Francisco

FY13:
Lake Michigan — Houston – Galveston — SE New England
Anchorage

Project Seahawk:
The Department of Homeland Security and the Department of Justice are working on transition options including identification of resource requirements, port partner participation and a projected timeline. Although no specific transition details have been developed at this time, the Department of Justice has stated it intends to fund Project Seahawk through Fiscal Year 2009.

While Project Seahawk has been a success in the Port of Charleston, and many lessons learned and information technology deliverables are being used to inform plans and projects in support of other interagency operations centers, each port is unique and the Coast Guard is approaching the establishment of interagency operations centers on a one-by-one basis. The level and scope of port partner participation, the operating environment and the specific security and safety needs of each port will drive the eventual makeup and operations of the interagency operating center.

Question#:	7
Topic:	minimum standards
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Section 204 of the SAFE Port Act gave DHS until January 11, 2007 to initiate a rulemaking to establish minimum standards and procedures to secure containers in transit, and until April 11, 2007 to issue a final rule. DHS not only missed both these deadlines, but on May 18, 2007, it sent a letter to Congress stating that the Department had decided not to initiate a rulemaking because the Department did not believe "the necessary technology exists for such solutions." On August 8, 2007, several Senators sent a letter to CBP Commissioner Basham, urging him to reconsider that decision and move quickly to release requirements for a container security device. On August 21, 2007, CBP responded, stating they have developed some preliminary requirements, and that they were under review at DHS. Now Congress is hearing that a container security device standard won't be released before the April 2008 deadline.

What is the status of the Department's requirements for container security devices? Do you expect DHS will be able to release those standards this calendar year?

Answer:

On May 18, 2007, the Department of Homeland Security (DHS), consistent with the requirements of section 204 of the Safe Ports Act, notified Congress of its decision not to initiate a rulemaking proceeding to establish minimum standards for securing containers in transit to the United States within the mandated timeline. DHS readily acknowledges that the process of securing the container is a critical component of a multi-layered strategy to secure the entire supply chain. However, the department does not believe, at the present time, the necessary technology exists for such a solution.

CBP is working actively on the development of system and component technical requirements for a Container Security Device (CSD) System and upon approval by the DHS Secretary, plans to publish a Request For Information (RFI) in the near future. DHS policy concerning applicability and use will be decided upon when an acceptable device(s) is approved. It is anticipated that the device may be used in specific trade lanes.

In September 2007, CBP decided to demonstrate the use of proven Radio Frequency (RF) transponder technology to reconcile in-bond transactions between origin and destination points in response to concerns raised in a Government Accountability Office (GAO) Report (GAO-07-561, April 2007). RF transponders and readers, currently operationally deployed at CBP border facilities under the Free and Secure Trade (FAST) program, were chosen for this planned demonstration. The RF transponder technology is

Question#:	7
Topic:	minimum standards
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

supplemented by digital image capture capabilities (to determine that the container/trailer was not switched) to demonstrate an automated capability to reconcile in-bond transactions. CBP has developed plans, made preparations for, and acquired equipment to support this demonstration with in-bond shipments between the Ports of LA/Long Beach, California, and Laredo, Texas. This demonstration is currently planned for December 2007.

CBP recognizes that current commercial off-the-shelf (COTS) sensor technologies are not operationally ready to support container security or in-bond shipments. CBP and DHS Directorate of Science and Technology (S&T) have tested the most promising technologies and have been unable to find any system ready for immediate operational deployment. In order to assist the industry in developing solutions to satisfy CBP operational needs, CBP, in conjunction with S&T, has developed a CSD Requirements document and related Interface Control Documents. These documents are currently under DHS review, and they will be released shortly through a CBP RFI process.

CBP will continue to monitor the state of technology to acquire and test the most promising COTS solutions for container security and in-bond shipments. These technologies may result from current CBP activities, responses to the upcoming RFI, or otherwise identified through market research. These technologies will undergo both laboratory and field evaluations to assess performance in the operational environment. CBP will also continue to explore the use of operationally proven technologies, such as RF transponders, to immediately address container security and in-bond shipment issues.

Question#:	8
Topic:	ASP systems
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The SAFE Port Act authorized DNDO testing and evaluation activities, and FY2007 DHS Appropriations Act required the Secretary certify that the Advanced Spectroscopic Portal (ASP) systems provide a significant improvement in detection performance over the current generation of monitors. This Committee has asked that GAO provide Congress with an evaluation of the reliability of the testing that conducted earlier this year at the Nevada Test Site (NTS) by DNDO. In seeking this review, we emphasized to GAO that it should not delay the certification decision of the ASP procurement. In August, GAO promised the Committee a fast turnaround on this review as soon as DNDO provided the balance of the test results. However, my staff tells me that as of yesterday DNDO had not so far provided the test results and data.

