THE NATIONAL STRATEGY FOR MARITIME SECURITY

(109–43)

HEARING

BEFORE THE

SUBCOMMITTEE ON
COAST GUARD AND MARITIME TRANSPORTATION

OF THE

COMMITTEE ON
TRANSPORTATION AND
INFRASTRUCTURE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JANUARY 24, 2006 (CAMDEN, NEW JERSEY)

Printed for the use of the
Committee on Transportation and Infrastructure

U.S. GOVERNMENT PRINTING OFFICE
28–259 PDF WASHINGTON : 2006

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

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

DON YOUNG, Alaska, *Chairman*

THOMAS E. PETRI, Wisconsin, *Vice-Chair*
SHERWOOD L. BOEHLERT, New York
HOWARD COBLE, North Carolina
JOHN J. DUNCAN, Jr., Tennessee
WAYNE T. GILCHREST, Maryland
JOHN L. MICA, Florida
PETER HOEKSTRA, Michigan
VERNON J. EHLERS, Michigan
SPENCER BACHUS, Alabama
STEVEN C. LaTOURETTE, Ohio
SUE W. KELLY, New York
RICHARD H. BAKER, Louisiana
ROBERT W. NEY, Ohio
FRANK A. LoBIONDO, New Jersey
JERRY MORAN, Kansas
GARY G. MILLER, California
ROBIN HAYES, North Carolina
ROB SIMMONS, Connecticut
HENRY E. BROWN, Jr., South Carolina
TIMOTHY V. JOHNSON, Illinois
TODD RUSSELL PLATTS, Pennsylvania
SAM GRAVES, Missouri
MARK R. KENNEDY, Minnesota
BILL SHUSTER, Pennsylvania
JOHN BOOZMAN, Arkansas
JIM GERLACH, Pennsylvania
MARIO DIAZ-BALART, Florida
JON C. PORTER, Nevada
TOM OSBORNE, Nebraska
KENNY MARCHANT, Texas
MICHAEL E. SODREL, Indiana
CHARLES W. DENT, Pennsylvania
TED POE, Texas
DAVID G. REICHERT, Washington
CONNIE MACK, Florida
JOHN R. 'RANDY' KUHL, Jr., New York
LUIS G. FORTUÑO, Puerto Rico
LYNN A. WESTMORELAND, Georgia
CHARLES W. BOUSTANY, Jr., Louisiana
JEAN SCHMIDT, Ohio

JAMES L. OBERSTAR, Minnesota
NICK J. RAHALL, II, West Virginia
PETER A. DeFAZIO, Oregon
JERRY F. COSTELLO, Illinois
ELEANOR HOLMES NORTON, District of Columbia
JERROLD NADLER, New York
CORRINE BROWN, Florida
BOB FILNER, California
EDDIE BERNICE JOHNSON, Texas
GENE TAYLOR, Mississippi
JUANITA MILLENDER-McDONALD, California
ELIJAH E. CUMMINGS, Maryland
EARL BLUMENAUER, Oregon
ELLEN O. TAUSCHER, California
BILL PASCRELL, Jr., New Jersey
LEONARD L. BOSWELL, Iowa
TIM HOLDEN, Pennsylvania
BRIAN BAIRD, Washington
SHELLEY BERKLEY, Nevada
JIM MATHESON, Utah
MICHAEL M. HONDA, California
RICK LARSEN, Washington
MICHAEL E. CAPUANO, Massachusetts
ANTHONY D. WEINER, New York
JULIA CARSON, Indiana
TIMOTHY H. BISHOP, New York
MICHAEL H. MICHAUD, Maine
LINCOLN DAVIS, Tennessee
BEN CHANDLER, Kentucky
BRIAN HIGGINS, New York
RUSS CARNAHAN, Missouri
ALLYSON Y. SCHWARTZ, Pennsylvania
JOHN T. SALAZAR, Colorado
JOHN BARROW, Georgia

SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION

FRANK A. LOBIONDO, New Jersey, Chairman

HOWARD COBLE, North Carolina
WAYNE T. GILCHREST, Maryland
PETER HOEKSTRA, Michigan
ROB SIMMONS, Connecticut
MARIO DIAZ-BALART, Florida
DAVID G. REICHERT, Washington,*Vice-Chair*
CONNIE MACK, Florida
LUIS G. FORTUÑO, Puerto Rico
CHARLES W. BOUSTANY, Jr., Louisiana
DON YOUNG, Alaska
(Ex Officio)

BOB FILNER, California, Ranking Democrat
CORRINE BROWN, Florida
GENE TAYLOR, Mississippi
JUANITA MILLENDER-McDONALD, California
MICHAEL M. HONDA, California
ANTHONY D. WEINER, New York
BRIAN HIGGINS, New York
BRIAN BAIRD, Washington
JAMES L. OBERSTAR, Minnesota
(Ex Officio)

CONTENTS

TESTIMONY

PREPARED STATEMENTS SUBMITTED BY WITNESSES

THE NATIONAL STRATEGY FOR MARITIME SECURITY

Tuesday, January 24, 2006

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

The subcommittee met, pursuant to call, at 10:00 a.m., in the Multipurpose Room of the Campus Center of Rutgers State University of New Jersey, Hon. Frank A. LoBiondo [chairman of the subcommittee] presiding.

Mr. LOBIONDO. Good morning. The Subcommittee on Coast Guard and Maritime Transportation is meeting this morning to review the national strategy for maritime security in several federal programs to enhance security in the maritime domain. This field hearing is another in a series of hearings that the subcommittee has held since the enactment of the Maritime Transportation Security Act of 2002 to review the state of security in our Nation's ports and abroad. Under the Maritime Transportation Security Act, the Coast Guard and other Federal agencies have developed and implemented critical Maritime Security Program systems and procedures to improve our awareness of activities in the maritime domain and our capabilities to prevent future attacks in the Maritime Transportation System. However, despite the progress, several key mandates under the Maritime Transportation Security Act have yet to be completed.

One of these critical mandates is the National Maritime Transportation Security Plan. Despite repeated calls by this subcommittee and a deadline that was enacted as part of the Intelligence Reform and Terrorism Prevention Act last year, we still do not have this comprehensive national plan. I urge the Coast Guard and the Department of Homeland Security to complete this plan so that it can be implemented as soon as possible. I believe it is critical. While we do not have the National Maritime Transportation Security Plan, the administration has recently developed and released the National Strategy for Maritime Security to further coordinate the Federal maritime security efforts. The National Strategy is supported by eight components which address specific threats and challenges in the maritime environment.

These components call for increased cooperation, integration and in some cases, expansion of existing programs to enhance maritime security. The components do not, however, contain many details on how Federal agencies will accomplish the strategic objectives outlined under the Strategy. I am very interested to hear our witnesses testify this morning on how their respective agencies will take the recommendations and put them into practice in our ports and on the high seas.

The Strategy also calls for the Transportation Security Agency and the Coast Guard to conclude development of the Transportation Workers Identification Credential, or TWIC, that will ensure the identity of maritime workers that have access to sensitive areas aboard vessels and in our ports. I hope the inclusion of this recommendation signals that the administration is intent on finally completing this rulemaking. Congress required the implementation of TWIC, and when we passed the Maritime Transportation Security Act four years ago, the original deadline for the pilot program was December of 2003 and regulations to implement the program nationwide were supposed to go into effect in 2004.

I thank our local Delaware River ports for their participation in the pilot program, but it is time for the TSA to move forward with this program nationwide. I look forward to hearing more about the results of the pilot program and expect our witnesses to provide us with an update on when we can expect this now long overdue program with its regulations.

The National Strategy for Maritime Security is an important step in our efforts to improve our maritime security responsibilities, but there still is a lot of work that must be done and to take these plans and to translate them into programs and systems that provide enhanced security. I hope that the witnesses' testimony will address some of these challenges, that the subcommittee will learn how the Federal government plans to implement the recommendations. I welcome the witnesses and thank them for their testimony today and I am very pleased that we have several of our colleagues with us and I would like to first introduce and thank Congressman Mike Castle from Delaware for being here and Mike, ask you if you have any opening statement you would like to make?

Mr. CASTLE. I thank you, Chairman LoBiondo, for the opportunity of being here and for holding this very important and timely field hearing and also for allowing me to participate. I would also like to thank today's panel of distinguished witnesses, the first panel and the second panel to come for their presence at this hearing and obviously, their input. Although most of us are not members of the Coast Guard and Maritime Transportation subcommittee, I must say though, that Rob, Allyson and you and I were at a couple of these hearings. I sort of feel like we are part of this subcommittee at this point, but truly we are not. We have all worked closely on issues affecting the Delaware River and Bay, sometimes together, sometimes in opposition to each other.

In particular, since the terrorist attacks of September 2001, improving the security of the men and women who live and work in this part of the country has been our top priority. As all of you know, in July of 2004 the 9/11 Commission issued an extensive report detailing the challenges facing our government in the wake of the attacks in New York and Washington, D.C. The 9/11 report contains critical recommendations and port security has emerged as a significant part of this debate. While the report underscores the importance of securing our Nation's airports, the commission also noted that the increased security efforts around air travel have led to concerns that terrorists may turn their attention to softer targets such as maritime and surface transportation.

In fact, the 9/11 Commission identified container and cargo ships as one area of seaport security most vulnerable to terrorist infiltration. The committee's report identified several chilling scenarios in which terrorists could exploit holes in our commercial shipping system to smuggle nuclear, chemical or biological weapons into the country. As many of the people in this room are well aware, more than nine million marine containers come through U.S. ports each year, most of which are foreign owned and operated by foreign crews. On the Delaware River, the Port of Wilmington is among the busiest terminals, handling hundreds of vessels and millions of tons of cargo annually.

As of today, Customs and Border Patrol is capable of physically inspecting only a small fraction of a ship's cargo. As the Department of Homeland Security continues development of the National Strategy for Maritime Security, increased focus on new technology, such as real-time vessel tracking systems and smart box devices is essential to expanding our national defense system. Once these ships reach our ports it is also critical that we have effective procedures in place for the screening of personnel and ensuring the integrity of critical infrastructure.

The Transportation Worker Identification Credential program is one such initiative which uses cutting edge biometric technology to ensure security officials can protect against unauthorized use of our Nation's seaports. As a former member of the House Select Committee on Intelligence, I am a firm believer in TWIC and other biometric document security technologies.

In 2002 the Port of Wilmington was one of the locations selected to participate in the TWIC pilot program and since then thousands of Delaware workers have taken part in testing TWIC prototypes. The technology has a myriad of uses from border security to private sector security awareness. Although there have been some setbacks in TWIC, I am hopeful that we will soon be moving into the implementation phase of this important initiative.

Although much of the Department's focus has thus far been directed at securing our domestic port facilities, it is also essential that we find ways of improving security at foreign ports, especially in underdeveloped countries where true port security is sometimes nonexistent. The majority of cargo entering the U.S. is loaded in foreign ports and overseen by foreign officials. This presents a serious security problem since most foreign countries are far behind the U.S. in terms of maritime security.

The Government Accountability Office has also documented multiple vulnerabilities at international ports, underscoring the fact that U.S. port security is largely ineffective as long as foreign security remains lax. Like many other transportation sectors, maritime spending is designed for speed and efficiency. Container ships and other vessels carry approximately 80 percent of world trade and it is important that we not significantly impede the flow of commerce. In the end, a truly successful international security strategy will effectively increase security while minimizing the impact on trade.

And just as the international community needs to step up and participate in improving maritime security, so do Federal, State and local governments here at home. One key lesson learned from the mass confusion of September 11 and Hurricane Katrina is that our government has a significant information sharing problem. This is true for the intelligence community and it is true for Maritime Security. From the TSA down to State and local security personnel, timely information sharing and communication with private industry is crucial to improving our ability to accurately identify and respond to threats.

Today's hearing is an important part of this process and I look forward to hearing from each of our distinguished witnesses. Thank you, Mr. Chairman, and I yield back the balance of my time.

Mr. LoBIONDO. Thank you, Mr. Castle. Congressman Andrews, thank you so much for joining us and for all the help and advice you have given this subcommittee. Recognized.

Mr. ANDREWS. Thank you, Mr. Chairman. I am privileged to have this opportunity this morning. I want to begin by referring to a meeting we had just about a year ago on a similar related topic and that was the aftermath of the oil spill on the Delaware River. And I do want to commend Congressman LoBiondo, for his stewardship in achieving a significant legislative victory in 2005 which I believe lays the foundation to prevent such a spill from ever happening again, and I know that that is not the purpose, Frank, of today's hearing, but the commitments that you made and that we supported you on that day about a year ago. We thank you for that and congratulate you for that.

The enemy that we face in the global war against terrorism is above all things adaptive. It is an enemy that studied us rather well, that knows our weaknesses and is usually a few steps ahead of where we are going. Justifiably, this country has been focused intently on airplane and airline security since September 11 of 2001 and we should never rule out the possibility that the next attack will happen there. I think it is far more likely, however, that the next major attack on this country will happen through another means and obviously, one of the leading candidates of that means of attack is our shipping system, the 25,000 cargo containers a day that come into the United States.

We have given those who will testify today a huge responsibility. It is not surprising that there are issues of implementation with respect to meeting that responsibility. I am encouraged by the fact that what we have seen in the months that have passed since September 11 is an analytical clarity as to focusing on what the problem is. You know, there were calls after 9/11 for us to try to board every ship, inspect every container. We could do that. Obviously, there was an incredible early need to be analytically focused on where the real threat is.

There was a secondary need to follow up in putting in place the practical tools to make good use of those analytical conclusions and focus on where the threat is coming from. That is the focus of today's hearing, to see how we are doing in implementing the tools and strategies that we need to focus on the areas where we are at greatest risk. This is by no means an easy job, but it is an awfully important one. And you know, I wake up every morning wondering if this is going to be the day when the next assault will be launched on the country.

The first thing that comes to my mind is what can we do today to be sure that when that day comes, not if it comes, when it comes, that we are prepared to the maximum extent. So I commend the chairman for calling the hearing. I look forward to learning about the progress the Coast Guard and the Department of Homeland Security have made in preparing us for that day and in my own way, if I can contribute toward that preparation, I am eager to do so. Thank you, Mr. Chairman.

Mr. LoBiondo. Thank you, Congressman Andrews and let me take a moment since Rob commented on that hearing of almost a year ago and thank my colleagues because everyone that is here today, Congressman Castle, Congressman Andrews and Congresswoman Schwartz, along with Congressman Jim Saxton, gave some great recommendations, and just by way of an update, we fully expect that this will be part of the Coast Guard conference report which we hope to get concluded, maybe optimistically in February, sometime early in the year, that will become law and I think will go a long ways towards prevention in the future and I thank my colleagues.

Now I would like to turn to Congresswoman Schwartz and thank you for being with us today.

Ms. Schwartz. Well, thank you, Mr. Chairman. I also wanted to acknowledge the fact that I participated in that hearing that we had about the Athos spill just about a little over a year ago. It was my first, I guess, my first official activity as a new member of Congress. I actually had been a member of the committee probably for about a few minutes and you were very gracious in allowing me to participate in that hearing and I have to say it is the way it is supposed to work and I really just appreciate the fact that it was a hearing where people took it very seriously, both those who were testifying and those of us who were there asking the questions about how we could clean up from the spill and how we could prevent a future spill.

And I really thank you for your leadership in the Delaware River Protection Act and in getting that language into legislation and I am on that conference committee with the express purpose of holding on to as much of that as we can and getting that language done because it is important for us to move ahead and not only the clean up, which is mostly done, as I understand it, and I thank everyone for their updates on that, but also in making sure that we prevent any future spills. Which, again, I look forward to this hearing in a similar capacity and all of us, being deeply concerned about the safety and security of our citizens and of the Nation and as has been mentioned, the attention to our airports and air travel. Obviously, that was primary in our minds, but I have taken some time with some of the members in the audience to spend some time hearing more about the activities on the Delaware River, traveling the Delaware River a bit, up and down, and to commend the Coast Guard for the work that you do every day in securing and keeping secure our port.

So I think what we are interested in today is to hear from you about what works well, what doesn't, what more we can do, and I can tell you a specific concern that I have is the proposal for the L and G facility, the terminal that is proposed for Port Richmond and the really very serious concerns we have about whether, in fact, we could ever provide the security that we would need to have at the terminals. You know many of us are opposed to it for security reasons and I am interested in some comments that might be made on both the current commerce and trade, how to protect our citizens from anyone who might be coming on board a vessel, recreation vehicles, as well, of course. It is a very important part of my district to keep the Delaware River a thriving commercial port and also available for recreation, and I have all sorts of plans for ways that we might enhance the North Delaware, as well. So as we populate it more with both business and residents, we also want to make sure that it is as safe and secure as we need to make it for our citizens and for our commercial enterprises, so I look forward to the testimony and continuing under the leadership of Chairman LoBiondo to be able to take actions that we might need to, to secure the port for the citizens of both New Jersey and Pennsylvania and of course, Delaware, as well, so thank you.

Mr. LoBiondo. Thank you very much. Now we will turn to our first panel, Rear Admiral Craig Bone, who is the Director of Port Security for the United States Coast Guard, and Mark Hatfield, who is the Deputy Federal Security Director for Newark Liberty International Airport that is part of the Transportation Security Administration. Admiral Bone, welcome today and await your testimony.

TESTIMONY OF CRAIG E. BONE, DIRECTOR OF PORT SECURITY, UNITED STATES COAST GUARD; AND MARK O. HATFIELD, JR., DEPUTY SECURITY DIRECTOR FOR NEWARK LIBERTY INTERNATIONAL AIRPORT, TRANSPORTATION SECURITY ADMINISTRATION.

Rear Admiral Bone. Good morning, Mr. Chairman, and distinguished Congressional members. I am Rear Admiral Craig Bone, Director of Inspections and Compliance for the U.S. Coast Guard. I was Director of Port Security. We have now organized ourselves under Prevention Response and I have security responsibilities under that Director of Inspection and Compliance. It is an honor to be here today to discuss the Department's role in implementing the National Strategy for Maritime Security. The United States has a vital interest in maritime security. The National Strategy for Maritime Security prescribes for a holistic approach to dealing with a broad array of threats, addressing activities that span from prevention to post-incident recovery to achieve the following four objectives: Prevent successful terrorist attacks and criminal or hostile attacks; protect maritime-related population centers and critical infrastructure; minimize damage and expedite recovery; and safeguard the ocean and its resources.

The Strategy strives to achieve its objectives through enhanced international cooperation, maximize domain awareness, embed security into commercial practices, deploy layered security to unify public and private security measures and assure continuity of the marine transportation system to maintain vital commerce.

The concept of layered security is complex. It involves multiple types of activities to create a network of interdependent and overlapping checkpoints in this system which are designed to reduce vulnerabilities and detect, deter, and defeat threats. It entails developing security measures that cover the various components of the marine transportation system, including people, cargo, infrastructure, conveyances and information systems. These security measures span distances from foreign ports of embarkation, through transit zones, to ports of entry and beyond. They involve the different modes of transportation that feed the global supply chain and are implemented by various commercial, regulatory, law enforcement, intelligence, diplomatic and military entities.

