AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

DEPARTMENT OF HOMELAND SECURITY LAW ENFORCEMENT EFFORTS AT U.S. PORTS OF ENTRY

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

MARCH 15, 2005

Serial No. 109–38

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://www.house.gov/judiciary

U.S. GOVERNMENT PRINTING OFFICE

20–016 PDF WASHINGTON : 2005

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

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
BOB INGLIS, South Carolina
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL ISSA, California
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
ADAM SMITH, Washington
CHRIS VAN HOLLEN, Maryland

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

HOWARD COBLE, North Carolina, *Chairman*

DANIEL E. LUNGREN, California
MARK GREEN, Wisconsin
TOM FEENEY, Florida
STEVE CHABOT, Ohio
RIC KELLER, Florida
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
LOUIE GOHMERT, Texas

ROBERT C. SCOTT, Virginia
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ANTHONY D. WEINER, New York

JAY APPERSON, *Chief Counsel*
MICHAEL VOLKOV, *Deputy Chief Counsel*
ELIZABETH SOKUL, *Counsel*
KATY CROOKS, *Counsel*
JASON CERVENAK, *Full Committee Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

MARCH 15, 2005

OPENING STATEMENT

Page

The Honorable Howard Coble, a Representative in Congress from the State of North Carolina, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security 1

The Honorable Robert C. Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 3

WITNESSES

Mr. Jayson P. Ahern, Assistant Commissioner, U.S. Customs and Border Protection

Oral Testimony 6

Prepared Statement 7

Rear Admiral Larry Hereth, Director of Port Security, United States Coast Guard

Oral Testimony 12

Prepared Statement 14

Mr. Peter J. Scrobe, Vice President, American International Marine Agency, on behalf of the International Cargo Security Council

Oral Testimony 20

Prepared Statement 21

Mr. Jeff Keever, Deputy Executive Director, Virginia Port Authority

Oral Testimony 23

Prepared Statement 24

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Robert C. Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 47

Response to Questions for the Record submitted by Commissioner Jayson Ahern, U.S. Customs and Border Protection 48

Response to Questions for the Record submitted by Rear Admiral Larry Hereth, Director of Port Security, U.S. Coast Guard 58

Response to Questions for the Record submitted by Peter Scrobe, Member of International Cargo Security Council 70

Response to Questions for the Record submitted by Jeff Keever, Deputy Executive Director, Virginia Port Authority 72

Statement submitted by the Retail Industry Leaders Association (RILA) 79

DEPARTMENT OF HOMELAND SECURITY LAW ENFORCEMENT EFFORTS AT U.S. PORTS OF ENTRY

TUESDAY, MARCH 15, 2005

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 3:02 p.m., in Room 2141, Rayburn House Office Building, Hon. Howard Coble (Chair of the Subcommittee) presiding.

Mr. COBLE. Good afternoon, ladies and gentlemen. The Subcommittee will come to order.

Today, the Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, convenes a very important oversight hearing of the Department of Homeland Security to examine the security of the nation's seaports and the cargo entering these ports.

I have long contended that protecting our nation's seaports is a vital aspect of the overall war on terror. Press reports have indicated there's a lack of cargo inspections taking place at our ports of entry. This Subcommittee is concerned about these reports and looks forward to hearing the Department's response to these accounts and the plans to assure adequate inspections to protect our ports and the cargo entering the United States are taking place.

Today's hearing will focus on the efforts of three vital entities charged with protecting our nation's seaports from hostile threats. First, we will hear from the two primary agencies within the Department of Homeland Security charged with protecting our ports, that is the United States Coast Guard and the United States Customs and Border Protection.

The United States Coast Guard is the nation's leading maritime law enforcement agency and has broad multifaceted jurisdictional authority. As part of Operation Noble Eagle, the Coast Guard is at a heightened state of alert, protecting more than 361 ports and 95,000 miles of coastline, which is America's longest border. The Coast Guard utilizes both Maritime Safety and Security Teams as well as Port Security Units to protect our seaports.

Maritime Safety and Security Teams were created in direct response to the terrorist attacks on September 11, 2001, and are a part of the Department of Homeland Security's layered strategy directed at protecting our seaports and waterways. MSSTs provide

waterborne and a modest level of shoreside anti-terrorism force protection for strategic shipping, high-interest vessels, and critical infrastructure. MSSTs are a quick response force capable of rapid nationwide deployment via air, ground, or sea transportation in response to changing threat conditions and evolving maritime homeland security mission requirements.

The Coast Guard Port Security Units, the PSUs, are Coast Guard units staffed primarily with selected Reservists. They provide waterborne and limited land-based protection for shipping and critical port facilities, both within the continental United States and in other theaters.

We will also hear from Customs and Border Protection. The CBP anti-terrorism mission is not limited to the physical examination of cargo when it arrives in United States ports. The CBP, or the Customs and Border Protection, is also using intelligence from a number of sources to identify high-risk shipments in order to concentrate its inspection resources on them. For example, under bilateral agreements as part of the Container Security Initiative, CBP inspectors work in nearly 20 foreign ports to help ensure the security of U.S.-bound cargo before it disembarks.

Additionally, in November of 2001, the CBP established the National Targeting Center to serve as the national clearinghouse for targeting imported cargo for inspection. Among other tasks, the NTC interacts with law enforcement and the intelligence community to disseminate intelligence alerts to the ports. NTC, furthermore assists, in conducting research on incoming cargo, attempts to improve the targeting of cargo, and manages a National Targeting Training Program for CBP targeters.

Next, we will hear testimony from a local port authority, the Virginia Port Authority. The VPA has led the nation in radiological testing at its seaports and has successfully employed radiological monitoring equipment since December of 2002. In just this past year, in cooperation with Customs and Border Protection, VPA deployed some of its equipment to national security events, including the Presidential inauguration.

Finally, we will hear testimony from a representative from the International Cargo Security Council. The International Cargo Security Council is a professional association of cargo transportation and security professionals from the entire spectrum of cargo security. One of ICSC's goals is to improve cargo transportation security through voluntary Government/industry efforts.

In order to further this effort, ICSC is a leading proponent of encouraging industry to partake in CBP's Customs-Trade Partnership Against Terrorism. C-TPAT is a joint Government/business partnership where companies agree to improve the security in their supply chain in return for fast-lane border crossings and other important incentives. It is important to recognize that cargo and port security require the multi-layered approach in order to deter and detect all vulnerabilities and hostile cargo.

I am pleased that we have this representation here before us today and I look forward to their testimony, and I apologize to all of you. I normally don't give an opening statement this lengthy, but I think the subject matter at hand requires some detail.

And prior to introducing our distinguished witnesses, I am pleased to recognize the distinguished gentleman from Virginia, the Ranking Member of this Subcommittee, Mr. Bobby Scott.

Mr. SCOTT. Thank you, Mr. Chairman. I'm pleased to join you in this hearing on law enforcement efforts at our ports. The development of the Department of Homeland Security in the wake of the 9/11 tragedies brought about a shift of several law enforcement agencies from one Department to another with changes and reorganizations of their responsibilities in some cases.

There has been a significant change in responsibilities of the Federal law enforcement entities to communicate, coordinate, and cooperate with State and local law enforcement entities. As a result, some confusion exists in the public and Congress and among the various Federal and State agencies as to where the oversight responsibilities for these operations reside.

I am of the opinion that we should seek to clarify any such confusion by first asserting our jurisdiction over all Federal law enforcement entities and then working with those entities to insist their coordination and cooperation with each other and with State and local law enforcement entities.

So I'm pleased to join you in this first of a series of hearings that we'll be conducting in this regard and commend you for your foresight and leadership in this matter.

I'm particularly pleased to have Jeff Keever, the Deputy Director of our Virginia Port Authority, as one of our witnesses today. Our ports are a vital part of the nation's economy, handling over two billion tons of freight each year, and the Port of Virginia is the seventh-largest U.S. port in terms of general tonnage, handling annually—in terms of general tonnage handled annually and the second largest on the East Coast.

Operating alongside the nation's largest Naval base, assisting missions of the Defense Logistics Agency and the U.S. Transportation Command, security has always been a big job for the Port of Virginia. Secure, smooth, and efficient operations are not only critical to the deployment of our troops around the globe, but is also why the port has maintained a robust annual growth rate of more than 9 percent over the past few years.