When will DNDO provide GAO with all the final results and the underlying test data of so-called "Phase III" and "blind" tests conducted earlier this year the Nevada Test site in support of the ASP certification decision?

What has caused the delay in releasing the results of these tests, which were completed in April?

Answer:

The GAO has had the Phase I and III test data since June 25, 2007 (see attachment). The Phase 3 Test Report, which will be classified, is currently in final review within the Department, and the Blind Test Report is presently being prepared. The analysis and assessment of the data is an enormous undertaking that takes a significant amount of time, effort, and collaboration.

Question#:	9
Topic:	security concerns
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: What has DHS been told by port stakeholders are the port stakeholders' most critical port and supply chain security concerns?

Answer:

CBP, through our discussions with the Departmental advisory committee, COAC, has been told that the most critical issue for port stakeholders is ensuring that the government has a comprehensive plan for business resumption in the aftermath of a maritime security incident.

Question#:	10
Topic:	safety concerns
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The focus for port security has tended to be on the movement of goods and monitoring data regarding the contents of a cargo container, its shipper and intended destination. Are there other factors that should be considered to ensure our nation's safety?

Answer:

There are a host of other factors to be considered. The Department of Homeland Security (DHS) is deeply committed to identifying those factors, evaluating risks, and taking action to mitigate them, as appropriate, within the boundaries of our resources.

For example, we have identified small vessels (those defined as under 300 gross tons, whether commercial or recreational, and not otherwise regulated for security) as posing potential risks to the maritime domain. We have been working diligently to accurately asses this risk area and develop a mitigation strategy. As a part of this effort, in June, we hosted the National Small Vessel Security Summit, in which nearly 300 stakeholders from the small vessel community, states, federal agencies, and local communities, cooperated in analyzing possible terrorist uses of small vessels and developing possible preventative actions. The results of this summit are currently being used to craft a DHS Small Vessel Security Strategy.

We are committed to ensuring that ports are physically secure, beyond addressing cargo, through such programs as:

- The Transportation Worker Identification Credential (TWIC), currently being rolled out across the country;
- The Port Security Grant Program, which has distributed billions of dollars to security stakeholders;
- The Area Maritime Security Committees which have developed comprehensive Area Maritime Security Plans, which are being further refined through the inclusion of salvage and recovery annexes; and
- The Domestic Nuclear Detection Office's West Coast Detection Pilot, which will focus on reducing vulnerabilities to rad/nuc threats along maritime pathways into areas of high consequence.

We have also been highly engaged in the President's Import Safety Working Group, which recently delivered an Action Plan that identified areas where the U.S. Government could work to ensure the safety of imported consumer goods.

These examples illustrate only a small fraction of the Departments efforts to ensure the safety and security of the Nation.

Question#:	11
Topic:	training
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: According to GAO, CBP faces difficulties in recruiting qualified staff and in some instances has deployed personnel overseas without the requisite training. How does the agency plan to address these challenges?

Answer:
While CBP has on occasion deployed personnel without the requisite training, it has only been to CSI ports where there were seasoned, experienced CBP Officers with the requisite training and experience already deployed to these locations. The seasoned CBP Officers provided hands on and on the job training. This did not diminish the ability of the CSI port to target effectively. Those individuals lacking the required pre-requisite training were subsequently returned back to the U.S. to receive all required training as timely as possible.

Question#:	12
Topic:	CSI ports
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Although recommended by GAO and the SAFE Port Act, minimum technical operating standards for non-intrusive inspection equipment at CSI ports have yet to be established. What assurances does our nation have that this equipment is capable of detecting weapons of mass destruction within high-risk containers? Which agency within the Department is responsible for the development of standards for NII and radiation detection technologies, and when will standards be established? Is the Department working with port operators to consider possible logistical and configuration constraints this equipment may need to meet?

Answer:

Due to sovereignty concerns, CSI cannot set standards in a foreign country for the purchase and deployment of NII systems. However, it is recommended that host nation counterparts purchase NII systems that follow the guidelines of the World Customs Organization (WCO) Customs Compendium, Container Scanning Equipment, Guidelines to Members on Administrative Considerations of Purchase and Operation. Moreover, this language has been included in all Declarations of Principles signed from May 2005 and beyond. It should be noted that as a requirement for participating in CSI, foreign governments must purchase their own NII equipment and that equipment must either meet or exceed the capability of NII equipment used by CBP domestically.