The National Strategy for Maritime Security defines Maritime Domain Awareness, or MDA, as the effective understanding of anything associated with the global Maritime Domain that could impact the safety, the security, the economy or the environment of the United States. MDA, or Maritime Domain Awareness, is neither a program nor a mission, but a state of awareness necessary to achieve maritime security. The Department of Homeland Security, therefore, has tasked the Coast Guard to act on its behalf for implementing the system and processes necessary to achieve the level of MDA required by the National Strategy.

The Maritime Domain Awareness Implementation Team, co-led by the Department of Defense and the Coast Guard, oversees the implementation of the national plan to achieve MDA. This plan is a cornerstone for the successful execution of the National Strategy for Maritime Security and serves to unify efforts across Federal government and the private sector, as well as civil authorities within the U.S. and with our allies and international partners, as well.

Additionally, DHS has worked hard to align all our regulatory and policy development efforts with Customs and Border Protection, the Coast Guard and the Transportation and Security Administration. We meet regularly to discuss policy, participate in interagency regulation development teams and sit on the Operation Safe Commerce Executive Steering Committee. Between DHS, CBP, the Coast Guard and TSA, we coordinate the work of our various Federal advisory committees so we understand all of the trade community's concerns and priorities. Now that the Maritime Transportation Security Act of 2002 and the International Ship and Port Facility Code have been implemented in the port and the facility and at the vessel level, we are monitoring compliance and carefully noting issues for further improvements to the regulatory framework.

We are working closely with TSA, the lead agency for the implementation of the Transportation Worker Identification Credential, TWIC, to assist in the implementation of this new credentialing program. The credentialing program will ensure that all U.S. port workers, including all U.S. mariners, have undergone an extensive security background check and have been found eligible to work within our port facilities and on U.S. ships. The Coast Guard is fully supportive of this regulatory effort. We will do everything within our ability to assist TSA in the development of this rulemaking and ensure that the TWIC and Merchant Mariner Credentialing initiatives are complementary in order to minimize the burden on mariners in the future.

Internationally we continue our efforts with the International Maritime Organization, as well as visiting foreign countries to assess the effectiveness of anti-terrorism measures in foreign ports. To date, 44 countries have been assessed, with Malaysia being the most recent visit, and 35 have been found to be in substantial compliance with the International Ship and Port Security Code. The Coast Guard is on track to assess approximately 45 countries a year, and our goal remains at a 140 countries that we hope to engage by September 2008.

As stated in the National Strategy for Maritime Security, we must pursue an integrated, unified approach with all maritime partners, domestic, international, public and private to ensure the security of the Maritime Domain remains safe and secure. Such collaboration is fundamental to implementing the National Strategy and vital to protecting the interests of the United States. Thank you for the opportunity to testify today. I will be happy to answer any questions at the appropriate time, sir.

Mr. LoBiondo. Thank you, Admiral Bone. Mr. Hatfield, welcome today.

Mr. Hatfield. Thank you so much, Mr. Chairman.

Mr. LoBiondo. We look forward to your testimony.

Mr. Hatfield. Mr. Chairman and distinguished members of the subcommittee, I am both pleased and honored to have an opportunity to speak with you today and hopefully be responsive to your inquiries on the Transportation Security Administration's TWIC, or Transportation Worker Identification Credential project, which we are partnered with our friends from the U.S. Coast Guard in producing. The delivery of the that program, its implementation, will fulfill requirements in the Maritime Transportation Security Act and I am very pleased that I am alongside Admiral Bone in front of the subcommittee today.

The TWIC program has three major goals. First, we are developing a common, secure biometric credential, the physical piece that will represent the credential, that is interoperable across transportation modes and compatible with the existing independent access control systems. Secondly, we are establishing processes to verify the identity of each TWIC applicant, complete a security threat assessment on the applicant and positively link the issued credential to the applicant.

Finally, we will quickly revoke cardholder privileges for individuals who are issued a TWIC credential but subsequently are determined to pose a threat to national security after the issuance of that credential. TSA planned the TWIC program in four phases. We have completed the first three, the first one being planning; the second one, a technical evaluation; the third phase, a prototype process; and then finally, the fourth phase, implementation, itself.

This past summer we completed the testing of the prototype phase and the overall TWIC solution was evaluated against a full range of business processes, policies and requirements. This included enrollment centers and enrollment, security threat assessments, verification of claimed identity, card personalization and production, card issuance and processes for card replication.

Moving to the next phase now, implementation requires the promulgation of a rule. TSA and the Coast Guard, using the experience and the information gained in the prototype testing are currently preparing a joint Notice of Proposed Rulemaking. The

NPRM will propose standards for security threat assessments of workers with unescorted access to secure areas of maritime facilities and vessels. In addition, it will offer standards for a biometric identification credential that reflects the results of a satisfactory assessment and for access control procedures to prevent unauthorized entry into these secure areas, and it will provide a process for redress for workers who are denied a TWIC card. The proposed rule will also address the fee authority enabling the program to be fully supported through user fees.

Before I conclude, I would like to briefly focus on three other areas of maritime security initiatives under way. Intermodal transportation systems converging at America's ports are highly interdependent and of great economic importance. These networks have a highly critical—high criticality rating and demand significant security attention. TSA and the Coast Guard have jointly developed and implemented the Port Security Training Exercises Program, otherwise known as PortSTEP, to provide maritime transportation security communities nationwide with training exercises, evaluations and information technology products to enhance security in the port and maritime environment.

Eight PortSTEP exercises have been completed and a total of 17 exercises are scheduled for the year 2006, building toward an objective of conducting 40 exercises in all. PortSTEP will culminate in a fully vetted and tested port and transportation security exercise pilot program that can serve as a model for TSA and other government agencies. In coordination with the Coast Guard, TSA has implemented the SAIL test project to develop screening technologies and capabilities aimed at enhancing security on ferry systems. This multi-phased effort has tested and evaluated the use of explosive detection systems on two major ferry systems.

The TSA developed and deployed a van portable Z backscatter X-ray system on the Cape May to Lewes Ferry, for explosive detection document scanners on the passenger-only ferry in San Francisco Bay to look for individuals who may have had contact with explosives or IUDs. Planning is underway to initiate a third phase of this important program which will test a total screening program for both passengers and vehicles, targeting that on a large ferry operation.

In addition, TSA is managing a $3.6 million research and development grant program to test and evaluate explosives trace detection equipment for screening passengers, baggage and vehicles in the ferry and cruise line industries. A request for applications for grant awards for vehicle screening equipment will be published this spring. And grants for passenger and baggage screening equipment have already been awarded and procurement of that equipment for testing by the Transportation Security Laboratory in Atlantic City is underway.

After completion of a 30-day test period for deployment of equipment, after that 30-day test period, the deployment equipment will commence for field tests across the maritime passenger industry. This concludes my prepared oral statement. I will be pleased to answer any questions of the committee.

Mr. LoBiondo. Okay. Thank you, Mr. Hatfield. We are going to start off with Congressman Castle with questions.

Mr. CASTLE. Well, thank you, Mr. Chairman. I am in the process of reading a book called Memorial Day. I don't know if you have read it or not. I have got about 50 pages to go and basically it is about the importation on a ship of different aspects of a nuclear bomb and then another bomb which came in from Mexico or something of that nature and they are at this point getting ready to blow up Washington, D.C. I have 50 pages to go, so if I am a little jumpy today, you will understand the nature of my questions and my concern of what possibly can happen here.

Let me start with you, Admiral Bone. First of all, let me just congratulate the Coast Guard on the tremendous work in Katrina. You have probably heard that before, but I just think that is very admirable in terms of, you know, what our military services can do to make a difference. My questions are, I guess, could be anything, but I would like to know more about the whole smart container technology. I remember the last time, perhaps, I looked at this or perhaps at a hearing, we were inspecting something like 2 percent of the containers and then we were having some trouble identifying where containers were coming from and that is where the smart container technology, trying to determine in real time where things are, came into place. And that still does concern me.

I frankly have an abiding concern that we have spent a lot of our TSA dollars and time on airport security and I worry about rail security and cargo security and I worry about how these things are advancing. And don't get me wrong. I think everybody is trying their very hardest and it is very hard to do these things, but I want to make sure they advance as rapidly as possible and I am convinced that we are going to need things like smart technology or whatever it may be in order to truly get the highest degree of safety we possibly can. Can you just bring us up to date on where that whole business of tracking cargo in real time with the smart technology stands?

Rear Admiral BONE. Sir, first off, thanks. Thank you very much for the commendation on behalf of the members of the men and women of the Coast Guard responding to Katrina. But in regard to your specific question, the lead for cargo security is the Customs and Border Protection, not the Coast Guard. We work very closely with them. And that smart technology and the actual technology used in scanning, screening and even targeting is the responsibility of that agency and it is best that they actually respond to that for the record, and I know that the department has indicated that they would respond to specific questions like that. What I will tell you, though, is they were working more closely than ever with CBP, both in identification, upfront, of the cargos, through the Advanced Notice of Arrival System, as well as working with them in the National Targeting Center where the containers and the cargos are screened and targeted.

We have people also with Customs that work in our intelligence center so that the Customs personnel are privy to all intelligence and threat information in their targeting scheme and ability. Also, the results of our International Port Security Program, where we assess, through port visits at foreign countries, the risks and the threats are built into their targeting system based on our reports. So you have an integrated approach, but the lead, again, for that particular system and integration and assessment of that, before it arrives and also when it is at the port, is in Customs. We have the water-borne leg of that, if you look at it, meaning Customs helps us identify that threat and risk and then on the water, we work to address that, again, in an inter-agency forum, those cargos, before they arrive, if need be or at the port, itself.

Mr. CASTLE. Let me sort of go off on a different tangent. I guess either of you can answer this, but I worry about we are doing in the United States, but I realize it is so, that almost virtually, a lot of the shipping which we are going to see is going to be from outside of the United States into the United States. And you mentioned in your testimony about the different ports you look at in foreign countries, et cetera, but I think the foreign port security issues are really important, particularly those who have less available resources. I imagine in some countries it is almost non-existent. I don't know what your inspections are showing, but I can't imagine that in some of the third world countries where we might have some shipping there is a lot of security going on. Is there anything being done with respect to international maritime security, for example, some sort of an international regulatory body or anything of that nature? And have we considered tying international security into trade agreements or any other way of enforcing this so that we can be more comfortable in terms of what is happening in those countries as they start to load containers and bring them into the United States?

Rear Admiral BONE. Yes. In fact, the International Maritime Organization is directly involved in this. Our international ship and port security code mirrors the MTSA code with regard to security, so security both for their facilities, their vessels and even the individuals moving through the system, and qualifications for security officers are inclusive and already are in place. In fact, that is what our international port security visits do. We look and assess whether or not they are implementing the international code that has been put in place and if they don't, in which case we have had a number. As I said in my testimony, we have visited 44. We have found 36 of them to be in compliance. The other ones actually receive a demarche from the State Department, at which point in time it informs them that they have not met the requirements of ISPS and as such, the U.S. will be taking actions with regard to vessels that visit that port.

Vessels that go to those ports and continue trade have to move themselves to a higher maritime security level that involves increased security while they are in the port, as well as there is increased targeting of their cargos automatically by Customs and Border Protection, as well as us. Vessels that comply with that, again, receive increased level of attention upon arrival and if we believe there is a significant threat, they can be basically denied entry. The vessels that don't actually carry out those activities, we board those offshore. Those that don't carry out those activities are denied entry into the United States.

Mr. CASTLE. But it is a continuing quest. You mentioned there is 140 countries you want to do by 2008. You have done 44, so you still obviously have a number more to go.

Rear Admiral BONE. Yes, sir.

Mr. CASTLE. So we won't have a final answer for a couple more years.

Rear Admiral BONE. Yes, sir. Mr. Congressman, but over 75 percent of the cargos, we targeted both the high risk as well as those which—

Mr. CASTLE. The high production.

Rear Admiral BONE. —present the highest amount of cargo. And again, that helps us, again, to target where do you put your resources? One of the comments earlier was, we know we can't do everything, so how do you best assess that risk, look at the highest risk regions and address those first or those highest flow areas so that if we do, God forbid, have a security incident within, we can identify and clear more quickly—

Mr. CASTLE. Right.

Rear Admiral BONE. —those which are legitimate and not hamper their commerce flow.

Mr. CASTLE. And my final question is to Mr. Hatfield. Bring me up to date, if you can, on your time line for TWIC and what is happening during the sustainment phase and if you consult with the private sector, I mean we have it in the Wilmington Port and they seem to like it, but they seem to see some logistic problems and that is to be expected, obviously. But I think it is very important that TSA stay on top of that to make the corrections that I would imagine that the usage of information technology probably changes month by month, if I had to guess.

Mr. HATFIELD. Indeed, sir.

Mr. CASTLE. So can you bring us up to date on that whole TWIC business?

Mr. HATFIELD. Indeed. And of course elemental to any time line is the fact that we are looking to deliver against the requirements of the Maritime Security Transportation Act. And that is a key driver in all of this. The time line, as I had mentioned in my statement, we have completed three of the four phases that we have broken this into and direct to the question, we are in the drafting process right now for the Notice of Proposed Rulemaking. That is an effort that we are conducting jointly with the Coast Guard. We have built upon all of our experience through the prototype, through the technical evaluation, the early planning, to make sure that we have industry input, that we have our stakeholders represented and of course, they will have ample opportunity once that NPRM is released to comment on it before it goes into its final phase.

What does all that mean to implementation? Well, we had senior representatives testify or brief members of Congress last year and they presented a very aggressive time line, speculating perhaps October of this year. I can say that that was a very aggressive speculation and I don't know that that is possible under any scenario. If you look at the NPRM process, and of course there are other elements, the fact that it is a fee-based system requires additional work, additional time in crafting the system. The review for OMB, itself, is two 90-day periods. That is six months of review unless they decide to or agree or volunteer to shorten their section of it.

So we have TSA finishing up the draft, presenting it to the Department, who will then clear it for review by OMB and then we have the public comment periods, too. So all of that said, your best case scenario, if you do the math, it adds up—it heads towards 12 months and that is not a speculation on how long it will take, it is just sort of a cataloging of the various steps in this final process. But the good news is we are in the final process and if I could have a moment just to mention, because you asked about specifically the Delaware River/Bay area, the involvement of the stakeholders, the involvement of our prototype partners and those who were involved during the technical evaluation and the planning, I know that we have gotten kudos and received praise for our inclusiveness during that planning and the kind of double edge to that is, with all that inclusiveness we get a more valid product and I think that is really important at the end of the day, but that takes more time and so that is just one of those contextual pieces that in each of these steps we have sought to be extremely inclusive and not be dictatorial or take a government knows best position, but in fact, really reach out because one of our key objectives is to facilitate commerce and if we overburden them, we won't be facilitating them.

Mr. CASTLE. Thank you. I yield back, Mr. Chairman.

Mr. LOBIONDO. Thank you, Mr. Castle. Congresswoman Schwartz.

Ms. SCHWARTZ. Thank you. As I said in my opening remarks, I would like to just explore a little bit of the position on the proposed L and G liquefied natural gas terminal for Port Richmond, in particular, so I just want some background. You know this as well. I know you may want to call on someone else, so I guess it is mostly questions for Admiral Bone. As I understand it, in November 2005 the Coast Guard did complete some preliminary review about security assessment for the proposed L and G facility in New Jersey, in Logan Township, New Jersey, and concluded that for you to do the appropriate security measures, you were able to conclude that you had, I guess, enough resources to accommodate two to three L and G carriers per week, which, I guess, is what they were proposing. Could you speak to what it would mean if, in fact, if we did—if an L and G facility went into Port Richmond, if we saw more carriers than that, does that mean you would not be able to assess the—be able to, I almost used the word guarantee, but I think that that is actually too strong a word, but to be able to provide the security that is necessary. And basically, in just your preliminary judgment about assessing, one of our deep concerns, of course, is not only the number of carriers, but the density of population when you go further up the Delaware.

We are looking at 1.2 million people that live in Philadelphia, probably more than that if you are looking at the number of people who come in during the day, during the course of the day who work or come into Philadelphia for other reasons, you are talking about maybe a million and a half people to protect several times, many times a week; whether that is, in fact, at all practical; whether you would be able to make some, any kind of assessment at this point that you could provide some security on that. So could you speak to how prepared we might be to handle such a facility?

Rear Admiral BONE. Well, first off, the specifics of—there is a process, a very comprehensive process that is looked at. And each port, if you have seen one port, you have seen one port. Each port has its own unique characteristics, its own challenges regarding safety and security and the same thing is true about facility locations, and this process, again, is a national process in which each of the captain of ports, and I am assuming you know your local captain of port who is here today, who would be involved in that process, in identifying each one of those risks.

What I would say is it involves an assessment of the transit, as well as the facility, itself. It is a very comprehensive process and it takes into account all the other operations that take place in the port and the risks associated with them, whether or not we collectively, and not just the Coast Guard, can meet the requirements needed to provide for the safe and secure operations of the facility as well as the transit, safe and secure transit of that vessel. I don't know the specifics of this port, so I would be presumptuous to even make a statement on it. What I will say is that this is not unique in the United States, to look at liquefied natural gas or individuals intent to expand liquefied natural gas, and the Coast Guard has looked at this very seriously and again looking at both the safety and security.

And I can assure you that the facility and the safe operation, secure operations that won't be approved by the Coast Guard, a plan wouldn't be approved by the Coast Guard and forwarded for consideration unless it, in fact, the Coast Guard was, in fact, assured we could provide for that and that is the commitment that I can give you with that regard. And even when we do put some forward, we say we could do this provided these factors are all put in place. That includes Coast Guard and other resources involved; it is not exclusive. It is looked at as an entire system and the whole system has to be in place to be safe and secure, for cargoes in particular, a hazard like L and G.

Ms. SCHWARTZ. Well, and again, I don't know if this is going to go forward. There is quite a bit of opposition for a number of reasons, but I certainly do look forward to working locally with the Coast Guard here and doing that kind of assessment and your willingness to say it just can't be done, you know, it can't be secure. That is a possibility, I assume, as well. There can always be resources, but it also may not be, but there also may be just too great a risk, as well. That is a possibility in making that kind of assessment, I assume.

Rear Admiral BONE. That is always a possibility, yes, ma'am.

Ms. SCHWARTZ. So I look forward to your commitment to working on that assessment and making that kind of judgment. Let me ask generally, because of your broader responsibility, do you ever look at—rather than just looking at each site in and of itself, consider doing some determinations ahead of time? So basically saying these are locations where we might be able to accommodate a facility more safely, so we are not just looking at the oil industry or private sector or actually in the case of Philadelphia, PGW saying, working with the private sector, here is where we want to put it and then we respond. Because, in fact, we do have serious energy needs in this country and we do want to do more to end our reliance on foreign oil, so we are looking for alternatives. L and G might be a part of that, certainly in the northeastern corridor, and yet we tend to just respond to particular proposals and might there be another alternative, which is basically to say here is a facility, there is a low population, we could provide security here. Why doesn't somebody come into this location rather than always looking to respond to a proposal that comes up?