As part of its focus on security, the Port of Virginia checks 100 percent of the containers leaving the port for radiation detection and monitoring equipment before they leave the port on trucks. And as a result of its successful cooperation with the U.S. Customs agencies, there has not been a theft at the port for about 8 years. That's quite a record in security when you consider that estimates of thefts from other ports across the U.S. range as high as $30 billion annually.

Yet despite the fact that our ports have risen to the challenges, their ability to continue to meet them in a world of changing threats and circumstances will depend in large measure on our assistance and support. I'm concerned, Mr. Chairman, that we have not been as diligent in supporting our seaports as we have with our airports and our other border crossings. It appears that we have left much of the responsibility to the ports themselves compared to what we have done to assist our airport and border crossing operations.

I expect that we'll hear about details of what we can do from our witnesses, so I look forward to their testimony and to working with you, Mr. Chairman, in clarifying our oversight responsibilities for the various law enforcement entities and strengthening our ports so that they can do their vital job in securing and sufficiently moving cargo and people. Again, I appreciate your leadership in this manner.

Mr. COBLE. I thank the gentleman from Virginia.

I ask unanimous consent that all Members of the Subcommittee be allowed to introduce their opening statements and be made a part of the record, and we're pleased to have the distinguished gentleman from Arizona, Mr. Flake, joining us, as well.

Gentlemen, it's the practice of the Subcommittee to swear in all witnesses appearing before it, so if you all would please stand and raise your right hands.

Do each of you solemnly swear that the testimony you are about to give this Subcommittee shall be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. AHERN. I do.

Admiral HERETH. I do.

Mr. SCROBE. I do.

Mr. KEEVER. I do.

Mr. COBLE. Let the record show that each of the witnesses has answered in the affirmative.

You may be seated, and I am now pleased to introduce our distinguished panel. We do, indeed, have four distinguished witnesses with us today.

Our first witness is Mr. Jayson P. Ahern, Assistant Commissioner at the Office of Field Operations of the U.S. Customs and Border Protection. As Assistant Commissioner, Mr. Ahern manages an operating budget of $2.2 billion and directs activities of more than 25,000 employees. Moreover, he oversees the programs and operations of 20 field operation offices, 317 ports of entry, and 14 pre-clearance stations in Canada and the Caribbean. Prior to this position, Mr. Ahern served as Director of Field Operations for the Southern California Customs Management Center. Mr. Ahern is a graduate of Northeastern University and has completed the intensive program at Harvard University.

Our second witness is Rear Admiral Larry Hereth. Rear Admiral Hereth is currently serving as the Director of Port Security in the Marine Safety, Security, and Environmental Protection Directorate at the United States Coast Guard Headquarters. As Director of Port Security, he oversees all aspects of the Coast Guard port security mission and has directed the development of the maritime security regulations. Previously, he served as Commanding Officer of the Coast Guard Marine Safety Office in San Francisco Bay, as well as commanded a unit in Turkey. He is also a recipient of the Department of Transportation Security's Gold Medal Award. Rear Admiral Hereth is a graduate of the United States Coast Guard Academy and earned his M.B.A. from the Florida Institute of Technology.

Mr. Peter Scrobe is our third witness, who is a member of the International Cargo Security Council and former Chairman of Government Affairs Committee at ICSC. Mr. Scrobe has been in the

marine insurance industry for 30 years. He is currently an Advisory Board Member of the U.S. Merchant Marine Academy and Vice President of the American International Marine Agency Loss Control Services Worldwide. Additionally, Mr. Scrobe is an active consultant to the Department of Homeland Security through the Homeland Security Institute. Previously, Mr. Scrobe has worked to develop the marine loss control operations for American International Marine Agency. Mr. Scrobe received his undergraduate degree at the Herbert H. Lehman College.

I'm going to confess my geographic ignorance, Mr. Scrobe. Where is that?

Mr. SCROBE. In New York.

Mr. COBLE. It's in New York. And Admiral, if I may ask, I didn't know we had an installation in Turkey. Was that——

Admiral HERETH. It was a long time ago.

Mr. COBLE. It's good to know I'm up to speed now, and I'm now pleased to recognize Mr. Bobby Scott, who has requested permission to introduce our fourth distinguished witness.

Mr. SCOTT. Well, thank you, Mr. Chairman.

Jeff Keever has served at the Port of Hampton Roads since 1977, when he joined the staff at the Hampton Roads Maritime Association and the Hampton Roads Shipping Association. After a brief absence, he returned to those associations and was named Executive Vice President of the Hampton Roads Maritime Association and the Hampton Roads Shipping Association. In November of last year, he joined the Virginia Port Authority as Deputy Executive Director, the agency's number two position. He frequently represents the VPA's interests in the Virginia General Assembly as well as the port's customer base around the world.

He is a former President of the Hampton Roads Foreign Commerce Club, the Hampton Roads Traffic Club, and the Propeller Club. He is past Chairman of the Virginia Conference on World Trade. He serves as a member of the Board of Directors of the Virginians for Better Transportation, Virginia District Export Council, and served on the board of the Virginia Chamber of Commerce.

He was honored in 2001 by the Hampton Roads Maritime Association when he received the prestigious Distinguished Service Award, and he also received the Society of Maritime Industry's Distinguished Service Award in February 2004.

He received his B.A. in political science at the University of Richmond and has two children, a daughter and a son, who attend Norfolk Academy.

Mr. COBLE. I thank you, Mr. Scott.

Gentlemen, it's good to have you all with us. Now, I am advised that we will have a House floor vote in approximately 1 hour. We try to operate here, gentlemen, under the 5-minute rule. We impose that rule against ourselves, as well, and so when we question you all, if you could be terse in your response, that will help speed things along.

When you see the amber light illuminate in your face, you will know that you're running out of time. That will be about—I'll give you about a minute to go from that. So if you could, confine your statements to the 5 minutes. We have your written statements. They've been examined. They will be reexamined.

Mr. Ahern, we will start with you.

TESTIMONY OF JAYSON P. AHERN, ASSISTANT COMMISSIONER, U.S. CUSTOMS AND BORDER PROTECTION

Mr. AHERN. Good afternoon, Mr. Chairman, Congressman Scott. Thank you very much for the opportunity to testify and update you on the advancements the U.S. Customs and Border Protection continues to make in the areas of targeting and inspecting cargo.

Automation, electronic information, and technology are critical tools to facilitate the progress we have and will continue to make with regards to securing the nation's seaports. These tools help push our borders outward and reinforce the components of CBP's layered defense.

CBP continues to develop its layered risk management approach to safeguarding U.S. borders from threat by land, air, and sea. Automated manifest information allows us to screen shipments through our targeting systems and 100 percent of identified high-risk shipments are inspected. CBP's multi-layered strategy incorporates legislative and regulatory initiatives, international and trade organizational priorities and partnerships, improved automation support, new detection technologies, and enhanced personnel training, and a combination of local and national targeting expertise.

CBP recognizes that no single strategy is 100 percent effective, so the focus is on layering multiple initiatives and partnerships together to accomplish its mission. Although these layers are closely interwoven and no one layer is more important than the others, I would like to focus on those most closely associated with the targeting and inspection of sea cargo. An adversary may circumvent any single defense, so CBP does not rely on one enforcement strategy, facilitation program, or inspection process or technology. We employ these layers in combination to substantially increase the likelihood of a nuclear or radiologic weapon and a weapon-grade material will be detected.

CBP is committed to collecting the most reliable data possible. We demonstrate this commitment by working hard on new legislation and regulations and establishing a proactive manifest compliance program. The Trade Act requires manifest data to be transmitted to CBP before the arrival of shipments to facilitate the advance targeting so necessary. In the sea cargo environment, manifest data is required 24 hours prior to lading on a vessel overseas. The scope and the reliability of this data is reinforced by the publication of the Trade Act final rule on December 5 of 2003 that mandates the trade to provide advance electronic cargo information for all modes of transportation.

The Automated Targeting System, known as ATS, is a flexible, constantly evolving system that integrates enforcement and commercial databases. It is a targeting tool that helps CBP focus its inspectional efforts on the high-risk cargo. 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 then divided into thresholds associated with further action that CBP must take relative to documentation review, use of technology, or physical inspection.