DHS continues to work with terminal/port operators to determine if NII and radiation detection equipment deployments are impacting trade and the flow of cargo at foreign ports. DHS routinely meets with Secure Freight Initiative (SFI) partners to discuss SFI deployments and their effects on the flow of cargo. As discussions with stakeholders continue, these metrics will be expanded, readjusted, and supplemented.

In accordance with Section 121(f) of the SAFE Port Act, the Domestic Nuclear Detection Office (DNDO), in collaboration with the National Institute of Standards and Technology (NIST), shall publish technical capability standards for the use of NII and radiation detection equipment in the United States. Since Section 121(f) requires such standards to take into account relevant standards and procedures utilized by other Federal department or agencies as well as those developed by international bodies, NIST is presently conducting a study of the detection capabilities required by existing national and international consensus standards for radiological and nuclear detection.

Prior to deploying NII or radiation detection equipment, a complete site survey is conducted at the proposed site. During this survey port /terminal operators are encouraged to participate and provide input. All stakeholders are given the opportunity to provide input into final designs. Deployment activities do not commence until all stakeholder concerns and input have been addressed and satisfied.

Question#:	13
Topic:	GTX
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: The Department is considering developing a Global Trade Exchange (GTX) as a means to enhance its assessments of containers. Does DHS have a timeline for initiating such a program, or is this still in an early planning phase?

Answer:
CBP will be issuing a Request for Quotation (RFQ) shortly to solicit proposals from the private sector for the development of a data clearinghouse to serve as a potential platform for the international exchange of customs related trade data. At this time we anticipate the RFQ issuance in December 2007.

Question#:	14
Topic:	pilot program
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Joseph I. Lieberman
Committee:	HOMELAND SECURITY (SENATE)

Question: Section 235 of the SAFE Port Act requires DHS conduct a 1 year pilot program to assess the risk posed by and improve the security of empty containers at U.S. seaports. What it the status of this pilot program?

Answer:
CBP currently inspects, either physically and/or with NII technology, a significant percentage of inbound empty containers arriving via commercial vessel from foreign locations and will continue to maintain this program.

In FY 2008 CBP plans, in conjunction with the U.S. Coast Guard, to begin a pilot program to visually inspect domestic empty containers as they enter terminal operations at 22 seaports.

Question#:	15
Topic:	supply chain strategy
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: The current draft of the International Supply Chain Strategy does not address gaps and redundancies or the way forward in supply chain security. It is more a compendium of existing programs and practices. Does DHS intend to issue the final International Supply Chain Strategy and how, specifically, will it address gaps and redundancies in the strategy?

Answer:

The DHS Strategy to Enhance International Supply Chain Security, submitted to the Congress on July 13, 2007, was the initial report required by §201(g)(1) of the SAFE Port Act. The Department fully intends to meet the requirements of the Act, including §201(g)(2), which specifies that a final report be submitted not later than 3 years following submission of the initial report.

The initial version of the strategy intentionally established the overarching framework for the secure flow of cargo through the supply chain, building on existing national strategies; plans specific to individual segments of the supply chain and transportation system; and numerous programs and tactical plans developed or being developed by components and agencies. In developing the final report, the Department intends to use the first version as the basis for consultation with domestic and international stakeholders. As such, it deliberately focused on clarifying the DHS-layered security strategy and demonstrating how the current and ongoing programs interlock.

A significant focus of the final version will be based upon this consultation as the Department identifies gaps and redundancies across the supply chain and implements harmonized systems to address them. Where gaps are identified, the final strategy will identify strategic objectives to mitigate them. Where true redundancies are identified, strategic objectives to harmonize the supply chain security system will be outlined, and where possible, programs detailed. However, many of what may be conceived to be redundancies are instead differing layers of the security scheme. As there is no single fail-safe system or program that can guarantee absolute security, DHS must rely upon a multi-layered approach to ensure the integrity of the entire supply chain, from the point of stuffing through arrival at a U.S. port of entry. This multi-layered approach includes the use of advance electronic information, automated systems, technology, and partnerships with the trade and foreign governments.