Rear Admiral BONE. Right. Well, the natural response to that is offshore and offshore facilities are inclusive in that, but those even bring challenges, themselves, in other words to ensure the security of that facility, as you become dependent upon it, the further offshore you have it, the more complicated the resource base is, so that presents a level of complexity. I tell you, it is a private business and if you—what you are looking at is where to place something which is a hazardous environment, you know, that you are looking at in particular. Well, the oil and chemical industry might be equally interested as the L and G or a nuclear power plant or other business entities, you know, and just start identifying for one particular mode or industry over another is not the business of government, I don't think.

Ms. SCHWARTZ. Okay.

Rear Admiral BONE. I mean, and we haven't really been charged.

Ms. SCHWARTZ. You may be right. These are private enterprises.

Rear Admiral BONE. At least we haven't been charged.

Ms. SCHWARTZ. But it is interesting to think about, actually, sort of being a little more proactive, saying here is where we know it would be safer to do such a thing, so it is interesting to consider as we move forward.

Rear Admiral BONE. I think your point is on track. I think what we have tried to do in identifying the criteria, we have identified those criteria which make it more difficult.

Ms. SCHWARTZ. Yes.

Rear Admiral BONE. And then you have to overcome those obstacles. And so if somebody looks at what is being considered, they will look at what they have to overcome and again, the more complex you make it, again, further up river, so to speak, that you move something, then there is more challenges, more infrastructure that you are going to pass. There is going to be more population centers and I agree that in general, especially if it is places where other activities are involved and it is not just an industrial base or a farming area, it does create increased risk and increased challenges for those responsible for providing security for it if it is put in place.

Ms. SCHWARTZ. That is pretty close to saying it is a good idea, so I will leave it at that. I kind of agree with that, so I will declare victory and move on, exactly, which is great. So my only other question would be just related more broadly to the security plans that you require of every facility along the Delaware River and I know you review those plans and assessed them. Do you feel, at this point, that those are adequate? Do you have some concerns about whether your own determination that it be facilities, just waterfront property is adequate? Are there other facilities you feel that we ought to be, that use the river or nearby, that ought to also have security plans and should we be looking more broadly at other major, particularly oil and chemical facilities, that we would want them to make sure that they not only have plans, but that you reviewed them, that they meet the appropriate requirements?

Rear Admiral BONE. Well, one, we have, in fact, examined and found in compliance all the facilities that remain in operation that are required under the MTSA, and the issue isn't so much new plans, it is like anything else. You can put a plan together but now you have to implement it and you have to do it consistently. So it is the lapse of security with regard to those facilities that we have to keep from having occur. And we provide regular exercises and spot checks and random checks of those facilities and we have found facilities noncompliant, you know, not meeting their plan and have taken actions, either in some cases, actually shut down the facility because the security violation is so poor; in other cases, maybe limit cargo transfer or operating in a particular portion of the facility until it is overcome. But those normally, again, are implementation of the plan.

For other facilities in the port, the MTSA and the subcommittee and Congress basically put forth the authority within the Captain of the Port to identify other requirements as may be deemed necessary, but may not meet the threshold of those facilities' security plans and the training and requirements of the people at those facilities and all of those requirements that surround that, as for example, in marinas or other locations. But those are very specific, usually security driven events, increased threat in a particular segment where these other facilities other exist and then a captain of port can implement with, again, the State, the local government, as well as the industry, the actions that is necessary to prevent or provide protection for that area.

Ms. SCHWARTZ. Okay. So I just—you mentioned two things and I will just conclude on this, is that it is not just the plans, it is actually having the training, the people who are involved knowing really what is in that plan, being prepared to implement those plans should they need to, and communicating with others. I think there is a group that meets on a regular basis. I actually visited with them here on the Delaware River, who really do meet each other, know each other and share plans and should an incident occur, be able to communicate with each other. That is one of things that we hear all the time, the ability to communicate across jurisdictions, across geographic areas, I mean to be able to know what each others' plans are and to be trained to implement those plans, as it is critical, the plans on the books, so I am glad that you are paying attention to and I think it is important for you to pay attention to those pieces, as well, not just the written plans in a drawer somewhere.

Rear Admiral BONE. Well, I think your point on the area maritime security committees and their efforts, again, is, as I said in my testimony, this is Federal, State, local, industry, public and private sector responsibilities and it is done not just at the local level, but also on the national level. The National Maritime Security Advisory Committee provided input to the TWIC process and looked at international security issues, as well, and has advised us as we go forward and continues to do so with future regulatory efforts or policy changes.

Ms. SCHWARTZ. Thank you. Thank you, Mr. Chairman.

Mr. LOBIONDO. Congressman Andrews.

Mr. ANDREWS. Thank you, Mr. Chairman. Rear Admiral, in your testimony you mentioned that there are approximately 25,000 containers a day come into the United States, or I believe it is in the committee's preparatory material, and there is a process by which there is an intelligence analysis of which one of those containers should be prescreened when they are loaded at ports outside the United States and that is a product of the intelligence work of a number of agencies.

On a scale of one to ten, ten being perfect and zero being terrible, what is your degree of confidence in the quality of work of that intelligence process in determining which containers should be prescreened before they come to the United States?

Rear Admiral BONE. Well, what I will tell you is that every bit of information that is available to the Customs and Border Protection and to the National Targeting Center that I visited, I am convinced it is vetted, examined and that they, in fact, are doing everything in their power and using every source available to them to target the containers that present the highest risk and to work in an inter-agency effort in order to address that threat. So it is overseas as well as at sea and here in the United States.

Mr. ANDREWS. So is it an eight, is it a nine? What is it?

Rear Admiral BONE. Well, I would say it is a ten for what they know.

Mr. ANDREWS. Okay.

Rear Admiral BONE. What I would offer, is that doesn't mean, I don't want to imply that it is perfect. I don't want to imply that our intelligence systems are perfect and I don't want to imply that there aren't individuals with intent to try to find any gaps in it, but I can tell you that the level of effort that is being given across all agencies to work collectively to not—to thwart that and actually identify those is—

Mr. ANDREWS. Yes. I don't doubt that the effort is there, there is no question about that. What suggestions might you make to improve the process? And again, that is with no disrespect to those trying to run it. Where are we deficient in terms of developing more powerful intelligence?

Rear Admiral BONE. Well, in one of the areas that we are working, the international environment and again, also with Customs, is with both long range identification tracking as well as notice of arrival and departure. And in those notices of arrival and departure, the information being required for vessels before they depart the port so that, again, it allows more time for analysis and assessment, inclusive, as well as of the crews, of where it came from, where it is going to, the cargo, itself, who manufactures it, et cetera, Customs looks at—again, it is better for Customs to answer, give a specific answer to this kind of question, but I can assure you that there is, in fact, an international effort to improve both the notification and the tracking. Again, the ability to screen when a target—you want to be able to identify those things which you have a high level of confidence in and screen those out from those that you have a lower level of confidence in. And the long range identification tracking system will allow us to track a vessel up to 2,000 miles offshore.

Mr. ANDREWS. We are very pleased with one of our local companies here in Camden that Mr. LoBiondo and I have both worked with, led by a gentleman named Jacob Baines, has developed software that helps in that identification process. We are happy that one of our local industries is participating in that. What percentage, obviously without compromising any intelligence information, what percentage of the 25,000 containers that come into the country in any given day are screened and inspected before they are loaded at a foreign port?

Rear Admiral BONE. I don't—again, because I don't do that, Customs and Border Protection does that, they would have to give you that.

Mr. ANDREWS. Okay. In your testimony you talk about radiological screening which is taking place at the Ports of New York and New Jersey and in Long Beach in California. Are those the only two ports where there is radiological screening today?

Rear Admiral BONE. Again, I know that there is radiological screening in other ports. Again, specifically where that—there is screening being done, not just in the ports, but offshore, as well, on vessels and in foreign ports. It would be better that I provide an answer for the record on that.

Mr. ANDREWS. What technological capability do we have to do radiological screening before a vessel gets to port? Here is the scenario I worry about. Terrorists load a dirty bomb onto a container on a vessel and the vessel arrives at the Port of New Jersey and New York and we are able to detect the presence of the dirty bomb and five seconds later it detonates. How defective are we and what technology exists to detect the presence of the dirty bomb before it ever gets to the port?

Rear Admiral BONE. Again, there is, in fact, efforts under way, in foreign ports, as well, that Customs has worked internationally and again, they should talk to the specificity regarding that versus we don't—we again don't have that responsibility. It is a core responsibility. We do have technology that we utilize offshore and again, part of this is, just as you said, it is based on the targeting, based on the—

Mr. ANDREWS. Is the technology based upon boarding the vessel or is it based upon some aerial observation of the vessel?

Rear Admiral BONE. The technology—there is multiple levels of technology and actually going into detail about that technology wouldn't be in the best interest of the government.

Mr. ANDREWS. Okay, I understand.

Rear Admiral BONE. But there is, in fact, a layered set of technologies in order to detect that type of a threat.

Mr. ANDREWS. If terrorists put a chemical weapon in a container and sailed it into a United States port today, do we have any technology that would detect it?

Rear Admiral BONE. Yes, there is some technology that could detect it.

Mr. ANDREWS. Is it deployed?

Rear Admiral BONE. There is deployed technology that could detect it provided, again, what you have to have is identification of it. You know, we don't—you don't go and try to inspect or examine every container, but if there is intelligence provided on it, there is an ability to respond to it. One of the things that has been put in place that brings both—all agencies' assets, it is called Maritime Operations Threat Response—

Mr. ANDREWS. Yes.

Rear Admiral BONE. —capability, MOTR, as it is referred to, and its capability is when a threat is either identified or a terrorist or some piracy event were to take place, regardless of where it is, the capabilities within the U.S. government are brought together to respond to that, including the DoD. This isn't limited—

Mr. ANDREWS. I understand.

Rear Admiral BONE. —to the Coast Guard.

Mr. ANDREWS. Are there technological capabilities that could, in a non-invasive way, detect the presence of a chemical weapon? That is to say, through a UAV or some other mechanism?

Rear Admiral BONE. I am not sure that I could give you an accurate testimony.

Mr. ANDREWS. One final question. And I don't mean this in any way to be critical, but I think it is an observation. From what you just told me, it sounds like we still very much have an intelligence-based protective system here, that we have a system that is really based upon good collection of human intelligence that gives you good leads on which ships to interdict, board and inspect, is that correct?

Rear Admiral BONE. Well, it is intelligence and assessments. I mean, the assessments have been made—

Mr. ANDREWS. I understand.

Rear Admiral BONE. —of the manufacturers, assessments have been made of ports and their systems, assessments are made of ships and the carriers and their historical records. There are assessments made of countries and their, you know, whether the country even has legal authority, you know, and has a mechanism to provide security in their system.

Mr. ANDREWS. Is it fair to say that the principal line of defense against a weapon of mass destruction being brought into an American port is the quality of our intelligence?

Rear Admiral BONE. No, again, there is counter-proliferation efforts underway every day. We have our members in our armed services that are engaged in that overseas. It is not purely intelligence. There are actions being taken every single day to detect and intercept and to screen, not just those, again, that are targeted, but even randomly, so I wouldn't limit it to intelligence and make that kind of a statement.

Mr. ANDREWS. Rather than limited, I said principal source of defense.

Rear Admiral BONE. It is the principal mechanism that we use, it is not—it is the principal mechanism, I think it is true and we refer to Maritime Domain Awareness, like I said, is looking at everything and it is the analysis of that to identify where is it that you address and also, even what you are trying to protect, you know. You look at the conveyance is one thing, like you said. The execution is another. We understand that terrorists want to kill as many people as possible, so we look at that entire layer of security that needs to be in place, not just overseas, but because it isn't necessarily foolproof in one location and we know everyone has to work together and we look at that full layer and the ability to detect and intercept anywhere along, from the manufacturer to the delivery source.

Mr. ANDREWS. I appreciate your answers very much. I would just say to the Chairman that I listened to the Chairman's opening statement and I appreciate his customary courtesy in expressing his concerns about the delay in issuing these regulations executed in this plan. I would just echo what he said, that I am a bit concerned that the sense of urgency that we ought to have about the gravity of this threat is not where it ought to be and I appreciate the work of the subcommittee and shall we say, increasing that sense of urgency and I would lend my voice in support to the Chairman as he continues that effort. Thank you.

Mr. LOBIONDO. Thank you, Congressman Andrews. Admiral Bone, sort of following right up on that with the Maritime Transportation Security Act required the development of the National Maritime Transportation Security Plan. When will the plan be submitted to Congress?

Rear Admiral BONE. I can tell you that the plan has completed inter-agency review and is going through a final review at the Department of Homeland Security, so I can't give you an exact date or time, but I can tell you it is in its final stages. I don't have— I can't—

Mr. LOBIONDO. I understand. It is a little frustrating for us just not to have any—

Rear Admiral BONE. I think what is important is the Strategy, you know, provides where you need to work and areas of emphasis. The plan identifies specifically what inter-agency responsibilities have and what you will see in the plan are many of the efforts that you already see underway, as well as identification and maybe this leads to Congressman Andrews' concerns of the areas where we know we have more work to do.

I didn't want to imply that we solved everything and we don't have much more to do in the way of screening, in the way of technology, in the way of Maritime Domain Awareness and even in our tactics, but I can assure you that that plan does identify it and that the agencies are working collectively on those. We are not waiting for the approval, no more than the ports didn't wait for the National Strategy to begin their efforts working to secure the ports. And I would say the key is the plan is out there. Now, how are we going to go about executing that plan and those responsibilities? And I think when you see—when the plan actually comes before Congress, you will be familiar both with the areas that are being worked, but also you will be able to identify those gaps and hopefully, then, the same support you have with MTSA on, as the Coast Guard and CBP and TSA and the other agencies undertake their efforts to close those gaps.

Mr. LOBIONDO. Well, as I think maybe Mr. Castle indicated in one of his statements, we have so many areas of concern for transportation security, but this committee deals with maritime and with 750 billion or so dollars to the Gross Domestic Product, a lot of our economy at risk and there are a number of us who have repeatedly said that we are not satisfied with the emphasis that has been put on maritime anti-terrorism or port security in terms of an overall product delivered. Not that there aren't many good people that are working on this, but there is a point at which our patience wears pretty thin. If we were to ever have an incident, we have to be able to answer, you know, why we didn't do something sooner and we want to give the proper amount of time to allow for a thorough product to be delivered, but there is a limit to that.

Rear Admiral BONE. I understand.

Mr. LOBIONDO. Along a different line, the Maritime Transportation Security Act also requires the development of a long range vessel tracking system, which many of us believe is extremely crucial. Can you comment or give us the status of negotiation with our international partners to develop standards and criteria for these systems?

Rear Admiral BONE. Yes. We are actually hopeful that in May of this year that IMO will adopt the long range identification tracking system requirements and actually put them into place. And again, the implementation will be over a period of time as with any of our regulations, but by the adoption of that, that would allow for the U.S. government to go forward and institute domestic regulations that match the international standard. And the U.S. is moving forward to have that adopted in May of this year.

Mr. LOBIONDO. Okay, thank you. Mr. Hatfield, you talked a little bit about the TWIC card and some of the delays and you explained some of that. In relation to the TWIC card, can you comment, will—when this is finally developed and implemented, will a maritime worker who is issued a TWIC card be able to use that card at all U.S. ports?

Mr. HATFIELD. Let me answer that by first describing the prototype which is really providing us that roadmap for where we go from here, and in the prototype, interoperability is a key component of that, the ability to grant those privileges, access privileges to a cardholder so that that individual may access various facilities and by making sure that that privilege granting authority is defined and is vested in the appropriate hands. So yes to your question, it will be interoperable if it follows the same course as the prototype and we expect it will, and to when it will be implemented, we are prepared to implement it following the successful promulgation of the rule, and we are in that process right now.

I would like to say we are further along in that process than we are, but we are in that process and we are working with due haste to get the draft cleared out of TSA, present it to the department so that it can then go to OMB and I think we are hopeful, as you are, that OMB may be able to do it in less than the allotted 90 days for that first review and we will see how that proceeds. But I cataloged those steps that are necessary, not that you need me to explain the process, but a swift execution of each of those steps, including public comment in our processing and integration of those comments will get us to the point where we can forward and implement. And that is important to be compliant with the law.

Mr. LOBIONDO. That is good news. We have had testimony at previous hearings raising a lot of concern that there are different requirements at different ports and that this is not necessarily the TWIC card, but just with overall security requirements, and this can be very confusing and challenging for folks to understand if they are required to do something at one port but not required to do it at another port and how does this all come together? We are hopeful that this can be—we can have some basic standards that everyone knows they have to adhere to.

Mr. HATFIELD. It will make uniform an important part of this access security. It will still, though, vest that authority and that policy making opportunity to local facility managers to tailor the policies and procedures for accessing their site, but it provides all of the operators, in its current iteration, the opportunity to have a common use tool so that they have that interoperability and then can build their own site-specific plans around that.

Mr. LOBIONDO. Thank you. Admiral Bone, the Department of Homeland Security has created several university-based centers of excellence to study security related matters. Unfortunately, no center of excellence for Maritime Domain Awareness has been put together or established or looked at. I think that is one of the really critically important issues for the future on an overall total picture. Would you care to comment on what sort of information and/or analysis could such a center produce and if the center right here, let us say at Rutgers, what that might be able to offer to the Coast Guard?

Rear Admiral BONE. I think that first off, especially in Maritime Domain Awareness, where we are trying to integrate all technologies, all capabilities, both those current and those future that are yet to come about, and the integration of sensor technologies, that an academic forum is a great place in order to provide input into that process. And just as DHS has identified other centers of excellence, as you have indicated, MDA would be, I agree, I generally agree that that would be a prime area to look towards, as well.

I met earlier with a gentleman who has some technology and I know is going to testify later, or is scheduled to testify later on radar systems and high frequency systems, HF frequency systems and we need to look at, again, all systems, all capabilities and that includes information systems. That includes existing marine exchange systems, you know, why completely replace everything that is good, that is already in place? Why not best utilize that technology, that capability which exists and I think that with our home port product, we have an opportunity to do that. Just by example, in the university where people have fresh minds and some of our best ideas come out of our lieutenant commanders who come from graduate school and the lieutenants, we implement internally and I think it is a great idea.

Mr. LOBIONDO. Thank you. Do any of my colleagues have any follow-up?

Ms. SCHWARTZ. I just had one or two questions, if I may, thank you. Just to understand, Admiral, when you said that this card, the TWIC will have, let me understand, it will have some basic elements that will be consistent across all facilities, all ports, but then they could add on, each port authority could add on additional elements? Does that mean each card which, as the Chairman said, would you just be—

Mr. HATFIELD. Let me take another run at that for—

Ms. SCHWARTZ. Yeah.

Mr. HATFIELD. —elimination.