The National Targeting Center, the NTC, has made significant progress since it began around-the-clock operations on November 10 of 2001 and began the task of reorienting our narcotics-based targeting methodologies and technologies for anti-terrorism and national security missions. By January of 2003, NTC staff relocated to a state-of-the-art facility in Northern Virginia that accommodates representatives from all of CBP. We broadened the scope of CBP targeting and NTC now has on-site liaison officers from the United States Coast Guard, the Transportation Security Administration, Immigration and Customs Enforcement, the Federal Air Marshals, the Department of Agriculture, and the NTC has also provided targeting expertise to the Department of Homeland Security Operations Center, the Terrorist Screening Center, and the National Counterterrorism Center to support the timely and accurate flow of information pertaining to national security and terrorist activity.

The Customs-Trade Partnership Against Terrorism, known as C-TPAT, also came into being as a result of the tragic events of September 11. CBP began to work with the trade to devise a strategy to protect the global trading network or supply chain against the exploitation by terrorists from loading docks in foreign environments to the ultimate destinations here in the United States.

Participation in C-TPAT has grown exponentially, and today, membership stands at 8,816 members, 4,600 of those that are certified members. Currently, we have enrollment from the importing community, carrier community, broker and freight forwarders community, consolidators, marine port authorities, and terminal operators.

The Container Security Initiative is an effort by CBP to secure ocean-borne traffic by placing CBP officers alongside host country customs officers to ensure that all shipments that pose a risk are identified in inspection at foreign ports of lading. Currently, CSI is in 34 ports in Canada, Europe, Asia, and Africa.

Non-intrusive inspection technology is another cornerstone of our layered strategy, and technologies deployed in our air and seaports include large-scale gamma imaging devices and also radiation detection capabilities, and I'll speak more of that when we get into the question and answer period.

In conclusion, CBP's targeting and inspection programs depend upon one another to operate at full potential. We're constantly looking at ways to improve and make them stronger. CBP works very aggressively with the trade and other Government partners to legislate improvements regarding data timeliness and quality, which augments the abilities of highly-trained personnel to use cutting-edge technology for targeting, detecting and securing terrorists and implements of terrorism destined for the United States.

Thank you very much, Mr. Chairman. I would be happy to answer your questions later.

Mr. COBLE. Thank you, Mr. Ahern.

[The prepared statement of Mr. Ahern follows:]

PREPARED STATEMENT OF JAYSON P. AHERN

Good afternoon Chairman Coble, members of the Subcommittee. Thank you for this opportunity to testify and update you on the advancements U.S. Customs and

Border Protection (CBP) continues to make in the areas of targeting and inspecting cargo.

Automation, electronic information and technology are critical tools that facilitate the progress we have, and will continue to make, with regards to securing the nation's seaports and the cargo that traverses them. These tools help CBP push our borders outward and reinforce the components of CBP's layered defense.

DHS continues to develop its layered, risk management strategy for safeguarding U.S. borders from threat by land, air and sea. CBP's multi-layered responsibilities under this strategy incorporate legislative and regulatory initiatives, international and trade-organization partnerships, improved automation support, new detection technologies, enhanced personnel training, and a combination of local and national targeting expertise. DHS recognizes that no single solution is 100% effective, so the focus is on layering multiple initiatives and partnerships together to accomplish its mission. Today I would like to focus on CBP activities associated with the targeting and inspection of sea cargo.

- National Strategy for Maritime Security—Policy directive to integrate and align all U.S. Government maritime security programs.
- Trade Act—Legislation that requires advance, detailed, and accurate information for targeting shipments before arrival to the United States.
- Advanced Trade Data Initiative (ATDI)—CBP effort to gather and analyze specific information already available from commercial supply chain participants.
- Smart Box Initiative—Test and Evaluation effort to assess commercially available container security devices.
- Non-Intrusive Inspection Technology—Advanced inspection equipment to screen shipments rapidly for WMD, nuclear or radiological materials, terrorist weapons, and other contraband.
- The Customs-Trade Partnership Against Terrorism (C-TPAT)—A public-private partnership program for securing global supply chains.
- The Automated Targeting System (ATS)—The premier tool employed by CBP personnel to identify high-risk targets in the cargo environments; targeting rule sets are in production for sea, truck, and rail cargo. CBP anticipates deployment of ATS Air Cargo Targeting during the second quarter of the 2005 calendar year.
- The Container Security Initiative (CSI)—Cooperative arrangements with trading partners to push our borders outward by inspecting high risk containers prior to loading, and;
- The National Targeting Center (NTC)—A single location for targeting technology and subject matter expertise.

An adversary may circumvent any single defense, so CBP does not rely on any one enforcement method, facilitation program, inspection process, or technology. CBP employs these "layers" in combination to substantially increase the likelihood that potential terrorist threats, including a nuclear or radiological weapon or weapons grade material, will be detected.

TRADE ACT

CBP is committed to collecting the most reliable data possible. We demonstrate this commitment by establishing a proactive manifest compliance program. The Trade Act requires manifest data to be transmitted to CBP before the arrival of certain shipments to facilitate advance targeting. In the sea cargo environment, manifest data is required 24 hours prior to lading on the vessel overseas. The 24 Hour Manifest Rule, along with proactive monitoring of the manifest data by CBP, is improving the timeliness and quality of the data which, in turn, increases CBP's early detection capabilities. This improvement is key to CBP's targeting success in the sea environment at both domestic and foreign locations.

The scope and reliability of this data is reinforced by the publication of the Trade Act Final Rule on December 5, 2003, that mandates the trade to provide advance electronic cargo information for all modes.

Additionally, when entry information is provided later in the supply chain, ATS is able to factor this information into the risk assessment. Entry data supplements manifest data, and is some of the most detailed and accurate information available for targeting.

CBP continues enhancing its data quality by testing additional data sources such as booking and stow plan data through our ATDI. We are also collaborating with

our Trade Support Network to identify additional data sources that can be effectively and efficiently integrated into our targeting and research process.

ADVANCED TRADE DATA INITIATIVE (ATDI)

The goal of the ATDI is to gather and analyze specific information already available from commercial supply chain participants in advance of, and in addition to, the 24-Hour Rule and entry data currently collected.

The ATDI has four ultimate goals:

- Identify the true port of origin and all stops along a shipment's transit to the United States
- Identify all parties associated with the shipment
- Determine the veracity of commodity descriptions
- Improve CBP risk management and targeting

Recently we completed Phase I of the ATDI, which demonstrated the ability to capture, analyze, and evaluate advance trade data provided by consenting U.S. importers via an ocean carrier portal (i.e., ocean carrier data contained in bills of lading, booking confirmations, and shipment status messages). In Phase II, which runs through April 2005, we plan to add additional data sources.

SMART BOX INITIATIVE

In January of 2004, CBP began Phase 1 of the CBP Smart Box Initiative. This initiative, which is one of a number of DHS Research, Development, Testing and Evaluation programs for container security,[1] involves five C-TPAT partners both large and small. These partners have agreed to incorporate enhanced container security measures to evaluate the efficacy of off-the-shelf technologies with an added electronic Container Security Device as well as an International Standards Organization compliant mechanical seal affixed to each container.

Securing containers is essential in achieving DHS's vision of a comprehensive supply chain security program. A terrorist must not be able to open a container in transit to introduce a weapon of mass destruction or other threat without DHS being aware of the attempt.

Results of Phase 1 will further allow CBP to define design and performance standards for the operational use of such technology, an effort we will undertake cooperatively with the Science and Technology Directorate's Container Security Program, including the Advanced Container Security Device (ACSD) program. The Department's goal in the Smart Box Initiative and the ACSD effort is to identify viable and cost effective container security devices that detect tampering and alert government and the trade when tampering does occur so we can initiate appropriate response mechanisms to determine whether a potential threat may have been introduced.

NON-INTRUSIVE INSPECTION AND RADIATION DETECTION TECHNOLOGIES

Non-Intrusive Inspection Technology (NII) is another cornerstone in our layered strategy. Technologies deployed to our nation's sea, air, and land border Ports of Entry that focus on radiation technology include large-scale X-ray and gamma-imaging systems, as well as a variety of portable and hand-held technologies.

NII technologies are viewed as force multipliers that enable us to screen or examine a larger portion of the stream of commercial traffic while facilitating the flow of legitimate trade, cargo, and passengers.

As of February 2005, 164 large-scale NII systems have been deployed to Ports of Entry. These include Vehicle and Cargo Inspection Systems (VACIS), Mobile VACIS, Rail VACIS, Truck X-ray, Mobile Truck X-ray, Mobile Sea Container Systems, and Pallet Gamma-ray Systems.