Question#:	16
Topic:	radiation monitors
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Daniel K. Akaka
Committee:	HOMELAND SECURITY (SENATE)

Question: As you know, the work that DNDO has been doing to test the new radiation portal monitors has been subject to a lot of scrutiny and criticism. Most recently, the Government Accountability Office requested the results of Phase Three and blind tests that were performed on the portal monitors back in April. Despite repeated attempts to get that data, GAO has not been able to do so. DNDO contends that the test results are still being worked on at NIST. The tests were performed in April. It is now October. Have the Phase Three and blind test results been provided to GAO? And if not, why has this taken so long and when will they be ready?

Answer:

On June 25, 2007 a CD containing Phase I and III test data was released to the GAO. The Phase 3 Test Report, which will be classified, is currently in final review within the Department, and the Blind Test Report is presently being prepared. The analysis and assessment of the data is an enormous undertaking that takes a significant amount of time, effort, and collaboration.

Question#:	17
Topic:	TWIC rule
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Norm Coleman
Committee:	HOMELAND SECURITY (SENATE)

Question: Assistant Secretary Baker, the current TWIC rule requires all U.S. Coast Guard merchant marine license holders to obtain a TWIC. My question deals with the very small operators. In particular, those mariners that hold an Operator of Uninspected Passenger Vessel (OUPV) license. These licenses limit the mariner to carrying no more than six passengers for hire. What is the history behind requiring TWIC cards for these license holders?

Answer:

The Maritime Transportation Security Act of 2002 requires all individuals issued a license, certificate of registry, or merchant mariner's document (by the USCG) to obtain a biometric transportation security identification card. Per previous federal law, 46 CFR 15.601, every self-propelled, uninspected vessel as defined by 46 U.S.C. 2101(42)(B), carrying not more than six passengers, must be under the direction and control of an individual holding a license as operator. In summary, current law requires OUPV license holders to obtain a TWIC and DHS has no authority to waive or lessen the requirements.

DHS is concerned on the potential impact to OUPV license holders and is taking action to address. TSA and USCG have established a partnership to integrate the background checks within the TSA and USCG credentialing process. Through this process, TSA will conduct background checks for security issues and USCG will conduct safety and suitability checks to ensure mariners meet security, safety, and character standards. Furthermore, USCG is combining USCG-issued credentials into a single document, the Merchant Mariner's Credential (MMC)--eliminating duplicative security threat assessments.

These streamlining efforts are planned to eventually eliminate the need, in most cases, for mariner visits to one of the 17 Regional Exam Centers for license application and renewal. Instead, it should be considerably more convenient in time and travel expenses for mariners to accomplish initial application and renewal at one of the 147 permanent TWIC enrollment sites and complete the remainder of the USCG credentialing process by mail. As the planning for the MMC and associated requirements mature, DHS will continue to seek to mitigate impacts to OUPV license holders.

Question#:	18
Topic:	OUPV
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Norm Coleman
Committee:	HOMELAND SECURITY (SENATE)

Question: If a mariner has no need to access secure vessels or facilities (in other words, the TWIC card might never be scanned or checked), what is gained by requiring these OUPV licensed mariners to obtain a TWIC that is not already gained by virtue of holding the OUPV?

Has TSA and/or the Coast Guard considered waiving the TWIC requirement for this segment of the population?

Answer:

Please see answer to Question 17.

Question#:	19
Topic:	performance measures
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: In GAO's latest report on the SAFE Port Act, GAO stated that they have recommended to DHS that the Department develop strategic plans, better plan the use of its human capital, establish performance measures, and otherwise improve program operations. GAO also stated that DHS has generally concurred with the recommendations and is making progress implementing them. Can you please update me on where DHS is in the process of developing these plans and performance measures?

Answer:
Proper metrics are critical to ensure the execution of the DHS mission as it relates to the SAFE Port Act. In preparing the report to Congress required by the SAFE Port Act, DHS is currently developing and refining the metrics to improve program operations, to better use its human capital, and to evaluate successes and challenges. Some examples of possible metrics to improve program operations within the SAFE Port Act include: the maximum throughput in Secure Freight Initiative queues, container processing time, alarm rates, and domestic re-inspection rates. As discussions with stakeholders continue, these metrics and others will be expanded, readjusted, and supplemented. The report will be submitted in April 2008.

Question#:	20
Topic:	PSGP
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: The SAFE Port Act authorized $400 million annually for the Port Security Grant Program, doubling the amount the President requested in each of FY06 and FY07. I have had ongoing concerns about homeland security grants at DHS. Specifically, I'm concerned that these grant dollars are going to fund things that aren't remotely related to the items they were originally supposed to fund. This is a significant grant program. Please tell me the measures DHS is putting in place to ensure these grants are funding activities that directly relate to port security.