Ms. SCHWARTZ. Because you said both things, that it was consistent and then you also said that each port could, or each authority could actually add some of its own elements. Is that adding on elements or is it actually changing it so they won't be interoperable?

Mr. HATFIELD. No. The card itself is designed and as deployed in the prototype, was spec'd to contain the complete number of technologies, a magnetic stripe, a proximity chip, a smart card chip, to the bar code and a linear bar code. So by having all of those components, we address the need to be compatible with legacy systems, the existing access control systems that are in these 3200 identified facilities today, but we also provide state-of-the-art technology going forward so that as they upgrade their systems, as they—we have spec'd access control systems, by the way, to be compatible with the highest technology features of that card. So it can be used today in the most basic mag stripe, just like you run your credit card through the reader and it can go all the way up to the great potential offered by the smart card technology. So that is the range of flexibility we have to be compatible with site-specific technology and then when I talk about a facility being able to add privileges so they can say that this truck driver who currently only goes to Long Beach and San Diego, has got to take a long haul to Portland, he can be identified and granted privileges to access Portland. Of course, I use the West Coast by default because I am from Oregon, but I could come up with an analogy for the East Coast, as well.

Ms. SCHWARTZ. Okay. Just so the technology, so it can actually be used in each of these facilities, it is not adding additional elements or criteria.

Mr. HATFIELD. No, the card architecture is fixed—

Ms. SCHWARTZ. Okay.

Mr. HATFIELD. —but it is designed in a way to provide ultimate flexibility, again, to make sure it can be used today. We don't want to invent the technology of the future and then have to catch up to it.

Ms. SCHWARTZ. Thank you for that clarification. Thank you.

Mr. LOBIONDO. Mr. Castle? Mr. Andrews? Admiral Bone, Mr. Hatfield, I thank you very much. This will conclude the first panel. We will take a five minute break and let the second panel set and then we will proceed.

[Recess]

Mr. LOBIONDO. We will now reconvene the hearing and move to our second panel. We have three panel members who are with us today. We would like to welcome Lisa Himber, who is the Vice President of Maritime Exchange for the Delaware River and Bay Authority; Dr. Scott Glenn from the Institute of Maritime and Coastal Services at Rutgers University; and William Boles, who is the Director of Security for the Port of Wilmington. Ms. Himber, if you would please proceed.

TESTIMONY OF LISA HIMBER, VICE PRESIDENT, MARITIME EXCHANGE FOR THE DELAWARE RIVER AND BAY; DR. SCOTT GLENN, INSTITUTE OF MARINE AND COASTAL SERVICES, RUTGERS UNIVERSITY; AND WILLIAM BOLES, DIRECTOR OF SECURITY, PORT OF WILMINGTON

Ms. HIMBER. Thank you, Mr. Chairman, and good morning, members of Congress. As the chairman said, I am Lisa Himber and I am Vice President of the local maritime exchange, which is a nonprofit maritime related trade association. In addition, I also serve as vice chair of the National Maritime Security Advisory Committee and I am a member of the local area maritime security committee. This morning I am going to briefly discuss the National Strategy for Maritime Security, the Transportation Worker Identification Credential and the importance of expanded information sharing between the private and public sectors to improve and enhance Maritime Domain Awareness.

Let me start by saying that the commercial maritime industry strongly supports the core concept behind the National Strategy for Maritime Security, that is, to align Federal security programs into a comprehensive national effort. Since 9/11 we have made great strides in protecting our homeland. Certainly, individual port operators have implemented significant improvements and Congress and DHS agencies have established myriad new programs designed to mitigate threat. Yet, in many respects the only visible effect of these efforts is to make it more difficult and costly to process vessels, cargos and crews arriving at U.S. ports.

It is our hope that the National Strategy will bring some focus into the various individual initiatives. While the NMSAC, as a committee, did not evaluate the National Strategy for Maritime Security as a whole, members are working to address some of the individual components of the strategy. Currently, for example, we are working to develop a network of subject matter experts in the various industry sub-sectors of individuals upon whom DHS can call for advice and guidance. This will help DHS with one of the key results anticipated by the strategy and that is to assure continuity of the maritime transportation system in the aftermath of an incident.

However, the primary work of the NMSAC has been undertaken with regard to the TWIC program. Having been involved in the program since even before the August 2002 launch of the East Coast pilot, my organization and its membership is keenly interested in the successful deployment of the TWIC. In addition, the NMSAC also elected to make TWIC the number one priority on its agenda in recognition of the national importance of this program. Last May the NMSAC presented DHS with a full set of recommendations for TWIC implementation.

In the first phase of the TWIC program, and you have heard about the planning phase, we believe that TSA did everything right. Yet, in the years—as the years pass, there has only been slow progress and many participants have become disheartened. Some have abandoned the program altogether. Though we continue to believe in the TWIC concept, we are uncertain about its viability as currently envisioned and as an immediate suggestion, we believe that TSA and Coast Guard should develop a rule which reflects ongoing dialog with its industry partners. We believe it is imperative that those who work in and around the Nation's ports and who understand the environment must be involved in the decisions that are made with respect to the program.

NMSAC has not yet received a response from TSA to the recommendations we presented last spring, however we are expecting a briefing in the not-too-distant future. In addition to the TWIC, the National Maritime Security Strategy, the Port Security Grant Program, presidential directives and other communications have all highlighted the need for enhanced information sharing as critical to both incident prevention and response.

Maritime exchanges throughout the U.S. have been concerned with effective information sharing for nearly 150 years and we strongly support programs which capitalize on available information to meet a variety of missions. One example is the recent effort between the Coast Guard and the CBP to simplify electronic crew and passenger manifesting through a single program which meets the requirements of both agencies. There are several other opportunities to improve awareness while at the same time reducing costs for both the private and public sectors. For example, the Coast Guard and industry can and should work more closely together to implement a national real-time vessel monitoring program.

Private organizations are also well positioned to help captains of the port or local CBP port directors add local electronic message centers, distribution lists and other functionality to existing community information system. This would complement the work that the Coast Guard has already undertaken on its home port program, yet would relieve local Coast Guard personnel from administrative tasks, thereby freeing resources for security, search and rescue, environmental protection and other critical missions.

Other examples include expanded sharing of electronic information moving between public and private sector trading partners. We believe there are any number of additional opportunities to share information that is necessary to meet both security and commercial goals and we look forward to continuing to work with the Coast Guard and other DHS agencies to explore projects designed to meet the dual goals of facilitating commerce while at the same time improving homeland security. And I thank you for the opportunity to speak today and would be happy to answer any questions you may have.

Mr. LoBiondo. Thank you very much. Dr. Glenn.

Mr. Glenn. Thank you, Mr. Chairman, Congressman Castle, Congressman Andrews, Congresswoman Schwartz for giving me this opportunity to testify in the potential for Compact High Frequency Radars to contribute to port security through improved Maritime Domain Awareness. My name is Scott Glenn. I am a professor of Marine and Coastal Sciences at Rutgers University. I have been involved in the transition of new research technologies to national security applications since the Cold War. Today I will report on the rapidly expanding technology of Compact High Frequency Radars. I will briefly summarize what they are, how they could support Coast Guard missions at present status and what we need to do to go from here.

First, what is a high frequency or HF radar, as they are known? HF radars operate at very low power in FCC approved windows located between the AM/FM radio bands. Like all radars, when an antenna transmits a signal, that scatters off of targets and a second antenna receives the scattered signal. By placing the radar near the salty water's edge, HF radars take advantage of a radio's wave's ability to travel, as a ground wave, over the horizon and if they follow the curvature of the earth over the horizon, they can see targets that are beyond line of sight.

The two main targets for scattering at HF are surface waves and surface vessels. The larger returns are from the surface waves; we use those to map surface currents. The smaller returns from the hard targets are used to map vessel locations. Traditionally, HF radars aim their receivers using long linear rays hundreds or even thousands of meters long that must be deployed on isolated, straight flat beaches, a difficult real estate negotiation near most population centers. Compact HF radars overcome this limitation using the direction finding ability of circular antenna rays that fit on a single post.

Today, over 95 percent of the world's HF radars are the compact design, manufactured by a U.S. company, CODAR Ocean Sensors. Okay, how can this technology support the Coast Guard mission? Networks of Compact HF Radars, deployed onshore or even on buoys, can increase Maritime Domain Awareness through improved wide-area vessel surveillance and simultaneous environmental data collection. Over the horizon, HF radars provide a layered surveillance capability, bridging the coverage gap between line of sight microwave radars covering the near shore and global satellite systems that cover the open ocean.

Wide-area surveillance systems identify the location of all vessels within an operational area. By tracking vessel behaviors and comparing this information to the voluntary AIS network, we can improve the targeting of specific vessels for intervention well before they enter the port. Because intervention requires putting Coast Guard personnel to sea, up-to-date knowledge of the environmental conditions are required to minimize risks to safety. In the event of an incident, real-time environmental data is required to queue response teams for search and rescue efforts and to minimize further environmental impacts.

Okay, what is the present status of HF radar technology? Rutgers has maintained a continuously operating network of Compact HF Radars for surface current mapping and wave monitoring since 1999. In test demonstration projects with Rutgers, real-time current maps were shown to improve Coast Guard search and rescue response and NOAA's Safe Sanctuary's oil spill response. Recently, the administrator of NOAA wrote a letter to the Assistant Commandant in response to the Coast Guard outlining ways in which the two agencies collaborate in the development of a national HF radar network. I request that this letter be included in the written record.

Rutgers and CODAR Ocean Sensors have partnered in similar demonstration of Compact HF Radars for vessel tracking, conducting and HF—constructing an HF radar test bed at Sandy Hook, New Jersey. The dual use capability, combined with the lower cost and risk of a distributed network of compact radars that are both robust to counter-measures, has attracted research funding from the Office of Naval Research, the Counter NarcoTerrorism Project Office and the Department of Homeland Security. These projects have demonstrated the capability and are now focused on testing hardware enhancements to further improve performance.

Okay, what needs to be done in the next two years to pilot a vessel tracking system? We are at the point where today's challenges are shifting towards the integration of existing components into a real time operational system. A collaborative government/academic/industry partnership that contributes existing expertise and leverages existing infrastructure is a proven transition path. These necessary tasks are readily outlined and known academic and industry groups are available to work on them. International partners, in particular, the Norwegian military, are willing to contribute both money and expertise.

The Coast Guard has been asked by Congress to meet many needs within two-year timeframes. The best place to address one of these is Sandy Hook, where Rutgers maintains an active test bed operated by a collaborative team of the top U.S. experts in this technology. This test bed has been offering year-round real time, 24 hour-a-day service since 2001 and it is the most extensive test bed in the world using this latest technology. The Coast Guard is in a strong position to make this investment and we at Rutgers stand ready to assemble the team and the technology within a center of excellence to demonstrate this capability. Thank you.

Mr. LoBiondo. Thank you, Dr. Glenn. Mr. Boles.

Mr. Boles. Good morning, Mr. Chairman, members of the committee. My name is William Boles. I am the Security Manager and the Facility Security Officer at the Port of Wilmington, Delaware. In March of 2002, in conjunction with the Maritime Exchange, the Port of Wilmington volunteered to test the TWIC card. We stated that we would give the card the full test and we use it as our primary access card, unlike a lot of other facilities. A few months later, we had an East Coast TSA TWIC Team working with us to identify a process to develop a secure ID card that would meet legitimate security needs and legitimate maritime needs. Within a year, the team leader left the project and a whole new team emerged. In fact, over the past two years it has been a revolving door of TSA teams. The communication and cooperation that has always been a part of this project from the first team was no longer there. In the past two years there was little feedback on our ideas and suggestions and Port stakeholders were basically left to respond to the decisions made by the TSA.

The second phase of the TWIC card started on July 23, 2003 at the Port of Wilmington. We evaluated three different technologies, the magnetic stripe, the linear barcode and a contact version of the ICC chip. These are described in my written testimony. Over 3,800 technology evaluation TWIC cards were issued at the Port of Wilmington between July 23, 2003 and June 30, 2004.

The stakeholders were originally advised that the TWIC project would flow from one phase to the next. It didn't. The Tech Eval phase officially ended on October 20 of 2003 and a prototype phase at the Port of Wilmington started on June 1 of 2005. The Port of

Wilmington continued to use the Tech Eval, or the technology evaluation phase TWIC card during this 21-month period so our customers, tenants and employees would not have to get an interim card and then switch back again to the prototype phase card when that phase started.

The TSA gave us continuing support of the Tech Eval card until June 30 of 2004, but it ended abruptly. At this point, we were forced to issue a second type of ID card. We kept using the Tech Eval phase TWIC card as a main access control card even through the implementation of our facility's security plan on July 1, 2004, in addition to the interim card that we were now issuing and it numbered about 200 at that point. As you can well imagine, this caused administrative and access control problems for our port tenants, customers and employees.

On June 1, 2005 the prototype TWIC cards started being issued at the Port of Wilmington. Actually, enrollment started on that date. The first problem we had was that our security consultants couldn't get useful technical information from the Bearing Point people, who were assigned to the project by the TSA, about the TWIC card so we could correct our access control system software and to make the TWIC card work, and to find the proper readers. The prototype card issuance went very slowly in the beginning due to the fact that the card would not work without the readers and software corrections.

Once the readers were installed, interest began to grow in this new TWIC card. As of today, well over 1,600 individuals have been enrolled at the Port of Wilmington. There are also about 100 interoperable TWIC cards that work in our control system. These cards were created or obtained at the Maritime Exchange or Holt Terminals in Gloucester City, New Jersey.

I would like to close by making a few points. The Port of Wilmington is completely committed to the TWIC card. Notwithstanding the up and downs with our tenants, customers and employees, we now have a card that works, and everyone at the Port of Wilmington has noticed. We have a card that works in multiple facilities and with multiple levels of security. We can count on the fact that any TWIC card holder who comes to our gate has been vetted against a Terrorist Watch List. But with this reality, I would like to point out what I believe are two missed opportunities by the TSA in this prototype phase.

Number one is Canadian truck drivers. The Port of Wilmington is serviced by over 700 Canadian truck drivers from some of the largest trucking companies in Canada. I see this as a missed opportunity to have this card recognized by Customs and Border Protection at the Canadian border. The other missed opportunity is biometric readers. There is biometric information on the TWIC card and at the Port of Wilmington they missed a chance to test the biometric features of this card in a seaport setting.

As you see in my testimony, it was a failure with the ICC chip during the technical evaluation phase after that phase ended and we see this as a missed opportunity to see what fingerprint readers would have worked best in this environment.

Finally, my key request is to take this opportunity to appeal for continued support of this prototype phase TWIC card through the implementation date. This request is not only for the Port of Wilmington, but also for the Maritime Exchange Holt Terminals in Gloucester City, New Jersey. If you look at the final paragraph of my written testimony, you will see that the Port of Wilmington and Holt Terminals are now working together to better utilize this ID card. As we found out after the Tech Eval TWIC card phase ended, there may still be lessons learned about this card.

I thank you for the opportunity to speak about the TWIC card experience at the Port of Wilmington.

Mr. LoBiondo. Thank you, Mr. Boles. Mr. Castle.

Mr. Castle. Thank you, Mr. Chairman. I thank you all for your testimony. I want to focus on this whole TWIC business a little bit because it is a little bit disconcerting, and I will start with you, Ms. Himber, because just reading your testimony, and you also said this, I think. I don't know if you said it word for word the same way, but we believe TSA should develop a rule that involves the full participation of industry as partners in the process. The draft of the rule has been completed in the form of NMSAC recommendations. Is that, I mean, that comes from the point of view of where you come from, to a degree, obviously, but is that your only concern about this in terms of how to improve TWIC? Are there other things that you have observed or whatever and this is from, I guess, your judgment that heck, there is a private sector here that can help with this, as well, is where you are coming from?

Ms. Himber. Well, the regulatory process is one of the concerns. There are other concerns regarding the technical and implementation processes. The comment that I made in the document here was specific to the implementation of the rulemaking. As a pilot location, we put together a working group of Delaware River Port stakeholders and we were able to provide input and suggestions to TSA during the course of the pilot program. Concurrent with that or subsequent to that last year, we, as the National Security Advisory Committee, also worked very diligently to put recommendations on paper that could hopefully begin to start some dialog that we believed just simply hadn't happened yet. There are several concerns as far as the implementation of the program that still remain outstanding that we have not seen answers to.

Mr. Boles mentioned some specifically about how to incorporate foreign drivers, and I would add to that foreign seafarers, into the program. We still don't know whether TSA plans to issue a standard or to manage a program, although the MTSA clearly requires that they manage a program. We don't know what the background check processes will be, the waivers and appeal processes, and we don't know whether our workers are going to have to have an employer or other sponsor in order to obtain a card. These are large questions that we don't believe have had any dialog. There has been a lot of one-way communication from industry to TSA, but these are the types of things that I am referencing.

Mr. Castle. You raise a lot of questions. Let me go to Mr. Boles first and I may come back to both of you. Mr. Boles, sort of the same question, in a way, in looking at your testimony, I mean, some of your team leaders left the project, which I didn't totally understand. I don't know if it was a negative or just happened or whatever it may be, and then you critique some of the programs in terms of the bar code, the ICC chip, et cetera, which you seemed to do fairly well. And then there are some other issues that you raised in your oral testimony, and then some concerns, I think, with the providers, the corporate providers and some of the information, the scanners and that kind of thing. What is your view of where we are with the whole TWIC program at this place? I mean, my impression is at the end that you feel a lot of these problems have been straightened out and now we are doing better, but has this advanced as rapidly as it should? Has everybody in the government and in the private sector been as responsive as they should? Are we lagging behind? You know, what kind of mark would you give this after the time that you have dealt with it, because I think it is an important program and I am concerned that we are not doing all that we should do, which is—the value of a hearing like this, maybe you will give us all a list of things we should be going back and paying attention to?

Mr. BOLES. Yes, I feel that way, exactly. This is an extremely important program; that is why we volunteered to do the work that needed to be done to get it through. I believe we are about two years behind with the original implementation date, when we first got involved in this back in 2002. That had to do with the movement through the TSA and the different team leaders and breakdown in communications and right now—

Mr. CASTLE. I am sorry. You said we are lagging by about two years at this point?

Mr. BOLES. Yes, from the original implementation date, which was—I heard it mentioned earlier—was 2003, I believe I was. And so now we are in 2006 and it looks like we are going to be, from what I heard now, maybe in 2007 before the actual implementation comes out. But through all those problems and issues that we have dealt with, we actually do have a card that works now and we are testing it and I guess we have different levels of security to it. At the Port of Wilmington, the card not only works in the main gate—we have other access points, but it works in our administration building. We have several different levels of access in our administration building. We have tenants, Chiquita and Dole and it was Delaware, now Magellan Terminals, who are very interested in this card because they want to do an access card system for their own facilities and they just happen to be in the Port of Wilmington, but they are hesitant to take that step forward to commit to this card with us because they just don't know where it is going because of the lack of the progress for a while there, although they see it moving now. As I said, everyone now sees what it is capable of doing and they are very much behind it, but they are just waiting to see what happens as far as our sustainment period and if implementation occurs.