As noted above, CBP is also deploying nuclear and radiological detection equipment, including Personal Radiation Detectors (PRD's), Radiation Portal Monitors (RPM's) and Radiation-Isotope Identifiers (RIID's).

- CBP has deployed 441 RPMs nationwide. 54 are deployed to International Mail and Express Consignment Courier Facilities, 215 are deployed to Northern border land crossings, 54 are deployed to seaports, and 118 are deployed to the Southwest border.

[1] Other efforts include the Advanced Container Security Device program in the Science and Technology Directorate and Operation Safe Commerce in the Office of State and Local Government Coordination and Preparedness.

- Additionally, CBP has deployed 10,534 PRDs and 418 RIIDs nation-wide. Used in combination with our layered enforcement strategy, these tools provide CBP with a significant capacity to detect nuclear or radiological materials. Equally as important, NII technology has been instrumental in increasing the number of containers that are inspected by CBP.

CBP is actively engaged in the establishment of the Domestic Nuclear Detection Office, a jointly-staffed, national office established to develop a global nuclear detection system and acquire and support the deployment of the domestic portion of that system to detect and report attempts to import or transport a nuclear device or fissile or radiological material intended for illicit use. This office will integrate the research, development testing and evaluation of next-generation detection capabilities with the acquisition and deployment of these technologies to the field to ensure the most advanced capabilities are being used to protect our borders.

CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT)

The Customs-Trade Partnership Against Terrorism (C-TPAT) also came into being as a result of events of September 11th. CBP began to work with the trade to protect the global trading network or supply chain voluntarily and cooperatively. It was built upon the successful experience of U.S. Customs in promoting industry partnerships to improve security and deter narcotics smuggling.

The program began in November 2001, working with industry to develop reasonable guidelines that reflected the consensus (at that time) of what good security practices entailed. C-TPAT has provided a forum for the business community and CBP to exchange anti-terrorism ideas, concepts, and information to further secure the entire supply chain. This has been a learning experience for both industry and government.

Participation in C-TPAT has grown exponentially. In the first year C-TPAT enrolled 1000 members. As of March 10, 2005, C-TPAT membership stands at over 8,800 members, with 4,775 of those being certified partners (approved security profile and vetted by CBP) and 455 having been validated (physical verification by CBP Officers of security measures and practices in place) by CBP. Another 493 validations are underway. Current C-TPAT enrollment sectors include importers, carriers, brokers/freight forwarders/consolidators, marine port authorities and terminal operators, and Mexican foreign manufacturers

CBP seeks to ensure that its partners are honoring their commitments through a validation process. CBP cannot afford to offer the expedited commercial processing benefits that are part of C-TPAT for partners who are not holding up their end of the bargain. As a result, we are now sending specially trained CBP teams of C-TPAT Supply Chain Specialists all over the globe to visit the partners, their vendors, and their plants to verify that these steps have been taken.

C-TPAT is now moving to the next level and will be transitioning from its current set of recommended practices to minimum requirements that participants must meet for membership. As part of this program, CBP will further leverage the role of the importer to extend these supply chain security requirements throughout their supply chains. Specific enhancements to the security of the container, various facility and access controls, and requirements that business partners of importers adhere to similar requirements are also proposed. Through the natural evolution of the program, C-TPAT will be significantly strengthened, and, when combined with other security layers, will greatly enhance the confidence we have in the security of the oversees component of C-TPAT supply chains.

ATS

The Automated Targeting System (ATS) is a flexible, constantly evolving system that integrates enforcement and commercial databases. It is a targeting tool that helps CBP focus its inspection efforts on high-risk cargo. 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.

CBP works constantly to enhance and refine the ATS. The data that feeds the ATS is substantial, and the scope and reliability of this data is reinforced by the Trade Act Final Rule that mandates advance electronic cargo data inbound and outbound for all modes of transportation.

Although advance manifest data is a major component of what is analyzed, ATS also sorts through intelligence and data contained in Government law enforcement and trade databases. ATS is also able to access and analyze entry data when it is available. Entry data is some of the most detailed and accurate information avail-

able for targeting. CBP will continue to look for ways to improve the quality of the data that feeds the ATS; however, it should be noted that the ATS can detect anomalies in both accurate and false data. Such anomalies are strong indicators of deception.

Although constantly evolving, ATS is a proven targeting tool. Using advance manifest data, CBP has made several seizures overseas under the CSI initiative that included gas masks, tank periscopes and firearms.

CONTAINER SECURITY INITIATIVE (CSI)

The Container Security Initiative (CSI) came into being as a direct result of the events of 9-11. CSI is another layer in CBP's defense, the purpose of which is to push our nation's borders outward. 34 CSI ports are currently operational. These 34 operational ports are made up of ports from the original 20 largest ports, shipping the greatest volume of containers to the United States, and expansion ports added after the initial 20 ports were identified. These original 20 ports are points of passage for approximately two-thirds of the containers shipped to the U.S.

CSI fosters greater security via:

- Enhanced targeting through foreign government and trade partnerships and better data;
- Potential Department of Energy (DOE) involvement in radiation detection at overseas ports, and;
- Interdiction of threats before they reach the U.S.;

CSI also uses both automation and advanced inspection technology as force multipliers. For example, CSI has requisitioned Personal Radiation Devices (PRD's) to be deployed as CSI locations become operational. Additionally, CSI has requisitioned Radio-Isotope Identifier Devices (RIID's) for deployment to operational CSI ports with host country approval.

NATIONAL TARGETING CENTER (NTC)

The National Targeting Center (NTC) has made significant progress since it began round the clock operations on November 10, 2001 and began the task of reorienting narcotics based targeting methods and technologies for anti-terrorist and national security concerns. By January of 2003, NTC staff relocated to a state of the art facility in Northern Virginia that accommodates representatives from all CBP legacy disciplines, agriculture, customs, and immigration, as well as personnel from the Office of Border Patrol, the Office of Intelligence, and the Office of Information Technology.

Broadening the scope of CBP targeting, NTC has developed on-site liaison officers from the U.S. Coast Guard, the Transportation Security Administration, Immigration and Customs Enforcement, Federal Air Marshals, Federal Bureau of Investigation, Food and Drug Administration, and the U.S. Department of Agriculture. The NTC has also provided targeting expertise to the Department of Homeland Security Operations Center, the Terrorism Screening Center, and the National Counter-Terrorism Center to support the timely and accurate flow of information pertaining to national security and terrorist activity.

CONCLUSION

CBP's targeting and inspection programs depend on each other to operate at full potential, and we are constantly looking for ways to make them stronger. CBP works aggressively with trade and government partners to legislate improvements regarding data timeliness and quality, which augments the abilities of highly trained personnel to using cutting edge technology for targeting, detecting and securing terrorists, or implements of terrorism destined to the U.S. Thank you again, Chairman Coble, and the members of the Subcommittee for this opportunity to testify. I would be happy to answer any questions you may have.

Mr. COBLE. Gentlemen, I gave you all some faulty information. Our amber light is not working, and I'm told the amber light is now working. Okay. Admiral, we'll put you on notice. You won't be keelhauled if you violate, but that'll at least let you know the ice is getting thin on which you're skating.

Admiral HERETH. Yes, sir, I understand.

Mr. COBLE. It's good to have you, Admiral.

TESTIMONY OF REAR ADMIRAL LARRY HERETH, DIRECTOR OF PORT SECURITY, UNITED STATES COAST GUARD

Admiral HERETH. Good afternoon, Mr. Chairman, Mr. Scott. I look forward to discussing the Coast Guard's role to secure our ports and cargo chain today.

The marine transportation system, as you know, is a key asset that annually handles about 50,000 port calls from vessels, over 8,000 foreign vessels. This system contributes greatly to the U.S. gross domestic product, with nearly $750 billion worth of goods moving across our docks annually. A variety of reports have underscored the value of the marine transportation system to our economy and quality of life in the United States. The consequences of an attack shutting down our ports would be significant, so clearly, this is a system we must protect.

This, however, is a big challenge. Our underlying assumption has been that since trade is global and terrorism is global, we need a global solution to the problem. Our intention is to identify and intercept threats beginning as far from our shores as possible with additional protective measures added as vessels get closer to our homeland. Therefore, it's imperative that our efforts involve both domestic and international security regimes.