Answer: Per the Port Security Grant Program Guidance, only eligible entities may submit an application for funding and only for eligible port security projects.

Eligible applicants include:

- Owners or operators of federally regulated terminals, facilities, U.S.-inspected passenger vessels or ferries as defined in the Maritime Transportation Security Act (MTSA) 33 Code of Federal Regulations (CFR) Parts 101, 104, 105, and 106.

- Port authorities or other State and local agencies that provide layered security protection to federally regulated facilities in accordance with an Area Maritime Security Plan (AMSP) or a facility or vessel security plan.

- Consortia composed of local stakeholder groups (e.g., river groups, ports and terminal associations) representing federally regulated ports, terminals, U.S.-inspected passenger vessels or ferries that provide layered security protection to federally regulated facilities in accordance with an AMSP or a facility or vessel security plan.

Eligible projects include:

1. **Enhancing Maritime Domain Awareness (MDA).** MDA is the critical enabler that allows leaders at all levels to make effective decisions and act early against threats to the security of the Nation's seaports. In support of the National Strategy for Maritime Security, port areas should seek to enhance their MDA through projects that address knowledge capabilities within the maritime domain (e.g., access control/standardized credentialing, command and control, communications and enhanced intelligence sharing and analysis).

Question#:	20
Topic:	PSGP
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

2. **Enhancing prevention, protection, response and recovery capabilities.** Port areas should seek to enhance their capabilities to prevent, detect, respond to, and recover from terrorist attacks employing improvised explosive devices (IEDs), as well as attacks that employ other non-conventional weapons. Of particular concern in the port environment are attacks that employ IEDs delivered via small craft (similar to the attack on the USS Cole), by underwater swimmers (such as underwater mines), or on ferries (both passenger and vehicle).

3. **Training and exercises.** Port areas should seek to ensure that appropriate capabilities exist among staff and managers, and regularly test these capabilities through a program of emergency drills and exercises. Emergency drills and exercises (such as the Transportation Security Administration's (TSA) Port Security Exercise Training Program) test operational protocols that would be implemented in the event of a terrorist attack, and consist of live situational exercises involving various threat and disaster scenarios, table top exercises, and methods for implementing lessons learned.

4. **Efforts supporting implementation of the Transportation Worker Identification Credential (TWIC).** The TWIC is a Congressionally-mandated security program by which DHS will conduct appropriate background investigations and issue biometrically enabled and secure identification cards for individuals requiring unescorted access to U.S. port facilities.

5. **Efforts in support of the national preparedness architecture**. Port areas are encouraged to take steps to embrace any of the national preparedness architecture priorities, several of which have already been highlighted as priorities. The following six national priorities are particularly relevant: expanding regional collaboration; implementing as appropriate elements of the National Strategy for Maritime Security, the National Incident Management System, the National Response Plan, and the National Infrastructure Protection Plan and its corresponding Transportation Sector Security Plan; strengthening information sharing and collaboration capabilities; enhancing interoperable communications capabilities; strengthening CBRNE detection and response capabilities; and improving planning and citizen preparedness capabilities.

Applications are reviewed at the field level by the Coast Guard and the U.S. Maritime Administration (MARAD), and at the national level before a federal panel of subject matter experts from the Department of Homeland Security, the Federal Emergency Management Agency, Coast Guard, TSA, MARAD, U.S. Customs and Border Protection, and the Domestic Nuclear Detection Office to ensure that grant dollars are in fact funding activities that directly relate to port security.

Question#:	21
Topic:	FFATA
Hearing:	One Year Later: A Progress Report on the SAFE Port Act
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Last year, the President signed the Federal Funding Accountability and Transparency Act into law—an act which I introduced which requires the Office of Management and Budget to establish and maintain a public Web site that lists all entities receiving federal funds, including the name of each entity, the amount of federal funds the entity has received annually by program, and the location of the entity. DHS will be required to provide information on all DHS grants—including these port grants--to OMB to be posted on this public website. Will you cooperate with OMB to implement the FFAT bill?

Answer: Yes, the Department of Homeland Security will continue to cooperate with any request by the Office of Management and Budget to supply this information. The Department is currently posting those entities receiving Port Security Grant awards on public websites (http://www.ojp.usdoj.gov/odp/news.htm and (http://www.ojp.usdoj.gov/odp/whatsnew/whats_new.htm).

○