Mr. CASTLE. Is any other country doing this and if they are, are any of them further along than we are? Can we draw from other countries or is this just something that is almost unique to the United States at this point, or are we so far ahead that we are just the pioneers and you can't really draw from anybody else?

Mr. BOLES. I understand there is a program somewhat like this in Canada I have not seen. I speak to a lot of the Canadian truck drivers. I have not seen a card. The only thing I have seen is the Fast Card and that is where I think we missed a big opportunity. If you ever seen that Fast Card, the Fast program that Customs and Border Protection has at the Canadian border, it is basically a bar code and no photograph or a bunch of information on it, whereas—

Mr. CASTLE. Do you think we could do this here? Sort of an E-Z Pass?

Mr. BOLES. From what I see, this card is capable of doing most anything.

Mr. CASTLE. Okay. Do you both feel that the whole TWIC program is ultimately worthwhile in that these problems that you have faced already are starting to be resolved or can be resolved even with the loss of the two years? Are we going down a blind alley where people are just going to say this is ridiculous, you know, why bother, you know, the thing is ineffective; it works here, it doesn't work there? I mean, I am a little concerned about the whole future of it. I don't mean to lead you to a negative answer because I—this is a program I want to see work. I want to see it be positive, but I worry about some of the lags and the concerns that both of you have expressed.

Mr. BOLES. That is where I have asked the big favor that we continue with the sustainment period because our tenants and customers and the port stakeholders, themselves, if this sustainment period ends abruptly again, and then we are talking about another whole year before the actual implementation, it is very likely that interest will just simply just go away in this card and I don't know what could possibly happen. Someone just thinking now we are just going to go through an implementation that is going to die again, and that is what we are trying to avoid by continuing to issue this card and use the card and work with the card.

Gloucester City, apparently, is looking into taking this card and using the potential of it into their hiring system. We know that there is a possibility that we can do that with our off-site ILA Longshoremen of Wilmington. We have our own people pretty much included, but the ILA, who sometimes works, sometimes don't, there are ways that we can address that, and they are the type of things we look forward to doing once we know for a fact that this card is going to stay with us.

Mr. CASTLE. Thank you. Ms. Himber, do you have a response to that?

Ms. HIMBER. Yes, I continue to believe 100 percent in the efficacy of this program. I think it is the only right answer for the maritime sector and other transportation modes, potentially, as well. I share your concerns about the delays. In fact, I have been one of the most vocal people, I think, to express those concerns at TSA leadership levels. Having said that, do I think there are some opportunities to move along more quickly? Yes. And I think that there may be opportunities, again, with the TSA working with industry to move it along faster and potentially, even more effectively than might be the case when they do get to implementation. So yes, I think we should continue to go down this road. I would hate to see this work wasted. There are people who have already given up on it, as I mentioned, the participants in California have said thank you, it was very nice playing, but come back to us when you are ready. I think that would be a mistake, to abandon it at this point.

Mr. CASTLE. Okay, and I thank the entire panel and I yield back, Mr. Chairman. I may have to leave before it is all over, so I thank you.

Mr. LOBIONDO. Thank you very much for joining us and thank you for your valuable input.

Mr. CASTLE. Thank you, sir.

Mr. LOBIONDO. We are going to invite you to all our subcommittee meetings.

Mr. CASTLE. I am going to become a member of the subcommittee.

Mr. LOBIONDO. Okay. Ms. Schwartz.

Ms. SCHWARTZ. I just appreciated that line of questioning, actually, because I think it is gone so far in this and I think your expression that you feel like this is an important tool for you, is there anything else you want us to be saying to TSA or other, I mean, you expressed some of the emotional—and some of the specifics, but more specifically, you are saying move more quickly, talk to you? I think that is what we were just saying. I see labor is not at the table, but I know they had some of the same concerns that you expressed about appeals process, about who is covered, what information might be included, but either now or have you written down very specifically what you might want us to advocate on your behalf, or do you feel like TSA has not heard that they need to hear in order for us to get them to move more quickly and be more responsive to your concerns?

Ms. HIMBER. I think, at least from the TWIC program office staff, TSA has certainly heard our message and I think they understand and I guess I would second Mr. Bole's comment, part of the problem is, indeed, the rotating leadership within TSA. I believe that that is a big, big part of what the delay has been about. There may have been other reasons, information to which I may not be privy, so we continue to try to relay the message and the concern and any voice that could chime in, particularly yours, would be helpful. Yes, we do need to answer some of these key questions. Yes, we do need to get the program moving sooner rather than later and we do need to discuss it with the stakeholders before implementing any regulations.

Mr. BOLES. Just to reiterate, the most important part from my end is the continuance of the sustainment period. To give you a little idea of how frustrating it can be dealing with TSA sometimes is we started the sustainment period at the end of September. I remember, like September 30, my TSA—my trusted agent who does the enrollment for the TWIC card at the facility walked into my office about 4:00 p.m.; she works until 4:30. And she said I just got told to not come to work anymore and I said this program is going to be sustained. She goes no, I understand that it is not and if I come in tomorrow, I won't get paid. Well, I started making phone calls, Mr. Schwartz, and quite honestly, when Mr. Schwartz and other people on the TSA, there is now good contact, good communications going on and I understand the situation that they can be in sometimes, but she left at 4:30. I was under the impression that I might not see her again and that the program all of a sudden abruptly stopped again and she called me about 4:50 and told me that she would be in the next day, that she just got a call from her—the company that she was working for had called her to say that everything is okay, it is taken care of and I guess about five minutes later I got a call from Mr. Schwartz stating that the sustainment period, the papers had been signed, it was going to actually go on. So it is a very last minute nerve wracking and it is where our tenants and customers have gotten a little bit frustrated.

I am one of the people that Lisa thinks I am an eternal optimist and maybe I am. I have taken some bumps and bruises from my boss because I have supported this program and it has caused some issues and we would just appreciate if we could—if it was going to be sustained—we knew pretty well in advance, not half an hour after the program officially ended that it has been sustained. That is the type of thing that becomes nerve wracking and I have a tough time going upstairs and telling my boss that I am not sure if we are going to have this card tomorrow.

Ms. SCHWARTZ. Okay. Maybe that is something that the Chairman might want to consider, some conversation or something—

Mr. LOBIONDO. Would you yield for a second?

Ms. SCHWARTZ. Yes.

Mr. LOBIONDO. Based on what we have heard from the second panel, we have already made a decision that there will be a series of follow-up questions to be submitted to TSA in writing with written responses requested, and depending on what those responses are will depend on the subcommittee's next action of either quickly pulling together a full focused hearing or—there are some pretty disturbing things here, so yes, you are absolutely right, we will be following up.

Ms. SCHWARTZ. Well, you anticipated my request, so that is great. I think that is a very appropriate action and I fully support it, so thank you, Mr. Chairman. Thank you.

Mr. LOBIONDO. Mr. Andrews.

Mr. ANDREWS. Thank you, Mr. Chairman. I thank the witnesses for their efforts and their testimony. Ms. Himber, on page two of your testimony, you are talking about difficulties in the practical applications of some regulations and you say, "It is clear that many of the Federal regulations promulgated under various laws or presidential directives are simply unenforceable. The U.S. Customs and Border Protection requirement that information concerning all persons entering the United States be provided to the agency in an electronic format not less than 24 hours prior to arrival is an excellent example." What is wrong with that requirement? Why shouldn't we know at least 24 hours before someone enters one of our ports who they are?

Ms. HIMBER. In general, there is nothing wrong with the requirement. Where it becomes problematic, and why I use the word unenforceable, is when you talk about—and then I use the example in my document of the launch operator or the barge operator who might be departing a U.S. port going out to a ship for one purpose or another and then coming back into the United States. They don't know 24 hours prior who the crew is going to be. They may not know until 15 minutes prior to departing the U.S. to ferries. They won't know who their passengers are and they may or may not know who the crew members are. So that is one example of where there needs to be a little bit of tweaking.

Mr. ANDREWS. So perhaps the way to tweak that, and you do suggest this later in your testimony, is some sort of frequent flyer program where someone who frequently is involved in such a trip could be cleared in advance and that person could be on a list of people who would not have to be given the 24 hour notice.

Ms. HIMBER. Right.

Mr. ANDREWS. That sounds pretty reasonable to me.

Ms. HIMBER. The other concern, and I am not purporting to have the answer, but CBP is required to screen every person and how you do that with the pleasure boats, I wouldn't begin to presume, but they—or fishing boats or whoever, sightseeing boats, so—

Mr. ANDREWS. That is obviously a different issue and problem, but I did want to isolate on the shipping industry, itself, though. So one problem we have identified and isolated is where we have barge operators or other vessels that make frequent trips in and out of U.S. waters or out of ports. Are there any other problems for the shipping industry beside that one? Would this rule?

Ms. HIMBER. With this there are, let me say, ongoing questions. Most of the problems, since the regulation was promulgated in April of 2005, we have worked through them. It took some time and unfortunately, because of the nature of some of the regulations being promulgated under security, the rule is in place before you have answered all the questions, so it was difficult, it was challenging, but we did get through it. We are working through some additional concerns, but nothing at this point that anybody would consider show stopping.

Mr. ANDREWS. Well, I think what we would be interested in is if any of those questions yield other specific objections, like the one I think you have already wisely have made about the frequent passengers or frequent flyers. We would like to hear them. And then, Mr. Chairman, I would ask if in your list of follow-up questions if you could include a question to the Coast Guard about the possibility of creating an exception—or excuse me, it would not be the Coast Guard, it would be the CBP—the possibility of creating an exception to this rule or some kind of modification of the rule, as Ms. Himber has suggested.

Mr. LOBIONDO. We will ask.

Mr. ANDREWS. Thank you. I have no further questions.

Mr. LOBIONDO. Okay. Thank you, Mr. Andrews. Dr. Glenn, in your written testimony you stated that there are dual uses for CODAR and can you explain what these dual uses are and how they can be used for the Coast Guard in both the homeland security and in search and rescue?

Mr. GLENN. Dual uses that we presently use them quite extensively for current mapping around the U.S. We have a nice, extensive network off New Jersey. It has been tested by the Coast Guard and it has been shown to improve their search and rescue capabilities. If we can keep this network operating on something other than a scientist grant support, the Coast Guard is ready to put that as a regular tool onto their SAROPS planning tool. That is the first use and most well-developed use.

The other thing that we track with the CODAR systems are the vessels. This is a very high concern for Counter NarcoTerrorism and for the Department of Homeland Security and also the Office of Naval Research. The network is probably going to be in place for current mapping alone; saving lives, saving livelihoods and protecting the environment is a good enough reason to deploy this network. What we are trying to do at Sandy Hook is feed off of that network and use it for vessel tracking so we don't have to install a second network, so one network does dual use.

Mr. LoBIONDO. What other natural resource management response can be implemented with CODAR?

Mr. GLENN. One of the best examples of that is off the California—State of California just invested $22 million in putting the CODAR network across the whole State and the big driver for that was beach protection. The economies of the beach depend on the beach towns and the State, really, depend on clean beaches, and by knowing what is in the water and where it is going or if something washes up on the beach, where it came from, is critical information to keep the beaches clean and those economies going. And so that is one of the main uses of the system. The New Jersey Department of Environmental Protection is also very interested in how this can be used to look at low-dissolve oxygen off of our coast. It helps them decide where to sample, when to sample and when to put boats out. And so just as we do Maritime Domain Awareness for the Coast Guard, for vessel interdiction, we can do Maritime Domain Awareness for our own environmental groups or scientists, like myself, or fisheries groups that can then better respond to what is going on with their more expensive boats.

Mr. LoBIONDO. Low-dissolve oxygen?

Mr. GLENN. If you don't have a bubbler going in your fish tank and there is a top on it, eventually all the oxygen goes away and the fish die. The biggest example of that was in 1976 when there was a massive fish kill along our entire coast. There are several regions of recurrent low-dissolve oxygen along the New Jersey shelf and we have to worry about those because they affect mostly the benthic organisms, the shellfish that can't swim out of the way.

Mr. LoBIONDO. Okay, thank you. Ms. Himber and Mr. Boles, what you had to say about TWIC card was, I think, very helpful and important. Just to reiterate a little bit, I would like, since you know we are going to be doing some follow-up, could you just, for my sake, restate what you believe the top three challenges/problems are and/or questions that we need to focus on getting an answer? What are your top three?

Ms. HIMBER. My first one, of course, is the schedule. I would like to know why, you know, what is causing the delay and what we can do between now and implementation to minimize further delays. The second big question that I would ask and really, it is several issues lumped into one question, what is the status of the program as far as will it be government managed? When can we expect answers? I guess the easiest way to say it is when can we expect answers to the questions that we have posed regarding the critical open questions surrounding the program, such as waivers, background checks and appeals for our nationals in the program?

Mr. LoBIONDO. Mr. Boles?

Mr. BOLES. I would add again the sustainment to implementation for Wilmington and Gloucester City and the Maritime Exchange, but also definitely on the background checks. I work pretty closely with the union leadership and that is an extreme concern of theirs and in addition to that, as Lisa said, the appeal process outlined that. And the waiver process, from what I heard, the waiver process in Florida was used to grandfather employees at their seaports in good standing. I always try to figure out how they eventually came around to grandfathering in most of their employees and that is how they ended up doing it, I understand.

Mr. LOBIONDO. Okay, any follow-up from my colleagues? No. One final question for Ms. Himber. As a member of the National Maritime Security Advisory Committee, do you feel the committee is being utilized in full potential and that its recommendations are given full consideration by the Department of Homeland Security?

Ms. HIMBER. Yes and no. We did a lot of good work and I think particularly on the TWIC program. I am, you know, disheartened that we haven't gotten a response yet. There have been a couple of issues that have surfaced on the committee agenda that we are continuing to explore as possible agenda items. I think the committee will soon be, perhaps, more effective than it is today, but having said that, it has been in operation less than a year. It was ramped up and we met for the first time in just March of last year, so I think some of the members are kind of finding their way and we will put together a list of agenda items that we believe can be of distinct benefit to the DHS and we look forward to having that opportunity and getting those kinds of responses to improve the environment under which we all have to operate.

Mr. LOBIONDO. Okay. I want to thank the panel very much. This was extremely helpful. You can expect to continue to hear from us and we appreciate and look forward to your continued feedback. The subcommittee is now adjourned.

[Whereupon, at 12:24 p.m., the subcommittee was adjourned.]

DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF

REAR ADMIRAL CRAIG BONE
DIRECTOR OF INSPECTION AND COMPLIANCE
U.S. COAST GUARD

MARK HATFIELD
DEPUTY FEDERAL SECURITY DIRECTOR
FOR NEWARK LIBERTY INTERNATIONAL AIRPORT
TRANSPORTATION SECURITY ADMINISTRATION

ON THE

NATIONAL STRATEGY FOR MARITIME SECURITY

BEFORE THE

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

SUBCOMMITEE ON COAST GUARD AND MARITIME TRANSPORTATION

U. S. HOUSE OF REPRESENTATIVES

JANUARY 24, 2006

Good afternoon Mr. Chairman and distinguished Members of the Committee. It is our pleasure to be here today to testify on the National Strategy for Maritime Security.

An Overview of National Strategy for Maritime Security

On December 21, 2004, President Bush signed National Security Presidential Directive 41/Homeland Security Presidential Directive 13 (NSPD-41/HSPD-13) with the goal of establishing U.S. policy, guidelines, and implementation actions to enhance U.S. national security and homeland security. It directs that all U.S. Government maritime security programs and initiatives be coordinated in order to achieve a comprehensive and cohesive national effort involving appropriate federal, state, local and private sector entities. The Secretaries of Defense and Homeland Security were jointly charged with leading a collaborative interagency effort to craft a National Strategy for Maritime Security (NSMS) and eight supporting plans. The NSMS highlights some key ideas:

- The safety and economic security of the United States depend upon the secure use of the world's oceans. Maritime security harmonizes the need for protection against terrorist, hostile, criminal and dangerous acts with the need for vibrant, secure maritime commerce that underpins economic security and well-being. Therefore, the United States has a vital national interest in maritime security.
- Maritime domain security is a global issue. Because all nations benefit from this collective security, all nations must share in the responsibility for maintaining maritime security;
- Security in the maritime domain is a shared responsibility between the public and the private sectors.
- Maritime security encompasses threats from all criminal or hostile acts, such as the smuggling of contraband, illegal immigration, piracy, illegal harvesting of natural resources, and the threat of terrorist activities.

The NSMS strives for a holistic approach to dealing with the broad array of threats, addressing activities that span from prevention to post-incident recovery to achieve the following four objectives:

- Prevent successful terrorist attacks and criminal or hostile acts;
- Protect maritime-related population centers and critical infrastructure;
- Minimize damage and expedite recovery; and
- Safeguard the ocean and its resources.

The National Strategy strives to achieve its objectives through five cross-cutting strategic actions:

- Enhance international cooperation to ensure lawful and timely actions against maritime threats;
- Maximize domain awareness to support effective decision-making;
- Embed security into commercial practices to reduce vulnerabilities;
- Deploy layered security to unify public and private security measures; and
- Assure continuity of the marine transportation system to maintain vital commerce.

U.S. COAST GUARD

Implementing the National Strategy

NSPD-41/HSPD-13 created an interagency Maritime Security Policy Coordinating Committee (MSPCC) to serve as the primary forum for coordinating U.S. Government maritime security policies. The MSPCC coordinated the development of the NSMS and its supporting plans, and is now actively working on assigning responsibilities and tasks to agencies within the government for implementation.

Maritime Operational Threat Response or MOTR

The Maritime Operational Threat Response, or "MOTR" Plan, is part of the President's National Strategy for Maritime Security. In 2005, as part of the National Strategy for Maritime Security, Department of Homeland Security (DHS), Department of Justice (DOJ), and the Department of Defense (DOD) developed the MOTR Plan, which builds upon and improves the PD-27 process to ensure nationally coordinated maritime operational response to address the full spectrum of 21st Century maritime security and defense threats to, or directed against, the United States and its interests globally. MOTR addresses the full range of maritime security threats, including actionable knowledge of or acts of terrorism, piracy and other criminal or unlawful or hostile acts committed by both state and non-state actors. Maritime operational threat response includes the deployment of capabilities and use of force required to intercept, apprehend, exploit, and when necessary, defeat maritime threats. Implementation of the MOTR Plan envisions employing an integrated network of existing national-level maritime command and operations centers to achieve coordinated, unified, timely and effective planning and mission accomplishment by the U.S. Government. The MOTR Plan establishes the protocols and procedures for achieving that coordinated response and ensuring the delivery of desired U.S. outcomes. MOTR provides an effective mechanism for the United States to approach maritime security threats and to develop timely and tailored responses based on dispersed authorities, capabilities, competencies and partnerships. In short, MOTR improves the ability of the United States to bring the right assets to bear when maritime threats affect American interests anywhere in the world.