We have made excellent progress, both domestically and internationally, so far, but realize that there is much more to do. Internationally, we built a coalition of 148 countries under the auspices of the International Maritime Organization that have all adopted and implemented a security regime similar to MTSA in record time. This multilateral approach gives us more consistency among our trading partners and ensures that security must become a standard practice or a vessel operator will be faced with serious and costly delays.

To complement these new security standards, we worked in parallel with the International Standards Organization to develop an implementation guide to eight companies as they put into practice this major change. I am pleased to report an excellent initial success. Presently, only one out of 100 vessels that we board and inspect require us to take major port State control actions.

Cargo security is one of the principal components of maritime security. Customs and Border Protection has had a lead role in cargo security and the Coast Guard works to align our respective agency roles and responsibilities regarding international trade.

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

The Coast Guard has worked hard to coordinate all our regulatory and policy developments with CBP. We meet regularly to discuss policy. We participate in interagency regulation develop-

ment teams and sit on various other interagency committees. We also coordinate the work of our various Federal advisory committees so that we all understand the trade community's concerns and priorities.

The Coast Guard has fully supported CBP's initiatives. We also agree with CBP's view that international compliance and the establishment of international standards are needed to help gain global compliance and applaud their leadership to engage the World Customs Organization and the International Standards Organizations to leverage their efforts.

We thank you for the opportunity to testify and answer questions today. I'd be happy to engage in a discussion at the appropriate time, sir.

Mr. COBLE. Admiral, you set a record. Rarely do people beat the red bell. You walk off with the gold medal. [Laughter.]

[The prepared statement of Admiral Hereth follows:]

PREPARED STATEMENT OF REAR ADMIRAL LARRY HERETH

DEPARTMENT OF HOMELAND SECURITY
U. S. COAST GUARD
STATEMENT OF
REAR ADMIRAL LARRY HERETH
ON
CARGO AND PORT SECURITY
BEFORE THE
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
COMMITTEE ON JUDICIARY
U. S. HOUSE OF REPRESENTATIVES
MARCH 15, 2005

Introduction

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

On 9/10/01, our primary maritime focus was on the safe and efficient use of America's waterways. Since 9/11, we have made great progress in securing America's waterways, while continuing to facilitate the safe and efficient flow of commerce. There is no doubt that work remains, but there is also no doubt that we continue to improve maritime homeland security each and every day – thanks in large part to the continued strong interagency cooperation of those before you today.

Reducing Maritime Risk

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

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

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

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

Since 9/11 the Department of Homeland Security (DHS) and the Coast Guard have made significant strides to secure our homeland. Much has been done, and much remains to do. However, lingering and new maritime safety and security gaps continually present themselves and it is these risks we will continually work to reduce.

The Coast Guard guides its efforts by implementing policies, seeking resources, and deploying capabilities through the lens of our maritime security strategy.

Implement the Maritime Strategy for Homeland Security

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

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

Enhance Maritime Domain Awareness (MDA).

First, we seek to increase our awareness and knowledge of what is happening in the maritime arena, not just here in American waters, but globally. We need to know which vessels are in operation, the names of the crews and passengers, and the ship's cargo, especially those inbound for U.S. ports. Maritime Domain Awareness (MDA) is critical to separate the law-abiding sailor from the anomalous threat.

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

Create and Oversee Maritime Security Regime.

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

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

- Reviewed and approved over 9,600 domestic vessel security plans and 3,100 domestic facility security plans,
- Overseen the development of 43 Area Maritime Security Plans and Committees,
- Verified security plan implementation on 8,100 foreign vessels,
- Completed all domestic port security assessments for the 55 militarily and economically strategic ports, and
- Visited 19 foreign countries to assess the effectiveness of anti-terrorism measures and implementation of ISPS code requirements. An additional 10 countries are scheduled for visits by June 2005 with the goal of visiting all of our approximately 140 maritime trading partners; and
- Oversaw the development to the National and 43 Area Maritime Security plans.

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

- *Physical Security.* The first pillar of this framework is physical security. Through the implementation of the MTSA, we have significantly hardened the physical security of our ports. Roughly 3,100 of the nation's highest risk port facilities have implemented mandatory access control measures to ensure that only authorized persons are able to

gain access. They have established designated restricted areas within the facility gates and facility owners and operators are now required, under federal regulations, to implement screening protocols for ensuring that cargo-transport vehicles and persons entering the facilities are inspected to deter the unauthorized introduction of dangerous substances and devices. At the facility gates, containers are required to be checked for evidence of tampering and cargo seals are checked.

- *Identity Security*: Identity verification is the third critical element of port security, recognizing that we must know and trust those who are provided unescorted access to our port facilities and vessels. The Coast Guard is working very closely with the Transportation Security Administration (TSA), the lead for implementation of the Transportation Worker Identification Credential (TWIC), to assist in the implementation of this new credentialing program. Just over three months ago, TSA approached the Coast Guard and asked for assistance in implementing the TWIC in the maritime mode through a regulatory project. The Coast Guard is fully supportive of this regulatory effort and will do everything within our ability to assist TSA in the development of this rulemaking.

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

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

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

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

- *Culture of Security*: Finally, and perhaps most importantly we have been able to take important steps to instill a culture of security within a system previously focused almost exclusively on efficiency. Reducing the vulnerabilities of our vessels and ports required a cultural shift to put security at the top of the agenda rather than as an afterthought. It is centered on the people who must implement the new security measures. Under our MTSA regulations, facilities and vessels are required to designate individuals with security responsibilities, including company security officers, facility security officers, and vessel security officers. These individuals must have knowledge, thorough training and equivalent job experience. They must be familiar with, and responsible for, implementation of the specific security measures outlined in the facility security plan and they must be knowledgeable in emergency preparedness, the conduct of security audits, and security exercises. In addition, facility security officers must have training in security assessment methodologies; current security threats and patterns; recognizing and detecting dangerous substances and devices, recognizing characteristics and behavioral patters of persons who are likely to threaten security; and techniques used to circumvent security measures.

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

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

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

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

Conclusion

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

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

Mr. COBLE. Mr. Scrobe.

Mr. SCROBE. Do I get his excess time, sir? [Laughter.]

Admiral HERETH. I just wanted to listen to your counsel.

TESTIMONY OF PETER J. SCROBE, VICE PRESIDENT, AMERICAN INTERNATIONAL MARINE AGENCY, ON BEHALF OF THE INTERNATIONAL CARGO SECURITY COUNCIL

Mr. SCROBE. Good afternoon, Mr. Chairman, Mr. Scott. I'm Vice President of AIMA, American International Marine Agency, which is a managing general agent for member companies of American International Group. On behalf of the International Cargo Security Council, ICSC, and myself, I'd like to thank you for giving us the opportunity to speak here today. Although we have several minutes, we could spend hours discussing this subject matter. I'd also like to thank John Hyde of Maersk Line and Randall Mullet of CNC for their input.

For many years, we have worked with Congress, particularly on what was the original Crime Bill of 2000, which ultimately became the MTSA of 2002. It was long, hard work with Government and law enforcement to prevent cargo crime and protect the supply chain to this country by criminals and terrorists that would seek us harm.

Annual cargo crime losses are estimated domestically at $10 to $20 billion per year, $30 to $50 billion internationally, and therein lies the problem since there is no accurate recording of loss data. Although many believe the numbers to be much higher, this lack of a true data system contributes to our inability to properly analyze the magnitude of the problem, which impacts local businesses, jobs, and the economy at large, as well as to correctly allocate resources and identify anomalies that may indicate terrorist activity. We truly believe that cargo crime is the equivalent of economic terrorism.

Over the past several years, and since September 11, Customs and Border Protection have instituted the C-TPAT and CSI, and additionally, the port authorities have undertaken the public-private partnership with OSC, Operation Safe Commerce. Under the MTSA, the ISPS Code, which is a global initiative directly supervised by the Coast Guard, has, according to many carriers and port personnel, tightened port security due to reporting requirements, particularly here in the States.

C-TPAT was a tremendous start and raised awareness with importers and exporters by helping them and their providers to better understand the actual workings of the global supply chain and the effort involved with the entire process. Although voluntary in nature, the desired result was to allow for fast and secure movement of cargo. It has, in my opinion, enhanced the quality and security of the supply chain, but according to many has not yet shown the speed and fast tracking which would allow cargo to move into the country, and it's not due to C-TPAT itself but to congestion at many of the ports, such as Long Beach. This congestion, according to many experts, will worsen with expectation to double in the next 10 to 20 years. This also has to do with the fact that larger ships of 8,000 to 12,000 tons will be built and coming into the States soon.