Integrating the Layers of Security

The concept of "layers of security" is complex, involving multiple types of activities to create a network of interdependent, overlapping and purposely redundant checkpoints designed to reduce vulnerabilities, as well as detect, deter and defeat threats. It entails developing security measures that cover the various components of the maritime transportation system, including people, infrastructure, conveyances and information systems. These security measures span distances geographically—from foreign ports of embarkation, through transit zones, to U.S. ports of entry and beyond—and involve the different modes of transportation that feed the global supply chain; and are implemented by various commercial, regulatory, law enforcement, intelligence, diplomatic and military entities. A significant challenge to constructing integrated layers of security is the fact that many of the layers are the responsibility of different agencies. Integrating these disparate maritime security layers involves not only unity of effort, shared responsibility, partnership, and mutual support, but requires an agency with significant maritime security responsibilities to step up and act as a coordinator for the purposes of integrating the government's efforts to provide layered security.

Developing Maritime Domain Awareness

The National Strategy for Maritime Security defines Maritime Domain Awareness (MDA) as "the effective understanding of anything associated with the global Maritime Domain that could impact the security, safety, economy or environment of the U.S." MDA is neither a program nor a mission, but rather a state of awareness necessary to achieve maritime security. DHS therefore has tasked the Coast Guard to act on its behalf for implementing the systems and processes necessary to achieve the level of MDA required by the National Strategy. The MDA Implementation Team, co-led by DOD and the Coast Guard, oversees the implementation of the National Plan to Achieve MDA. This plan is a cornerstone for the successful execution of the National Strategy for Maritime Security and serves to unify efforts across the Federal Government, with the private sector and civil authorities within the United States, as well as, with our allies and international partners. MDA has many stakeholders. Within DHS, it supports and is supported by U.S. Customs and Border Protection (CBP), the Coast Guard, U.S. Immigration and Customs Enforcement (ICE), and the Transportation Security Administration (TSA). MDA also supports and is supported by DOD, as well as DOJ and other federal, state and local law enforcement agencies.

Preparing for Maritime Recovery Operations

The private sector has traditionally demonstrated an ability to adjust their activities in response to disruptions in the maritime transportation system, so much so that it has often been said to be "self-healing" in nature. Widespread disruptions caused by a security-related incident of national significance, however, could threaten to bring large portions of the maritime transportation system to a virtual standstill; hence, contingencies must be prepared. Assuring continuity of commerce requires extensive coordination between the public and private sectors in order to restart or keep the flow of commerce moving during or following such an event. On the national level, recovery policies and procedures that emphasize assuring continuity of commerce in the maritime domain, such as the Maritime Infrastructure Recovery Plan and the Plan to Re-establish Cargo Flow, must be closely coordinated with the other federal agencies and, most critically, the private sector.

Partnering for International Maritime Diplomacy

The Coast Guard, in consultation with the Department of State, the lead agency for international affairs, now more than ever, will play a vital role as an instrument of national security in protecting, promoting and defending the maritime interests of the United States and our international partners around the world. In our international maritime diplomacy role, the Coast Guard can assist other nations in: (1) development of national maritime policies, strategies, standards and legislation; (2) the professional and material development of national maritime security, maritime safety and naval forces; and (3) the development of other maritime management and regulatory regimes. The Coast Guard has traditionally been the chief advocate for the United States in international issues involving maritime safety. Since 2001, the Coast Guard has led interagency efforts to establish a maritime security regime via international forums such as the International Maritime Organization (IMO).

International Port Security Assessments

Internationally, we continue our efforts visiting foreign countries to assess the effectiveness of anti-terrorism measures in foreign ports. To date, 43 countries have been assessed, with China being the most recent visit, and 35 have been found to be in substantial compliance with the ISPS. The Coast Guard is on track to assess approximately 45 countries per year and our goal remains to visit about 140 countries with whom we trade by September 2008.

Long Range Identification and Tracking (LRIT)

Long Range Identification and Tracking (LRIT) is another area we have been pursuing on an international front. LRIT is all about increasing the transparency of vessels plying the global maritime concourse. It provides for persistent detection, classification, identification and tracking of cooperative vessels. This capability will align decision makers and operational commanders so they have a clearer understanding of the vessel traffic in areas of interest.

Through the International Maritime Organization, we, collectively, have taken the first step in making LRIT a reality – drafting amendments to the 1974 SOLAS Convention that address the interests of all countries concerned. It is also important to note that the proposed text of the LRIT amendment will make it clear that possession of LRIT information, by itself, gives Contracting Governments no new authority to act. Rather, it gives them the ability to acquire information on the whereabouts of vessels of concern to them.

Maritime and Cargo Security

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

Additionally, DHS has worked hard to align all of our regulatory and policy development efforts with CBP, the Coast Guard, and TSA. We meet regularly to discuss policy, participate on inter-agency regulation development teams and sit on the Operation Safe Commerce Executive Steering Committee. Between DHS, CBP and the Coast Guard, we coordinate the work of our various Federal Advisory Committees so that we all understand the trade community's concerns and priorities. Now that Maritime Transportation Security Act of 2002 and the International Ship and Port Facility Security (ISPS) Code have been implemented at the port, facility and vessel levels, we are monitoring compliance and carefully noting issues for future improvements to the regulatory framework.

U.S. CUSTOMS AND BORDER PROTECTION

CBP plays a significant role in maritime security and cargo security for the Department. CBP, as the guardian of the Nation's borders, safeguards the homeland---foremost, by preventing the entry of terrorists and instruments of terror into the United States, while, at the same time, enforcing the laws of the United States and fostering the Nation's economic security through lawful travel and trade. Contributing to all this is CBP's time-honored duty of apprehending individuals attempting to enter the United States illegally, stemming the flow of illegal drugs and other contraband, protecting our agricultural and economic interests from harmful pests and diseases, protecting American businesses from theft of their intellectual property, regulating and facilitating international trade, collecting import duties and enforcing U.S. trade laws.

In the aftermath of the terrorist attacks of September 11, 2001, the legacy U.S. Customs Service (now CBP) developed initiatives to meet our twin goals of improving security and facilitating the flow of legitimate trade and travel. CBP's homeland defense strategy to secure and facilitate cargo moving to the United States is a layered defense approach built upon five (5) interrelated initiatives. These initiatives include: the 24-Hour Rule and Trade Act rules, the Automated Targeting System (ATS) (housed in CBP's National Targeting Center (NTC)), the wide-spread use of sophisticated non-intrusive inspection (NII) technology at ports of entry, the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT).

Advance Electronic Information

As a result of the 24-Hour Rule and the Trade Act, CBP requires advance electronic information on all cargo shipments coming to the United States by land, air and sea, so that we know who and what is coming before it arrives in the United States.

Automated Targeting System

The Automated Targeting System is essential to CBP's ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags" and determine which passengers and cargo are "high risk" and should accordingly be scrutinized at the port of entry or, in some cases, overseas.

ATS is a flexible, constantly evolving system that integrates enforcement and commercial databases. ATS analyzes electronic data related to individual shipments prior to arrival and ranks them in order of risk based on the application of algorithms and rules. The scores are divided into thresholds associated with further action by CBP, such as document review and inspection.

Detection Technology at Air, Land and Sea Ports of Entry

NII technologies, including radiation detection equipment, are a critically important component of CBP's layered enforcement process that enable us to screen a larger portion of the stream of commercial traffic in less time while facilitating legitimate trade. Since September 11, 2001, CBP has developed a multi-faceted strategic approach to address the radiological smuggling threat that begins outside of the United States where the movement of nuclear and radiological materials may be initiated, and continues to the U.S. border. We currently have 170 large-scale NII imaging systems deployed (including 59 systems to seaports), 567 radiation portal monitors (RPMs) deployed (including 143 RPMs to seaports), 549 radiation isotope identification devices (RIIDs) deployed (including 200 RIIDs to seaports), and 12,449 personal radiation devices (PRDs) deployed (over 3,500 PRDs to seaports). Used in combination with our layered enforcement strategy, these tools provide CBP with a significant capability to detect nuclear or radiological materials.

Container Security Initiative

Every day, approximately 25,000 seagoing containers arrive at the Nation's seaports equating to nearly 9.2 million a year. About 90% of the world's manufactured goods move by container, much of it stacked many stories high on huge transport ships. Each year, 200 million cargo containers are transported between the world's seaports, constituting a critical component of global trade.

The fact is that, today, the greatest threat we face to global maritime security is the potential for terrorists to use the international maritime system to smuggle terrorist weapons – or even terrorist operatives – into a targeted country.

Clearly, the risk to international maritime cargo demands a robust security strategy that can identify, prevent and deter threats at the earliest point in the international supply chain, before arrival at a seaport of a targeted country. The Nation developed a cargo security strategy that addresses cargo moving from areas outside of the United States to our ports of entry. Our strategy focuses on stopping any terrorist shipment before it reaches the United States and then, only as a last resort, at a U.S. port of entry, if it should arrive there.

CSI enables CBP to work with our host counterparts to screen and inspect high-risk containers before they are loaded on board vessels to the United States. CBP implemented CSI in January 2002 because we recognized that inspecting containers with terrorist weapons concealed inside them, on arrival in the United States, would be too late. Today, CSI is one of the few multinational programs in the world actually protecting the primary means of global trade – containerized shipping – from being exploited or disrupted by international terrorists.

Through the CSI program, CBP deploys multi-disciplined teams comprised of agents, intelligence analysts, and CBP officers to selected foreign seaports throughout the world, to protect the United States and its citizens from both direct and indirect terrorist attacks in the maritime cargo environment. A critical component of the CSI program is the Non-Intrusive Inspection (NII) equipment, which includes radiation detection equipment, that allows the CBP teams sent to foreign ports to select containers for inspection prior to placement of the container on a ship bound for the United States, based on established risk factors and current intelligence. Under the CSI program, CBP may also loan foreign authorities non-intrusive inspection and radiation detection equipment until such time as the foreign authority is able to procure its own equipment, and CBP may provide training for domestic or foreign personnel involved in the CSI program. Today, CSI is operational in 42 ports in Europe, Asia, Africa, North America, and South America. CBP is working towards strategically locating CSI in additional foreign seaports with a nexus to terrorism.

To inspect all high-risk containers before they are loaded on board vessels to the United States, CBP plans to continue fostering partnerships with other countries and our trading partners. In addition, the World Customs Organization, the European Union and the G8 support CSI expansion and have adopted resolutions implementing CSI security measures introduced at ports throughout the world.

Customs-Trade Partnership Against Terrorism (C-TPAT)

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary partnership between CBP and industry to secure the international supply chain. C-TPAT importers secure supply chains from the foreign factory loading docks of their vendors to the port of arrival in the United States. CBP, in return, offers C-TPAT shipments expedited processing and provides C-TPAT participants with other benefits.

To join C-TPAT, a company must conduct a comprehensive self-assessment of its current supply chain security procedures using C-TPAT security criteria and best practices developed in partnership with the trade. A participant must also commit to increasing its supply chain security to meet minimal supply chain security criteria. Perhaps most importantly, participants also make a commitment to work with their business partners and customers throughout their supply chains to ensure that those businesses also increase their supply chain security. By leveraging the influence of importers, C-TPAT is able to increase security of U.S-bound goods to the point of origin (i.e., to the point of container stuffing). This reach – to the foreign loading dock – is beyond the regulatory reach of the U.S. Government, but critical to the goal of increasing supply chain security.

C-TPAT is currently open to all importers, cross-border air, sea, truck, and rail carriers, brokers, freight forwarders, consolidators, non-vessel operating common carriers, and U.S. Marine and Terminal operators. We are currently enrolling certain foreign manufacturers in the C-TPAT program and will continue to develop ways to include this important element of the supply chain in the program. The intent is to increase point of origin to point of arrival security into the supply chain.

Although C-TPAT is a partnership, the risk is too great to simply take participants at their word when it comes to their supply chain security. We have created a cadre of specially trained supply chain security specialists to validate the commitments made by C-TPAT participants and to ensure that the participants are increasing supply chain security as they have promised and that their measures are reliable and effective. These specialists meet with personnel from C-TPAT certified companies and their business partners and observe the security of their supply chains, including security at overseas loading docks and manufacturing plants, as well as transportation links outbound to the United States. Through this validation process, we work with certified members to identify ways that they can further increase their supply chain security. Companies that are not honoring their commitments may be suspended or removed from the program and lose their C-TPAT benefits.

As of January 6, 2006, C-TPAT has assessed and accepted the security profiles of 5,651 companies; there are more than 4,700 company profiles in various stages of the application and review process. We have completed 1, 480 validations, with an additional 2,304 validations underway or in the process of being completed.

Automated Commercial Environment (ACE) and the International Trade Data System (ITDS)
CBP has also worked vigorously to continue expansion of its Automated Commercial Environment (ACE), a multi-year modernization effort to reengineer critical business processes with the trade community and the information technology that supports them. This effort will greatly assist CBP in the advance collection of information for targeting high-risk cargo to better address terrorist threats and other high security concerns. And in doing so, it will help us expedite the vast majority of low-risk trade.

One important, fully integrated component of ACE is the International Trade Data System (ITDS). The ITDS initiative is an e-Government strategy being designed developed, and deployed jointly with ACE that will implement an integrated, government-wide system for the electronic collection, use, and dissemination of the international trade transaction data required by various trade-related federal agencies.

ITDS simplifies and streamlines the regulation, promotion, and analysis of international trade. It assists importers, exporters, carriers, and brokers in complying with federal trade, transportation, and other regulations by streamlining business processes. ITDS is customer focused and will serve as the government's 'single window' into international trade data collection and distribution.

In conjunction with ACE, ITDS will also improve risk assessment. By centralizing and integrating the collection and analysis of information, ACE will enhance CBP's ability to target cargo, persons, and conveyances. The trade data will allow for advanced inter-agency assessment of risks and threats to determine which goods and people must be scrutinized. In addition, through ACE, the ITDS will be capable of linking the government's law enforcement and other databases into one large-scale relational database that tracks all commerce crossing our borders. ITDS thus extends the functionality of ACE by bringing together critical security, public health, public safety, and environmental protection agencies under a common platform.

TRANSPORTATION SECURITY ADMINISTRATION

PortSTEP
Intermodal transportation systems converging at America's ports are highly interdependent and of great economic importance. Consequently, these networks have a high criticality rating and demand significant security attention. TSA and the Coast Guard have jointly developed and implemented the Port Security Training Exercises Program (PortSTEP), which contribute to meeting the mandates of the 2002 Maritime Transportation Security Act. PortSTEP is designed to provide maritime transportation security communities nationwide with training exercises, evaluations and accompanying information technology products to help strengthen the Nation's ability to prevent, respond to, and recover from a transportation security incident (TSI) in a port and maritime environment.

The first PortSTEP exercise occurred in San Francisco in August 2005. Seven more occurred during the balance of the year in Baltimore, Maryland; Anchorage, Alaska; Boston, Massachusetts; Puget Sound, Washington; Corpus Christi, Texas; Tampa, Florida; and Duluth, Minnesota. Valuable lessons have been learned and applied to improve intelligence information sharing, communications procedures, training programs and Area Maritime Security planning. Each PortSTEP exercise builds on the experience previously gained in a continual effort to deliver a top quality product and maximize its value in enhancing security of ports and intermodal systems. A total of 17 exercises are scheduled for 2006, building toward the objective of conducting 40 exercises in all. PortSTEP development will end in October 2007, culminating in a fully vetted and tested port and transportation security exercise pilot program that can serve as a model for TSA and other government agencies.

Delivered through the Area Maritime Security Committees (AMSCs), PortSTEP fosters and supports institutional relationships within the port environment including federal, state and local government partners, the surface transportation industry, intermodal transportation security managers, emergency managers, law enforcement, medical professionals, media, security personnel and all others involved in preparing for and responding to a TSI.

Secure Automated Inspection Lanes (SAIL) Program.

In coordination with the Coast Guard, TSA has implemented the SAIL test project to develop screening technologies and capabilities aimed at enhancing security on ferry systems. This multi-phased effort has tested and evaluated the use of explosives detection systems on two major ferry systems. TSA deployed a van portable Z backscatter X-ray system on the Cape May-Lewes Ferry, which carries vehicles and passengers between the southern tip of New Jersey and Delaware, and explosives detection document scanners on the high volume passenger-only commuter ferry in San Francisco Bay. Planning is under way to initiate a third phase, which will test a total screening program for both passengers and vehicles in a large commuter ferry operation.

Security Screening Research and Development.

TSA is managing a $3.69 million research and development grant program to test and evaluate explosive trace detection equipment for screening passengers, baggage and vehicles in the ferry and cruise line industries. A request for applications for grant awards for vehicle screening equipment will be published this spring. Grants for passenger and baggage screening equipment have already been awarded, and procurement of that equipment for testing by the Transportation Security Laboratory in Atlantic City is underway. After completion of a 30-day test period, deployment of equipment will commence for field tests across the maritime passenger industry.

Miami Synergy Project.

TSA operates the Miami synergy project, a joint baggage screening initiative targeting the intermodal junction of passengers changing between cruise ships and commercial air travel. In this program, baggage from Royal Caribbean Cruise Lines passengers is screened at the seaport by TSA personnel using portable machines and then transferred in-bond to American Airlines flights operating out of Miami International Airport. The program has significantly reduced congestion and stress on TSA screeners at the airport and received highly positive reviews from passengers. The Miami seaport baggage-screening program has averaged 1000 passengers and 1500 pieces of check-in luggage per 3 days of operation each week. To date, 112,842 passengers and 158,528 pieces of baggage have undergone security screening in this initiative.

Transportation Worker Identification Credential (TWIC)

The TWIC program was initiated by TSA in its earliest days to ensure that only properly cleared and authorized personnel could gain access to secure areas of the Nation's transportation system.

The goals of the TWIC program are to:

- Develop a common, secure biometric credential and standards that are interoperable across transportation modes and compatible with existing independent access control systems;
- Establish processes to verify the identity of each TWIC applicant, complete a security threat assessment on the identified applicant, and positively link the issued credential to that applicant; and

- Quickly revoke card holder privileges for individuals who are issued a TWIC but are subsequently determined to pose a threat after issuance of their credentials, and immediately remove lost, stolen, or compromised cards from the system.

TSA developed a plan to build the TWIC program in four phases: Phase I - Planning, Phase II - Technical Evaluation, Phase III - Prototype, and Phase IV - Implementation. TSA recently completed executing Phase III -- Prototype testing, in which the overall TWIC solution was evaluated against a full range of business processes, policies and requirements, including enrollment centers and enrollment, security threat assessments, verification of claimed identity, card personalization and production, card issuance and revocation.

Encompassed within the TWIC program are requirements established by the Maritime Transportation Security Act of 2002 (MTSA), Pub. L. No. 107-295, to prevent unaccompanied individuals from entering a secure area of a vessel or facility unless the individual holds a transportation security card. Additionally, the Act requires that all holders of Merchant Mariner Credentials obtain a TWIC. With MTSA as their guide, the Coast Guard and TSA have worked closely to develop the maritime component of TWIC and are currently preparing a joint Notice of Proposed Rulemaking (NPRM).