It is important to note that, with regard to cargo crime, ports have been less of a problem for theft of containers and trailers that we have seen. The majority of thefts and hijackings occur during the inland transit phase and usually prior to reaching final destination within the country. Mr. Chairman, I believe that various law enforcement agencies, in particular the multi-jurisdictional Cargo Task Forces, would also echo these same comments.

During consideration of the original Crime Bill of 2000, language to address intermodal aspects, enhance sentencing guidelines, creation of multi-jurisdictional Cargo Task Forces, and creation of a separate category for cargo crime in the Uniform Crime Reporting System, UCR, database was, unfortunately, not ever considered. To that end, Congressman Stearns has introduced bill H.R. 785, which the ICSC and the AIMU, American Institute of Marine Underwriters, strongly supports. This bill has also been considered as part of a National Strategy as adopted in February 2005 by the Cargo Summit in Tallahassee, Florida. The summit consisted of private sector, law enforcement, and government representation from around the country. We ask that the Committee carefully review and act on this responsible and worthwhile legislation this year.

Over the past 5 years, there have been many studies, including "Best Practices" by the Volpe Center, and "Contraband, Organized Crime, and the Threat to Transportation and Supply Chain Function," an FIA study sponsored by ICSC and Brown Williamson. Each were produced prior to September 11, but they are still viable in order to protect the supply chain. I urge you, Mr. Chairman and all Members of the Committee, to review these important documents.

As I mentioned earlier, discussion on this topic could go on and on. This past December, at the Department of Homeland Security Cargo Summit, Secretary Loy indicated he has heard the various industries' concerns. Many of these concerns voiced were the potential for over-reaction, over-legislation by Government that might actually threaten the supply chain more than a terrorist attack. Further, although there have been discussions on a private sector-Government partnership, it has not become a reality of true sharing but appears to be more of a one-way street.

Problems will also be inherent in a Government that is looking for one critical magic bullet in solutions in devices and technology. We don't believe there is a magic bullet, but do believe that a working and proven process with the enhancement of these devices will work.

Thank you for your time. I'll answer questions later.

Mr. COBLE. Thank you, Mr. Scrobe.

[The prepared statement of Mr. Scrobe follows:]

PREPARED STATEMENT OF PETER J. SCROBE

Mr. Chairman and Members of the Committee,

Good afternoon, I'm Peter J. Scrobe, Vice President of American International Marine Agency, a Managing General Agent for Member companies of the American International Group, Inc.

On behalf of the International Cargo Security Council (ICSC) and myself, I would like to thank you for giving us the opportunity to speak today. I would say that although we only have several minutes to present, we could discuss this extremely

important subject matter for hours. I would also like to thank Mr. John J. Hyde, Maersk Line and C. Randall Mullet, CNF, for their input.

For over 10 years, we have worked with Congress on what was originally the Crime bill of 2000, and ultimately became the Maritime Transportation Act (MTSA) of 2002. The private sector has worked long and hard with government and law enforcement to prevent cargo crime and protect the supply chain to this country by these criminals and terrorists that would seek to harm us.

Annual cargo crime losses are estimated at $10–20 billion domestically and $30–50 billion internationally. Therein lies the problem, since there is no accurate recording of cargo loss data. Although many believe the numbers to be much higher, this lack of a true data system contributes to our inability to properly analyze the magnitude of the problem, which impacts local businesses, jobs, and the economy at large, as well as to correctly allocate resources, and identify anomalies that may indicate terrorist activity.

CARGO CRIME IS THE EQUIVALENT OF ECONOMIC TERRORISM!

Over the past several years and since Sept. 11th, 2001, Customs & Border Protection have instituted: C-TPAT (Customs-Trade Partnership Against Terrorism), and the CSI (Container Security Initiative). Additionally, the Ports Authority have undertaken the public/private partnership with OSC (Operation Safe Commerce). Under the MTSA, the ISPS Code which is a global initiative directly supervised by the USCG has, according to carriers and port personnel, tightened port security, due to reporting requirements, particularly here in the US.

C-TPAT was a tremendous start, and has raised awareness with Importers/Exporters, by helping them and their providers to better understand the actual workings of the global Supply Chain, and the effort involved with the entire process. Although voluntary in nature, the desired result was to allow for fast and secure movement of cargo. It has, in my opinion, enhanced the quality and security of the Supply Chain but according to many has not yet shown the speed in which cargo would move into the country, primarily, due to the heavy congestion at the ports. This congestion, according to experts, will probably worsen with an expectation to double in the next 10–20 years.

It is important to note that, with regard to cargo crime, the ports have been less of a problem for theft of containers and trailers. The majority of thefts and hijackings occur during the inland transit phase and usually prior to reaching final destination. Mr. Chairman, I believe that various law enforcement agencies, in particular, the Multi-Jurisdictional Cargo Task Forces would also echo these same comments.

During consideration of the original Crime Bill of 2000, language to address intermodal aspects, enhanced sentencing guidelines, creation of Multi-Jurisdictional Cargo Task Forces and creation of a separate category for Cargo Crime in the Uniform Crime Reporting System (UCR) data base, was unfortunately not ever considered. To that end, Congressman Stearns (R-FL) has introduced Bill HR 785, which the ICSC, and the AIMU (American International Marine Underwriters) strongly supports. This bill has also been considered as part of the "National Strategy" as adopted in February, 2005 by the "Cargo Summit", in Tallahassee, FL. The Summit consisted of the private sector, law enforcement and government representation from around the country. We ask that the Committee carefully review and act on this responsible and worthwhile legislation, this year.

Over the past five years, there have been many studies, including, "Best Practices" (Volpe Center) and "Contraband, Organized Crime and the Threat to the Transportation and Supply Chain Function" (FIA Study-ICSC and Brown Williamson). Each were produced prior to Sept. 11, and they are still current in their content and viability to protect the Supply Chain. I urge you Mr. Chairman, and all members of the Committee to review these important documents.

As I mentioned earlier, discussion on this topic could go on and on. This past December at the Department of Homeland Security Cargo Summit, Secretary Loy indicated—"he has heard the various industries' concerns". The concerns voiced significantly were the potential for over reaction and legislation by government that might actually threaten the Supply Chain more so than a terrorist attack. Further, although there have been discussions on a private sector government partnership, it has still not become a reality of true sharing, but more of a one way street.

Also, problems will be inherent in a government that is looking for one "magic bullet" solution in devices.

The ICSC doesn't believe that there is such a "magic bullet" device. In the end, we believe that any number of devices, working in an established and proven proc-

ess will enhance the securing of the Supply Chain and further protect it from terrorists and criminals alike.

And the ever present question—who will be footing the bill?

I would leave the Committee with one final thought. We are here to assist and work with the public sector and we are asking for you to assist us in making the Supply Chain as secure as possible. It is only through true partnership that success can be met.

Once again, thank you for allowing me to attend and speak on
this extremely important subject matter.

Mr. COBLE. Mr. Keever.

TESTIMONY OF JEFF KEEVER, DEPUTY EXECUTIVE DIRECTOR, VIRGINIA PORT AUTHORITY

Mr. KEEVER. Good afternoon, and thank you, Mr. Chairman and Congressman Scott. It's a privilege to appear before you today to discuss the Virginia Port Authority's experience with port security.

The Port of Virginia is the seventh-largest container facility in the United States and the second-largest facility on the East Coast in terms of general tonnage. The Port of Virginia is designated as a strategic port by the U.S. Maritime Administration, and as such, must be ready to support wartime mobilization and onload of military equipment for deployment overseas. In addition to the three Virginia Port Authority marine terminals, the Port of Virginia contains over 80 private port facilities covered by the Maritime Transportation Security Act, including coal and petrochemical terminals, commercial shipyards, and a wide range of other facilities.

To date, VPA has received $11.4 million in port security grants. VPA has contributed an additional $11 million of its own funds to complete the required security enhancements. The $11.4 million in port security grants received by VPA to date fall far short of what is needed. VPA has identified three high-priority projects that are necessary to mitigate serious shortfalls in our security posture. These three projects require at least an additional $12.5 million.

The Port of Virginia has been successfully employing radiation monitoring equipment since December 2002 and has led the nation in radiation monitoring at seaports. The radiation detection equipment ensures that 100 percent of all import containers leaving the terminal by truck are monitored and any detection of radiation is resolved before the container leaves the VPA terminal. There is no Federal policy or regulation requiring any marine terminal or operator to conduct radiation monitoring. VPA's current program was self-initiated well before there was a national program and no other port in the nation has done likewise. CBP is responsible for monitoring inbound cargo for radiation and has a multi-year program to deploy radiation monitoring equipment at all land, sea, and air ports of entry.

The Port of Virginia has enjoyed a longstanding, productive relationship with the Federal agencies on the front line of port security, the Coast Guard and CBP. Both are still stretched thin and coping with significant equipment challenges. For example, the Coast Guard does not have the proper equipment to board and inspect vessels in all weather conditions. CBP also faces personnel and equipment challenges. CBP is forced to rotate its limited number of vacuous cargo inspection systems among multiple ports and

facilities. A suspect container that must wait for days to be inspected is a latent threat to homeland security.

The solution is to ensure that CBP has the the resources it needs. Congress must ensure that adequate resources are dedicated to guaranteeing the security of the nation's seaports. MTSA-mandated security measures are far beyond what the port industry would need to implement for the security of their own facilities. In short, the port industry has been mandated by Federal law to protect the nation against terrorist attacks.

Although Federal law placed significant responsibility for homeland security on the shoulders of the port industry, the Federal Government has not provided the funding stream commensurate with the financial burden the port industry must bear to implement MTSA, which is unique in all of U.S. homeland security. The aviation and ground transportation industries have not been required to meet similar mandates. The safety of commercial aviation has been federalized, the burden taken off the aviation industry, and over $11 billion spent for airline passenger screening and security.

Similarly, CBP bears full responsibility at land ports of entry. For example, the Ambassador Bridge connecting Detroit, Michigan, with Windsor, Ontario, is a major land port of entry and a critical link in the supply chain for the cluster of automobile factories around Detroit, yet neither the auto industry nor the trucking industry has been addled with the cost of providing security for this port of entry. Only the maritime port industry has been compelled, under threat of fines and Coast Guard sanctions, to bear the high cost of protecting the nation against terrorists.

The port industry is doing the best it can with the resources it has. The American Association of Port Authorities has recommended that funding for the Port Security Grant Program be increased to $400 million per year, which we support. Security funding could be earmarked from the over $25 billion collected in Customs revenue from duties and importation fees each year.

The Virginia Port Authority's experience with port security and radiation monitoring offers important lessons for enhancing U.S. homeland security. Much progress has been made, but much more remains to be done. America's ports take their responsibilities seriously and are dedicated to doing the best they can to protect the nation. They have earned your respect.

Thank you, and I'll be happy to answer any questions you may have.

Mr. COBLE. Thank you, Mr. Keever.

[The prepared statement of Mr. Keever follows:]

PREPARED STATEMENT OF JEFF KEEVER

Good Afternoon Mr. Chairman and distinguished members of the Committee. It is an honor and a privilege to appear before you today to discuss the Virginia Port Authority's experience with port security and radiation monitoring.

As you have heard from Commissioner Bonner, combating the smuggling of illegal and potentially dangerous cargo into the United States is a daunting task due to the sheer magnitude of cargo entering the country every year; however, it is critical to the success of America's homeland security strategy. But just as important is the protection of America's ports against terrorist attacks. About 8,100 foreign flag ships and 9,200 U.S. flag vessels make almost 60,000 arrivals in the 361 U.S. commercial ports annually. These ports contain approximately 3,200 maritime facilities that

could be targeted. Despite the magnitude, they must remain national priorities if our country is to be protected from devastating loss in terrorist attacks.

OVERVIEW OF THE PORT OF VIRGINIA

The Virginia Port Authority (VPA) is an agency of the Commonwealth of Virginia, reporting to the Secretary of Transportation. VPA's state-owned port facilities are known collectively as The Port of Virginia and include three marine terminals in Hampton Roads: Norfolk International Terminals (NIT), Portsmouth Marine Terminal (PMT), and Newport News Marine Terminal (NNMT). VPA also owns the Virginia Inland Port (VIP), an intermodal rail facility located near Front Royal, Virginia. These terminals are operated by Virginia International Terminals (VIT), the non-profit, non-stock corporate operating affiliate of VPA. Additionally, VPA hosts a number of private corporations on its terminals.

The Port of Virginia is the seventh largest container facility in the United States and the second largest facility on the East Coast in terms of general tonnage. In 2004, VPA handled 1.81 million TEUs of containerized cargo, an increase of 9.9% from 2003. Containerized cargo handling at The Port is projected, conservatively, to grow by 9% in 2005. Additionally, VPA handled 14 million tons of general (non-containerized) cargo in 2004, a 6.25% increase over 2003. Also in 2004, The Port of Virginia received calls from more than 2,000 ships delivering or picking up containers and other general cargo.

The Port of Virginia functions as a major economic engine. In Hampton Roads, only the military rivals The Port in employment and contribution to the regional economy. But The Port does not only benefit the Hampton Roads region—over eighty businesses have located distribution centers throughout the state to take advantage of proximity to The Port, benefiting many local economies. According to a 1999 economic impact study by Martin Associates, overall activity at The Port translates into 165,000 port and port-related jobs, $762.5 million in business revenues, and $60.7 million in state and local taxes throughout the Commonwealth. In 2003, the Bureau of Economic Statistics reported that The Port of Virginia plays a part in over 180,000 jobs, with salary and wages in excess of $5 billion.

The Port of Virginia is designated as a Strategic Port by the U.S. Maritime Administration (MARAD) and as such, must be ready to support wartime mobilization and on-load of military equipment for deployment overseas. Because Hampton Roads is a major logistics node for the U.S. Armed Forces, the Defense Logistics Agency and U.S. Transportation Command move a substantial amount of containerized cargo and military vehicles through the VPA Terminals to and from Europe and the Middle East every week.

In addition to the three VPA marine terminals, The Port of Hampton Roads contains over eighty private port facilities covered by the Maritime Transportation Security Act (MTSA), including coal terminals, petrochemical terminals, commercial shipyards and a wide range of other facilities. The City of Norfolk has become a burgeoning cruise ship destination and has recently launched construction of a $40 million terminal that will greatly increase the number of cruise ships and passengers visiting Hampton Roads. The cruise ship business is growing rapidly. About 50,000 passengers visited Norfolk in 2003, around 100,000 visited in 2004, and another 114,000 are expected in 2005. The number of passengers could increase to 200,000 or more after the new terminal is complete.

Hampton Roads is not only a major commercial port, but also home to the largest concentration of U.S. Naval forces in the world. Two of VPA's marine terminals are located near major U.S. Navy facilities—NIT shares a fence line with Naval Station Norfolk, home to 5 aircraft carriers, 11 submarines and about 50 other naval vessels. PMT is adjacent to Norfolk Naval Shipyard and Norfolk Naval Hospital. The headquarters of the U.S. Atlantic Fleet, U.S. Joint Forces Command and NATO Allied Command Transformation are located across the street from NIT. NNMT is located near Northrop Grumman Newport News Shipbuilding, the only shipyard in the nation capable of building nuclear powered aircraft carriers. Northrop Grumman also overhauls aircraft carriers and other naval vessels. The Hampton Roads region is also home to eight other Navy bases, three Army bases, and a major Air Force base.

Hampton Roads is also a major urban area. Its 16 cities and counties have a total population exceeding 1.574 million, making it the 6th largest urban area in the nation.

THE VIRGINIA PORT AUTHORITY'S EXPERIENCE WITH PORT SECURITY

VPA's guiding principle for security is that a state port authority has a higher level of responsibility than a private port facility operator. That is VPA has a moral

obligation to maintain high standards of security in order to protect the citizens of the Commonwealth of Virginia—and the American people in general—from the threat of terrorism. VPA must also be mindful of the importance of its contribution to the economy of the Commonwealth. We have a duty to foster commerce, trade and economic development in the Commonwealth of Virginia by promoting maritime commerce and freight shipment. This means that VPA must be competitive with other ports and strive to achieve the highest possible levels of productivity and efficiency. Thus, like every port authority, VPA is confronted with the challenge of reconciling its security responsibilities with its economic responsibilities.

Port Security After September 11, 2001. VPA had an aggressive security program well before the September 11, 2001 terrorist attacks. The Port Authority Police, sworn law enforcement officers of the Commonwealth of Virginia, have been highly effective at preventing crime on VPA's three marine terminals. Indeed, VPA has not had an incident of cargo theft in well over eight years. This is mostly due to the fact that the Port Authority Police verify that U.S. Customs and Border Protection (CBP) have properly cleared all cargo departing the terminals by truck and released for delivery. Police verification provides typical cargo processing operations with an additional and independent layer of anti-theft protection.