Full implementation of TWIC requires promulgation of a rule establishing standards for security threat assessments of workers with unescorted access to secure areas of maritime facilities and vessels, a biometric identification credential that reflects the results of a satisfactory assessment, access control procedures to prevent unauthorized entry into secure areas and redress for workers who are denied a TWIC. Issuance of the rule will also implement the fee authority enabling the program to be fully supported through user fees. TSA and the Coast Guard are utilizing the experience and information gained through Phase III-Prototype testing of the project, in which various access control systems were established, security threat assessments were conducted and biometric credentials were issued.. The Prototype testing phase was completed in the summer of 2005, paving the way for TSA and the Coast Guard to move ahead with the rule.

The initial rollout of TWIC in the maritime arena will impact port workers, merchant mariners and personnel in the trucking and rail modes who require unescorted access to port facilities and vessels.

In the NPRM, TSA and USCG will address statutory requirements that card production take place at a centralized, highly secure federally managed card production facility. Once produced, cards will be sent via express delivery services to the enrollment center where the applicant enrolled. The finished card will be issued at the enrollment center once the applicant has matched their biometric to the card. At that time the card will be activated and ready for use in the TWIC system.

The Coast Guard is working very closely with the TSA to assist in the implementation of this new credentialing program. The Coast Guard is supportive of this regulatory effort. We will do everything within our ability to assist TSA in the development of this rulemaking and ensure that the TWIC and Merchant Mariner Credentialing initiatives are complementary in order to minimize the burden on mariners in the future.

Maritime Cargo Container Security Initiatives.

TSA has provided dedicated support and has substantially contributed to the development of several programs to enhance security of maritime cargo containers.

- TSA is exploring programs to enhance cargo security across the maritime and intermodal transportation system.

- Through Operation Safe Commerce, originally a TSA initiative now led by the Department's Office of Domestic Preparedness, development projects aim to increase security throughout the foreign and domestic supply chain through the use of container seal devices and other technologies. The program is now completing Phase III and product testing.

- From February 28 to March 2, 2006, TSA will jointly host with DOD the biennial Security Seals Symposium. This event, a continuing program now in its seventh iteration, provides a forum for exchange of information and technology between government and the maritime industry. The Symposium will explore operational, procedural, and technical issues affecting security seals, tamper-indicating devices, and radio frequency identification (RFID) technology. Speakers and panel discussions will cover a broad range of subjects, including protection of cargo shipments into and within the United States, the role of security seals and associated products in meeting changing and challenging security requirements, international coordination to develop security seal requirements and standards to protect assets in transit and container monitoring and cargo transportation security and integration of technology.

Summary

Over the past several months and years, each of these efforts has begun to help us further the goals of the National Strategy for Maritime Security and will now be approached from the framework of that strategy and its supporting plans.

While the National Strategy for Maritime Security's primary focus is on securing the Nation's ports, waterways and coastal approaches, the funding provided for maritime security has enhanced our ability to increase awareness, outreach, prevention, response and recovery capabilities. The events of September 11, 2001, heavily influenced our focus on security, but natural disasters such as Hurricanes Katrina and Rita remind us of other vulnerabilities and threats to the Nation.

As stated in the NSMS, it is only through an integrated approach among all maritime partners—domestic and international, public and private—that the security of the maritime domain can successfully be improved. Such collaboration is fundamental to implementing this National Strategy and vital to protecting the interests of the United States.

Thank you for your time and we will be happy to answer any questions you may have.

TESTIMONY

before the

SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION U.S. HOUSE OF REPRESENTATIVES

by

William G. Boles
Security Manager

DIAMOND STATE PORT CORPORATION

PORT OF WILMINGTON, DELAWARE

January 24, 2006

Testimony of William Boles
January 24, 2006

Good morning to you Mr. Chairman, and to the members of this Committee. I want to thank you for the opportunity to present testimony today in reference the TWIC card experience at the Port of Wilmington, Delaware. My name is William Boles, and I am the Security Manager for the Diamond State Port Corporation. The Diamond State Port Corporation is owned by the State of Delaware and operates the Port of Wilmington, Delaware.

The Port of Wilmington, Delaware is a full-service deepwater port and marine terminal handling over 400 vessels per year with an annual import/export cargo tonnage of 5 million tons. Today, Delaware's terminal is the busiest on the Delaware River. In addition, over 185,000 trucks and 255,000 passenger vehicles pass through our main gate on a yearly basis. We are currently in our 'fruit season'. This begins in mid December and continues through mid May. The Port of Wilmington, Delaware is a major importer of Chilean fresh fruit in the United States. Our truck volumes during this 'season' can exceed 1,000 trucks and 1,200 passenger vehicles a day.

Early in 2002, the Port of Wilmington, Delaware volunteered with the Maritime Exchange for the Delaware River & Bay to partner with MARAD in a pilot project for the Transportation Worker Identification Credential card. Shortly afterwards, an East Coast TWIC Team met and worked with us in developing a process for this card, based on our individual needs. The Transportation Security Administration was assigned this project, and there was excellent cooperation and communication between the team and stakeholders.

Within a year, the Team Leader left the project and a whole new team emerged. The communication and cooperation also left with this original team, and the stakeholders were left to simply respond to decisions made by the Transportation Security Administration.

The Technology Evaluation phase of the TWIC card started on July 23, 2003 at the Port of Wilmington. We evaluated three (3) different technologies for access control during this phase of the project: the magnetic stripe, barcode and ICC chip (contact) were the three (3) technologies chosen.

- MAG-STRIPE – The magnetic stripe on the TWIC card was used in our primary access lane. Although this card had a limited level of security, it was quick, efficient and still works today.

- BARCODE – This technology was used in our truck entrance lane. It too had a limited level of security but also was quick and efficient. This technology continued to work until August 2005.

- ICC CHIP - This technology was used as a contact card. The TWIC card was physically inserted into a card reader at the pedestrian turnstile and was also used in the exit lane for trucks. In September 2003, the ICC Chip began to fail on a few TWIC cards, due to wear from the constant contact.

The integration teams chosen by the TSA for the technology evaluation phase of the TWIC card were exemplary. The communication and cooperation in implementing this phase of the TWIC card was smooth and uneventful. Any and all problems were quickly addressed and solved. Over 3,800 technology evaluation phase TWIC cards were issued at the Port of Wilmington, Delaware during this period.

The stakeholders were originally advised that the TWIC card pilot project was designed to flow from one technology phase to the next. This would have prevented the stakeholders from constantly changing access control cards every few months. One of our major concerns was having port tenants, customers and employees constantly switching from one access card to another and back again as each phase of the TWIC card project started and ended. My concern became a reality on May 30, 2004.

The technology evaluation phase officially ended October 20, 2003. However, in response to my concerns, the TSA arranged for continuing support for this card until the prototype phase began. On April 30, 2004 the Port of Wilmington, Delaware was notified that this continuing support would end on May 30, 2004 with no clear start date for the prototype phase. The Port of Wilmington then had to issue different identification cards to new employees, tenants and customers in addition to individuals who had to replace their TWIC card for whatever reason. This caused access control and administrative problems for the port and our customers.

On July 1, 2004 the Port of Wilmington, Delaware implemented its Facility Security Plan with the technology evaluation phase TWIC card as the basis of it's access control system, even though we were unable to issue any cards in that format.

On June 1, 2005 the Transportation Security Administration, through its integrator, 'Bearing Point', started enrolling individuals at the Port of Wilmington for the Prototype phase TWIC card. Interest in this card was minimal, because there were no readers in place to use these cards.

The Port of Wilmington along with its security integrator had been working with 'Bearing Point' for months attempting to obtain specific technical information in order to obtain the proper card readers to implement this card. It appeared that 'Bearing Point' was intentionally keeping this information for themselves since they did not provide it freely. It was only after several meetings with our security integrator, 'HID corporation' technicians, 'Honeywell' technicians and Mr. Greg Fisher of the TSA did we resolve the issue and obtain the proper readers. It was on June 30, 2006, the final day for the prototype phase of the TWIC card, when the prototype phase TWIC card readers were installed at our main gate access points.

Once the readers were in place, interest in this card increased and gradually port tenants, customers and employees enrolled. We had some difficulties with the card readers that were installed by 'Bearing Point's' integrators, but our security integrator resolved the issues and the Prototype phase TWIC card became the primary access card for the Port of Wilmington. We now have over 1,600 individuals enrolled for the prototype TWIC card. In addition to this, we have approximately 50 prototype TWIC cards working in our access control system that were created at either the Maritime Exchange for the Delaware River and Bay or Holt Terminal in Gloucester, New Jersey. We are also able to apply differing levels of access for individuals at our port, depending on their job descriptions.

The Port of Wilmington has completely committed itself to the TWIC card project. We have had our ups and downs in committing to this card, as have our tenants, customers and employees. But through it all, we now have an ID card that works. We can count on the fact that anyone with the TWIC card has been vetted with a Terrorist Watch List check. This phase of the TWIC card uses 'wireless' technology that quickly and efficiently allows access for authorized individuals with a card that is not likely to wear out in a short time period. With authorization, we have a single ID card that can be used in multiple TWIC participant locations or terminals. As far as I'm concerned, the TWIC card is a reality with two exceptions.

I believe the Transportation Security Administration missed out on two (2) opportunities to advance the success of this card during this prototype phase. Number one is the missed opportunity to enroll Canadian truck drivers. The Port of Wilmington, Delaware is serviced by over 700 Canadian truck drivers from some of the largest trucking companies in Canada. This naturally reduced the number of prototype TWIC cards at the Port of Wilmington, but also missed the opportunity of have this ID card recognized at the U.S. border with Canada. The second missed opportunity was not utilizing the biometric features of this card in a seaport setting. As learned from the ICC Chip failure during the technology evaluation phase, there was a missed opportunity to evaluate different fingerprint readers in a seaport setting to learn what readers would work best in this situation.

Finally, I would like to take this opportunity to appeal for continued support of the prototype phase TWIC card through the implementation date. We are currently in a 'sustainment phase' supported by the Transportation Security Administration until at least February 28, 2006. As I stated earlier, there was skepticism when this phase of the TWIC card started, due in part to the sudden termination of the technology evaluation phase. Our stakeholders are now accepting this 'new' TWIC card and appreciate the many features it presents. I know that Holt Terminals in Gloucester City, New Jersey is now talking with our security integrator to have this TWIC card not only serve as an access control card, but to also integrate it into their hiring system. Several tenants at the Port of Wilmington, Delaware are considering using this card to allow access to their facilities, however they fear that this program will quickly stop, just as before.

Statement of Dr. Scott Glenn, Institute of Marine and Coastal Sciences,
Rutgers, the State University of New Jersey
Before the Subcommittee on Coast Guard and Maritime Transportation
January 24, 2006

Compact High Frequency Radars for Increased Maritime Domain Awareness

Coordinated networks of Compact High Frequency Radars, deployed on shore and on buoys, are now a viable gap-filling technology that could be configured to increasingly support Coast Guard and other Homeland Security needs for Maritime Domain Awareness through improved wide-area vessel surveillance and simultaneous environmental data collection. Maritime Domain Awareness to support Port Security includes the need for wide area surveillance systems to identify the location of all vessels within a region of interest, and the ability to compare this field with the voluntary Automatic Identification System (AIS) reporting network to improve the targeting of specific vessels for inspection or intervention. Intervention activities require putting Coast Guard personnel to sea on vessels or aircraft. Maritime Domain Awareness includes knowledge of the environmental conditions within an operational area to minimize the safety risks to responding Coast Guard personnel. In the unfortunate event of an incident, real-time environmental data is required to cue response teams for Search And Rescue efforts and to minimize further environmental impacts.

Compact High Frequency (HF) radars are a widely accepted technology for environmental data collection, providing a unique current mapping capability and an inexpensive alternative for wave monitoring. Ongoing research at the Sandy Hook, New Jersey, HF Radar Testbed has demonstrated that Compact High Frequency (HF) Radars can simultaneously extend vessel detection and tracking capabilities over-the-horizon, well beyond the line-of-sight coverage of conventional Microwave Radars. This dual-use capability, combined with the lower cost and risk of a distributed network of compact HF radars, has prompted the formation of a collaborative government-academic-industry partnership to continue to refine and demonstrate new HF Radar technologies. The partnership's successes in the development and demonstration of a dual use technology that is now available to improve operations has attracted the attention of the international community, in particular the Norwegian military. Further investment in both the research partnership and the eventual operational agency could be directed to more rapidly transition Compact HF Radar technology into increasingly widespread use for Maritime Domain Awareness to improve Port Security.

Background

High Frequency (HF) Radars were first constructed during World War II in England in an attempt to detect approaching German aircraft. These early radars were designed to broadcast a radio signal in the HF band towards Europe, and then use a receiver antenna array 100's of meters long to acquire the backscattered signals from the intended targets. Unfortunately, the radars where "jammed" by a large signal from an unknown source that overpowered the expected hard target returns. In the middle 1950's, it was discovered that the jamming signals were not clever German counter-measures, but actually were HF radar signals that scattered off of surface waves in the North Sea. The process is known as Bragg Scattering.

Bragg Scattering occurs when the roughness elements causing the scattering are spaced at one-half of the wavelength of the transmitted radio signal. When this occurs, the backscattered signals from each roughness element are in phase and reinforce each other, producing what is known as a Bragg peak in the return signal. For HF radars, the typical broadcast frequencies range from 5 to 25 MHz in a portion of the spectrum located between the AM and FM radio bands. The wavelength of these broadcast signals ranges from 60 m to 12 m, with Bragg scattering occurring over ocean waves half as long. But ocean surface waves are not stationary. They propagate at well known speeds based on their wavelength. The backscattered Bragg peak associated with moving ocean waves experiences a Doppler shift. Just like the sound from a passing vehicle, surface waves moving towards the radar result in a slightly higher frequency Bragg peak, and surface waves moving away from the radar result in a slightly lower frequency Bragg peak. An additional Doppler shift occurs if the surface waves are also riding an ocean current. Again, the frequency of the Bragg peak is increased if the current has a component towards the radar, and is decreased if the current has a component away from the radar.

Recognition of this physical process in the 1970's prompted the additional development of HF radars as tools for mapping ocean currents. For current mapping applications, two or more radars distributed along the shore are required. Each radar measures the component of the current moving in the radial direction towards or away from itself. In regions where the radial current coverage from at least two radars overlaps at angles approaching 90 degrees, the total current vector can be estimated from its observed components. As in hard target tracking applications, the early radars required a long linear receiver array measured in 100's of meters. Just as all microwave radar receivers are many times longer than the few centimeter wavelength of the microwaves, the early HF radars all used linear phased arrays many times longer than the HF wavelength to aim the radars in a specific direction.

At this point it was recognized by NOAA scientist Dr. Donald Barrick that large phased arrays were impractical for widespread use. Because the decay of the HF groundwave is extremely rapid over dry land, HF radars need to be located within a few wavelengths of the salt water to take advantage of their over-the-horizon view. Because the biggest NOAA markets for current maps were expected around busy ports and population centers where beach and waterfront real estate was at a premium, it was expected there would be little tolerance for the installation of networks of large linear antenna arrays. To solve this problem, Dr. Barrick invented compact HF radars, and formed the company CODAR Ocean Sensors to develop and market the product, Using the direction finding properties of circular rather than linear arrays, CODAR HF Radar receivers can fit on a single post deployed near the water on a beach, dune, dock or cliff. Today, CODAR Ocean Sensors is the largest manufacturer of HF radars in the world.

In the 1990's, Rutgers University and CODAR Ocean Sensors formed an academic-industry partnership for the development of HF radar and its products through the support of the National Ocean Partnership Program. That partnership is now in its 9th year, focusing on the design, testing and rapid transition of the dual-use capabilities of compact HF radars. In this case, dual-use means both environmental products (currents and waves) and vessel tracking products. Today, the Rutgers University (R.U.) Coastal Ocean Observation Lab (COOL) operates the most advanced HF radar network in the world. The CODAR network is used to map ocean currents over the New Jersey continental shelf and the entrance to New York Harbor, to monitor waves and alongshore currents on the New Jersey coast, and to testbed new vessel tracking capabilities for homeland security, counter narco-terrorism, and naval applications.

Environmental Applications

For HF radars, the Doppler spectrum of the return signal produces a Bragg Scattering peak with a main center lobe and smaller secondary lobes on either side. The Doppler shift of the main center lobe is used to calculate ocean currents, and the smaller sidelobes are used to calculate surface wave parameters. The range and resolution of the radars is determined by its broadcast frequency, with lower frequencies producing longer ranges, and higher frequencies producing higher resolution.

Rutgers operates two CODAR HF radar current mapping networks in New Jersey. The 5 MHz long-range network provides current mapping coverage of the entire continental shelf offshore New Jersey. The 25 MHz high-resolution network provides high resolution nested coverage of the entrance to New York Harbor. Both networks were installed to support environmental research activities, attracting scientists from around the world. The environmental datasets are displayed on the R.U. COOL website (http://marine.rutgers.edu/cool) in real time for use by the general public. The nested high-resolution CODAR network is used by the NOAA fisheries groups based at Sandy Hook to improve their sampling, and by the New Jersey Department of Environmental Protection to observe the location of the Hudson River plume as it propagates along the coast. The long-range network is used by the U.S. Coast Guard for Search And Rescue and by the NOAA HazMat Response Team in response to potential oil spills. In a dedicated 1-month duration test of Rutgers long-range CODAR network and the Coast Guard's new SAROPS planning tool, use of the CODAR surface current maps over existing methodologies were found to significantly improve the efficiency of Search And Rescue activities. When CODAR surface currents where used as input, the SAROPS search areas were reduced in size, and the drifter targets deployed were more consistently found within the tool's projected search areas.

The Rutgers network is also being used to improve the distribution of surface wave observations along the New Jersey coast. Since surface waves depend on the smaller secondary sidelobes of the Bragg peaks, the observational range for waves is reduced compared to the range for currents. Nevertheless, CODAR HF Radars provide an important gap filling dataset for NOAA surf zone forecasts of rip currents. Rip currents depend on the nearshore wave and current environment, which are more highly variable as you approach the coast. Rutgers displays the nearshore waves and currents from its CODAR systems on the R.U. COOL website, and this data is then used by the NOAA National Weather Service regional office in Mount Holly to improve their rip current forecasts. Since HF radars are already distributed along the coast, Rutgers nearshore wave and current products can be used to reduce the number of wave buoys that must be deployed. The annual cost of maintaining an HF radar shore site is about one-tenth of the cost of maintaining an offshore buoy.

Vessel Tracking Applications

Two technologies presently are in general use for wide-area surveillance vessel tracking applications. Satellite radars provide global coverage but their updating frequency is limited by their revisit intervals, typically twice per day for polar orbiting satellites in low earth orbit. This limits their operational effectiveness to vessels that are still far out at sea. Microwave radars provide many rapid updates every second, but their range is limited by line-of-sight to the horizon. Vessels or low flying aircraft can hide from microwave radars by using the curvature of the earth to fly or sail under the radar. Microwave radars therefore provide excellent coverage nearshore. In contrast to microwaves, HF radio waves can travel long distances over the salty ocean as a groundwave, following the curvature of the earth where it can scatter off of targets that are over the horizon and otherwise hidden from view. HF radar with its intermediate over-the-horizon view and its intermediate updating intervals of several times per minute is the only gap filling technology that could provide coverage between the two existing microwave and satellite technologies. This potential is recognized by the Office of Naval Research, the DoD Counter NarcoTerrorism Program Office, the Department of Homeland Security and the U.S. Coast Guard. With funding provided and coordinated by ONR, CNTPO, and DHS, and in collaboration with the U.S. Coast Guard, the Rutgers-CODAR academic-industry partnership has developed an abandoned Nike missile site at Sandy Hook, New Jersey into the world's most extensive HF radar tesbed for vessel tracking. At Sandy Hook, Rutgers currently operates compact CODAR HF radars for vessel tracking at 5, 13, and 25 MHz.

Trade off studies indicate that a distributed network of many compact, inexpensive, low power HF radars is a less risky approach than the alternative approach of a smaller sparse network of larger, more expensive, high power HF radars. One of the issues in favor of the distributed network is countermeasures. A vessel can easily hide in the high energy Bragg peak associated with the surface waves simply by making its speed relative to the radar the same as the scattering ocean waves. This can be achieved for a known radar location using a simple hand-held multi-band radio tuned to the HF radar signal to determine its frequency, and a pocket calculator with a square-root function to calculate the desired vessel speed. About a $50 Radio Shack purchase is all that is required to defeat a multi-million dollar investment in a single radar. However, it is impossible for a ship to simultaneously hide in the Bragg peak of two radars with overlapping coverage.

Joint Rutgers University - CODAR Ocean Sensors partnership projects to develop the dual use vessel tracking and environmental capabilities of compact CODAR HF radars have been funded by ONR, CNTPO and DHS. ONR sponsored the initial tests to demonstrate the detection and tracking of large vessels with HF radar. CNTPO sponsored a similar series of test for small, fast vessels. One objective of both projects was to use the existing low powered compact CODAR systems to estimate the various terms in the Radar Equation that would enable it to be used to estimate performance for different transmit power and receiver directivities. One result of this study was the CNTPO funding of the development of a compact Superdirective antenna that has now been installed at the Sandy Hook testbed. The Superdirective concept applied here uses 9 antenna elements arranged in a circle on top of a pole to achieve the same directivity as a linear array 100s of meters long. Tests of the Superdirective concept at Sandy Hook are anticipated to lead to the development of a mobile Superdirective receiver that can be moved around the Caribbean for law enforcement purposes. DHS has funded the development of a transmitter buoy that will be multi-statically coupled to the CNTPO Superdirective antenna. Mono-static operation implies that the HF radar transmitter is in the same location as the receiver. Multi-static operation means that the receiver is gathering data from every transmitter in view, even if they are not co-located. The DHS concept is to place additional radar transmitters offshore on buoys that will extend the useful range further offshore and provide multiple looks at vessels over wide regions. The working concept is to implement a multi-static distributed network of many inexpensive compact radars for vessel tracking and environmental data collection.

Key Needs

Despite these successful demonstrations, obstacles still exist to the more widespread operational use of HF radar current and wave environmental products. Most U.S. HF Radar networks are operated by universities. Funding for operations and maintenance of the networks, including the extensive Rutgers CODAR network, presently depends on the research grant writing abilities of a few scientists. The Coast Guard cannot depend on the inevitable up and down cycles of research funding for an operational dataset. For the Coast Guard to adopt CODAR HF Radar as an operational input to SAROPS, dedicated operations and maintenance costs for the existing networks would have to be identified. In addition, capital costs for the acquisition of gap filling radars would be required to ensure that the data was available over the full area of interest. A second obstacle is the need to run the HF radar datasets through a NOAA Quality Assurance/Quality Control (QA/QC) program so that it receives the full liability protection of the U.S. government. Until this is done, many commercial groups such as shipping companies or harbor pilots will not use the data because of the potential for litigation. Many of the necessary QA/QC procedures already exist within the NOAA PORTS and NOAA NDBC systems, but require additional funding for NOAA personnel and HF radar operators like Rutgers to work together to implement the procedures on this new datastream.

The potential for collaboration between agencies is high. In 2003, Ocean.US founded the Surface Current Mapping Initiative Steering Committee to begin development of a plan for a National HF radar network as part of the U.S Integrated Ocean Observing System (IOOS). In 2005, Dr. Richard Spinrad, Assistant Administrator for NOAA contacted Admiral R. Dennis Sirois, Commandant of the Coast Guard proposing the two agencies work together to further the development of HF Radar as a national network. Two items key collaborative efforts would be the use of existing Coast Guard coastal properties as potential shore sites for HF radars, and collaboration in an effort to request the FCC to grant a primary license for HF radars in segments of the broadcast spectrum. Presently HF radar operators use secondary FCC broadcasts licenses on a not to interfere basis. This requires HF radar operators to search for open frequency bands with little noise, and occasionally move to different frequencies in response to others. A national operational network would require primary licenses to ensure its continuous availability.

A national HF radar network is likely to eventually be implemented based on the proven usefulness of the current mapping data alone. A plan for vessel tracking that leverages off this network is possible based on the research initiated at the Sandy Hook test bed. Superdirective antennas acting in multi-static mode can be deployed to listen in on the existing broadcast network for vessel tracking. Where necessary, the network can be augmented with additional transmitters deployed on shore or on buoys. Additional tasks to accelerate this transition are the continued refinement and testing of new shore and buoy based hardware at the Sandy Hook testbed, continued development and coupling of multiple vessel detection algorithms, and the implementation of tracking software that fits vessel tracks to the detection data then interfaces the tracks with the existing user interfaces of the Maritime Domain Awareness system environment. The Norwegian military has expressed interest in collaborating with the U.S. to further the operational integration of dual-use Compact HF Radars for Maritime Domain Awareness.

TESTIMONY

before the

SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION
U.S. HOUSE OF REPRESENTATIVES

by

LISA B. HIMBER
VICE PRESIDENT

MARITIME EXCHANGE FOR THE
DELAWARE RIVER AND BAY

January 24, 2006

Testimony of Lisa B. Himber
January 24, 2006

Good morning, Mr. Chairman and members of the Committee, and thank you for the opportunity to present testimony today. My name is Lisa Himber, and I am Vice President of the Maritime Exchange for the Delaware River and Bay. As you may be aware, the Maritime Exchange is a non-profit trade association representing the members of the commercial maritime industry in Southern New Jersey, Southeastern Pennsylvania, and Delaware. Our mission is to promote the safety, security, economic viability and environmental health of the Delaware River port complex. Included among our 300 members are those companies and individuals on the front lines of the international border of the port – such as port authorities and private terminal operators, tug and barge companies, labor organizations, vessel operators and steamship agents, just to name a few.

In addition, I serve as Vice-Chair of the National Maritime Security Advisory Committee (NMSAC), which as you undoubtedly know was established under the Maritime Transportation Security Act (MTSA) of 2002. I and my fellow NMSAC members are charged to provide advice to the Secretary of the Department of Homeland Security on matters such as national security strategy and policy, actions required to meet current and future security threats, international cooperation on security issues, and security concerns of the maritime transportation industry.

This morning I am going to address several topics related to maritime security and federal efforts to improve it: the National Strategy for Maritime Security (NSMS), the Transportation Worker Identification Credential (TWIC), the Port Security Grant program, and the importance of expanded information sharing between the private and public sectors to enhance maritime domain awareness.

National Strategy for Maritime Security

Let me start by saying that the commercial maritime industry strongly supports the core concept behind the National Strategy for Maritime Security: to align federal security programs into a comprehensive and cohesive national effort. Since 9/11, both the Congress and the Administration have made great strides in protecting our homeland. However, in the over four years since the 9/11 attacks, there has been very little in the way of collective tangible improvements in the maritime sector. Certainly individual port facilities and businesses have implemented significant improvements in infrastructure and standard operating procedures. And the federal government has launched myriad new programs designed to mitigate threat. Yet in many respects the only visible effect of these efforts is to make it more difficult and costly to process vessels arriving at U.S. ports and the crews and cargoes they carry. It is our hope the National Strategy for Maritime Security will bring some focus to the various individual initiatives.

The Strategy has three overarching goals: to preserve the freedom of the seas, to facilitate and defend commerce, and to protect the movement of desirable goods and people. Yet the specific objectives outlined in the plan speak only to the need to prevent attacks, protect maritime areas and infrastructures, minimize damage and expedite recovery. Many port business leaders have expressed a concern that the dual goals of threat mitigation and facilitation of trade are mutually exclusive; indeed, there are any number of instances when it can be demonstrated that compliance with new laws and regulations has led to increased direct costs of doing business as well as delays in vessel and crew processing. On the other hand, whether these efforts have prevented any security breaches is, at best, difficult to determine.

In addition, it is clear that many of the federal regulations promulgated under various laws or presidential directives are simply unenforceable. The U.S. Customs and Border Protection (CBP) requirement that information concerning all persons entering the U.S. be provided to the agency in electronic format not less than 24 hours prior to arrival is an excellent example. While members of the commercial cargo industry have radically altered their business processes to accommodate this requirement, the reality is the USCBP has neither a mechanism nor the resources to enforce this regulation as it relates to the multitude of pleasure craft that enter U.S. waterways from beyond international limits. Yet the small launch operators who ferry pilots and other personnel to ships outside the port districts are required to comply. The DHS should consider implementing programs which provide a means for one-time registration of regular visitors to U.S. seaports. While a program of this nature would undoubtedly take a great deal of work to establish, we believe that in the long run it will ultimately save time and resources for both federal inspectors and the private sector.

From an industry perspective, it would be extremely helpful if indeed the National Strategy could allow us to better identify risk rather than unilaterally imposing increasing requirements and/or restrictions on all people and goods moving through our nation's seaports.

That being said, the National Maritime Security Advisory Committee was not asked by DHS to review and/or comment on the Strategy document, nor is it likely that the NSMS will be placed on the Committee agenda.

However, Committee members have dedicated their time and expertise to addressing some of the individual components of the Strategy. Currently, for example, we are in the process of developing a network of Subject Matter Experts in the various industry sub-sectors upon whom DHS can call for advice and guidance. This effort will help DHS assure continuity of the Marine Transportation System in the aftermath of an incident, which is one of the strategic actions outlined in the National Strategy for Maritime Security.

The Committee is also addressing areas of concern regarding the Memorandum of Understanding between the Coast Guard and Customs as it relates to Asymmetric Migration – or procedures to be followed to address stowaways, deserters and absconders.

However, since its inaugural meeting in March of last year, the primary effort of the NMSAC was focused on developing recommendations for implementation of the Transportation Worker Identification Credential (TWIC).

Transportation Worker Identification Credential

Having been involved in the TWIC program even prior to the establishment of the Transportation Security Administration (TSA) and the August 2002 launch of the East Coast TWIC pilot project, my organization and its members are keenly interested in the successful deployment of this program. But TWIC is not only important to the Delaware River port community; the full NMSAC membership – which includes a diverse cross-section of maritime stakeholders – unanimously concluded that TWIC is among the most important components of the national maritime security effort. As a result members elected to make TWIC the number one priority on the NMSAC agenda. Last spring, the Committee presented DHS with a full set of recommendations for TWIC implementation.

Despite the many problems with TWIC over the last several years, we continue to support the idea of a standardized credential to be used at U.S. seaports. In the first phase of the TWIC program, the planning phase, TSA did absolutely everything right. They visited with a variety of operators at differing types of ports and were thus able to understand the full range of security needs. And they talked with the people who require access to multiple facilities – including pilots and other mariners, steamship operators, trucking companies, vendors and labor – and they met with other local federal, state and municipal agencies to better understand their needs and concerns. From that effort, TSA developed what we thought would be an effective plan to move the project forward. That was in May of 2003.

As the years passed with only the slowest of progress, particularly during the third and final "prototype" phase and its overabundance of problems last year, many became disheartened. Others abandoned the effort altogether.

The TWIC program staff has worked diligently with stakeholders in an effort to sustain what remains of the pilot program, but given the ongoing delays, we are concerned about their ability to continue to do so. Today, it can only be said that at the end of the day the project has taken far longer, cost substantially more, and includes significantly less functionality than it should have done. Unfortunately, we have no confidence that TSA will be able to meet even the current deployment timetable of implementation by October of 2006.

At this point in the process, we continue to believe in the concept, but are uncertain about its viability as currently envisioned. As an immediate suggestion, we believe TSA should develop a rule that involves the full participation of industry as partners in the process. The draft of the rule has already been completed – in the form of the NMSAC recommendations. We believe it is imperative that those who work in and around our nation's ports and who understand the environment must be involved in the decisions that are made with regard to the implementation of the TWIC program.

We also believe it is important to remind DHS that the TWIC was not developed for the benefit of the federal government. The original TWIC premise – as identified by the Credentialing Direct Action Group, which started this process four years ago, and which was embraced by industry – was to standardize a credential for *those people who need access to multiple facilities*. The goal of the TWIC was to eliminate the need for truck drivers and others to pay for multiple background checks and carry multiple credentials. It would also alleviate the need for individual port and other secure facilities to pay for the development and issuance of site-specific identification cards. These are the primary TWIC stakeholders, not the DHS.

Of particular concern now are some of the key questions surrounding the program, foremost among which is whether the federal government will manage the program or issue a standard. The MTSA, of course, requires that DHS issue this credential, and we believe that if TSA simply issues a standard, we may be back to where we were in October of 2001, with each port issuing its own cards. Other critical issues include those surrounding the background check requirements, waivers and appeals, whether an employer or sponsor would be required for a worker to obtain a TWIC, and how to include foreign seafarers and truck drivers in the program. The National Strategy for Maritime Security identifies a need for international cooperation, yet after three years of discussing the issue, the Transportation Security Administration program has not offered a solution to this last question.

NMSAC has not yet received a response from TSA to its recommendations; however we expect a briefing in the not too distant future. Our hope is that this will take place prior to publication of a proposed rulemaking, which we understand is scheduled for sometime during the first quarter of this year.

One of the reasons the Delaware River area was selected as a TWIC pilot program location was because of the work we had done prior to the events of 9/11 to develop a regional ID program for truck drivers calling multiple facilities in the tri-state region. After September 11, we quickly reprogrammed our efforts, then known as the Electronic Driver ID program, into a Delaware River ID program which would provide a standard identification to any individual requiring access to a secure facility in the region. During the first round of Port Security grants, we successfully applied for funds to expand our program. However in subsequent rounds, though the focus continues to be on projects with regional impact, the eligibility criteria have precluded regional associations from participating.

Port Security Grant Program

There are any number of opportunities for improvement which can best be made when both public and private sector port organizations work in tandem, particularly those associated with improved Maritime Domain Awareness. We have demonstrated on the Delaware River that by working together we can design programs that meet a variety of needs in both a cost-effective and timely manner. Unfortunately, though the Port Security Grant program purports to focus on enhanced regional cooperation, the grant process as it exists today does not lend itself well to regional initiatives. From the application itself, which requires the applicant to select one Congressional district, to the short time frame between announcement of eligibility criteria and application deadline – which is generally insufficient to bring interested parties together, discuss mutually agreeable project requirements, and if necessary, come to financial agreement on the required matching funds – it is difficult for communities to work together to implement regional initiatives under this program.

One example that comes to mind is the need to integrate the video surveillance images deployed by individual facilities into a common operating picture. This type of initiative would benefit local law enforcement agencies at all levels, and regional associations can both serve as project coordinators as well as the "neutral entities" to operate such systems. The administrative processes associated with the Port Security Grant Program should be modified to allow for these types of projects and applicants.

Expanded Information Sharing to Enhance Maritime Domain Awareness

The National Security for Maritime Strategy, the Port Security Grant Program, various Presidential Directives and other communications have all highlighted the need for enhanced information sharing as critical to both incident prevention and response. As a Maritime Exchange, our group and others like us throughout the U.S. have been concerned with effective information sharing for over 130 years. While originally Exchanges were formed to share ship movement, cargo, and crew information for commercial purposes, it is obvious that DHS and other law enforcement agencies require the same information for security purposes. We strongly support federal programs which capitalize on available information to meet a variety of missions. An example is the International Trade Data System, which is being designed to streamline reporting between the private sector and multiple federal agencies. Another is the recent effort between the Coast Guard and CBP to simplify electronic crew and passenger reporting via a single program which satisfies the requirements of both agencies.

Yet there are several other opportunities to improve awareness while at the same time reducing costs for both the private and public sectors. For example, the National Strategy for Maritime Security specifically cites the development and expansion of long and short-range vessel monitoring capabilities as a key requirement to achieve Maritime Domain Awareness. The Coast Guard and industry can and should work more closely together to implement a national real-time vessel tracking system. Though Coast Guard has identified the Automated Identification System (AIS) as a priority in its Maritime Domain Awareness program and promulgated regulations that require commercial cargo vessels to carry AIS equipment on board as of December of 2004, the agency simply does not have the infrastructure to receive and monitor the AIS images across the full extent of the U.S. maritime borders. Industry has demonstrated an ability to quickly implement this technology – as well as additional long-range tracking capability that goes beyond the limited visibility AIS provides. Maritime Exchanges, Pilot Associations, and ports/harbor masters have taken the lead on these types of initiatives, and the Coast Guard can undoubtedly benefit by partnering with industry in both the funding, development and operation of vessel monitoring programs.

In addition, Exchanges, pilots and others who are entrenched in the daily business operations of their ports are uniquely qualified to assist DHS in its efforts to obtain situational awareness and to help disseminate information to users at all levels. Although we do not necessarily have access to the various targeting databases, the reality is that, unlike our federal partners, most members in the private sector have lengthy institutional memories and can quickly and easily detect anomalies in port operations. Private organizations are also well-positioned to help Captains of the Port or CBP Port Directors to add local electronic message centers, distribution lists and other functionality to existing community information systems. This would complement the work Coast Guard has undertaken on its HomePort Program, while at the same time relieve local Coast Guard personnel from administrative tasks, thereby freeing resources for security, search and rescue, environmental protection and other critical missions.

Other examples include information sharing with regard to electronic data submitted to the federal government by ocean carriers, such as cargo manifests, advance notice of vessel arrival data, and vessel stow plan information. CBP and Coast Guard are already sharing crew/passenger information, Customs is providing cargo manifest data to port community information systems such as those operated by the Maritime Exchange, and many vessel operators are now voluntarily providing stow plan data – which they have historically shared with their port authorities and terminal operators – to CBP.

We believe there are any number of additional opportunities to share information that is useful both from security and commercial perspectives, and we look forward to continuing to work with Coast Guard and others to explore opportunities designed to meet the dual goals of improved homeland security and facilitation of commerce.

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