As Hampton Roads is home to the largest concentration of U.S. Naval forces in the world, VPA understood that its security efforts were integral to Navy and Coast Guard efforts to keep The Port secure. The Port of Virginia is a designated Strategic Port and therefore, is required to meet Federal security requirements related to mobilization and deployment of the U.S. Armed Forces and has had years of experience working with various Federal agencies on port security matters. Following the al-Qaeda attack on the *USS Cole* in October 2000, VPA worked closely with the U.S. Navy to ensure that our security measures and operations complemented and supported enhanced Navy force protection efforts. The result was a close working relationship with the Coast Guard Captain of The Port and the Navy's regional program managers for port operations and security.

VPA redoubled its security efforts from September 11, 2001 onward. VPA coordinated with the local U.S. Coast Guard Captain of The Port to increase security procedures at its terminals immediately after the terrorist attacks. In addition, a comprehensive security assessment was immediately undertaken and completed by the end of the year. This security assessment was published in February 2002—nine months *before* the Maritime Transportation Security Act (MTSA) enacted legislation requiring such assessments. This assessment identified priority security enhancements for which VPA began requesting Port Security Grants when that program was established in 2002. This initial security assessment was refined in a second Facility Security Assessment conducted in 2003 based on MTSA requirements and the Coast Guard Maritime Facility Security Regulations (33 CFR, Chapter 1, Subchapter H, Part 105).

For port authorities, fulfilling their responsibilities for homeland security is much more complicated than merely being in compliance with MTSA and the International Ship and Port Facility Security Code (ISPS). A number of other Federal and state policies, programs and guidelines related to homeland security and emergency preparedness impact them as well.

VPA Participation in the Customs-Trade Partnership Against Terrorism. VPA is a certified participant in the Customs-Trade Partnership Against Terrorism (C-TPAT). VPA signed a Memorandum of Understanding with CBP on March 11, 2003 to participate in C-TPAT as a Port/Terminal Operator. The required Security Profile was submitted to CBP on April 8, 2003, and in April 2004, a CBP Validation Team met with the VPA Director of Police and surveyed NIT. Based on the findings of the Validation Team and documentation provided by VPA outlining security enhancements then in progress, CBP validated VPA compliance with C-TPAT security standards on July 1, 2004.

Personnel Identification Programs. VPA anticipates that its security program will be impacted by and have to adapt to three emerging personnel identification programs: the Transportation Security Administration (TSA) Transportation Workers Identification Credential (TWIC), the CBP US-VISIT Program, and the International Labor Organization (ILO) revised Seafarers' Identity Documents Convention.

The TWIC program entails the development of a secure, uniform credential for transportation workers, including longshoreman, truck drivers and all marine terminal personnel, potentially including all persons with access to cargo shipping data. TSA has not published a timeline for TWIC implementation, but the program will likely commence in 2005. The technology required by TWIC may include significant access control upgrades as well as the installation of *2-stage* gates. These en-

hancements will require a major capital outlay commitment on the part of VPA, and may also negatively impact operating efficiency while upgrades are being made.

The US-VISIT program uses biometrics—digital fingerprint scans and digital photographs—to check visitors entering the U.S. against a database of known criminals and suspected terrorists. In 2004, CBP began implementing US-VISIT entry procedures at 115 airports, 14 seaports and the 50 busiest land ports in the nation. CBP has indicated that US-VISIT will be expanded to all air, land and maritime ports of entry as well. Although CBP is responsible for implementing US-VISIT, CBP will require support from Port Authority Police and modifications to VIT terminal operating procedures to ensure that crew and passengers aboard ships arriving at VPA terminals cannot circumvent CBP procedures.

The ILO Seafarers' Identity Documents Convention significantly upgrades the identification documents that seafarers are required to carry and includes the use of biometric technology similar to that used by TWIC and the US-VISIT program. Although CBP has not explained how the new Seafarers' Identity Documents will relate to the US-VISIT program, VPA anticipates that its procedures for controlling the movements of ships' crewmembers on its terminals will be impacted by the manner in which CBP elects to use the Seafarers' Identity Documents.

Emergency Preparedness Guidelines. VPA, and all port authorities, must also support state homeland security and emergency preparedness policies and guidelines, which are in turn driven by Federal policies and guidelines. VPA's emergency response plans and procedures must be compliant with the recently-published National Incident Management System (NIMS) and National Response Plan (NRP), and our training program must be consistent with the Homeland Security Exercise and Evaluation Program (HSEEP) published by the Office for Domestic Preparedness (ODP). Implementation of NIMS, NRP and HSEEP requires additional VPA funds. It is important to note that, for port authorities, implementation of these state security programs is separate from compliance with Federal programs such as MTSA and the Coast Guard security emergency response training and readiness requirements.

VPA must also comply with rapidly changing Federal and state programs related to public safety and emergency preparedness communications interoperability. Federal initiatives, guided by Project SAFECOM, are being implemented in the Commonwealth of Virginia by the Office of Commonwealth Interoperability and the State Agency Radio System (STARS) project. The existing Port Authority Police communications and information systems predate these emerging Federal and state interoperability requirements and will require significant upgrades to ensure that VPA can coordinate effectively with Federal, state, and local agencies in Hampton Roads during a significant port or regional emergency.

Federal Port Security Grants. The initial security assessment conducted in 2001 identified approximately $40 million in security enhancements for the VPA terminals. These recommendations were modified in the 2003 Facility Security Assessment to ensure that VPA security investments and requests for Port Security Grants would be focused on compliance with MTSA and the Coast Guard Maritime Facility Security Regulations.

To date, VPA has received $11.4 million in Port Security Grants, as follows:

	Grant Amount	VPA Contribution
Round 1, June 17, 2002:	$5.293 million	$1.499 million
Round 2, June 2003:	$3.090 million	$5.477 million
Round 3, December 10, 2003:	$0.875 million	$0.219 million
Round 4, September 10, 2004:	$2.120 million	$3.801 million

These funds have supported upgrades to fences and gates, installation of a closed circuit television perimeter surveillance system, enhanced access control for gates and critical buildings, command center enhancements, and other upgrades. In addi-

tion to funds received as Port Security Grants, VPA has contributed an additional $11 million of its own funds to complete the required security enhancements.

The $11.4 million in Port Security Grants received by VPA to date falls far short of what is needed. VPA has identified three high priority projects that are necessary to mitigate serious shortfalls in VPA's security posture. These three projects require at least an additional $12.5 million:

- **Upgrades to Port Authority Police Communications System.** Upgrades are required to comply with Federal SAFECOM interoperability standards. These standards are being implemented in Virginia by the Office of Commonwealth Interoperability and the STARS program, and are required for completion of The Port's Integrated Security System. The enhanced communications suite, which uses digital trunking technology and dedicated frequencies, will ensure that the Port Authority Police can effectively coordinate with Federal, state and local law enforcement and emergency response agencies in the event of an emergency. Total system cost is estimated at $1.5 million.
- **Command and Control Architecture.** A system must be developed which will integrate internal and external voice/data/video communications, police dispatch and radio systems with the command center alert and display system. This integrated system is required for compliance with MTSA and Coast Guard Maritime Facility Security Regulations, emergency response, real-time information exchange for maritime domain awareness, mandatory implementation of the National Incident management System (NIMS) and National Response Plan (NRP), credentialing and implementation of the Transportation Worker Identification Credential (TWIC) and US-VISIT Program, compliance with the Customs-Trade Partnership Against Terrorism (C-TPAT), and implementation of Federal and Commonwealth of Virginia continuity of operations requirements. Total cost is estimated at $10 million.
- **Cyber Security.** VPA and VIT information technology (IT) systems are vulnerable to a range of cyber threats that could defeat terminal and cargo security efforts. The threat is much more than just viruses and worms. Terrorists or other criminals could use cyber attacks to forge shipping documents to facilitate smuggling, circumvent CBP by releasing containers designated for inspection, divert delivery of containers from legitimate businesses to terrorist or criminal front companies, identify container contents for theft or pilferage, forge visitor passes or other identity documents to gain access to terminals, or disrupt security systems and port facility operations. VPA must implement a cyber security system that will thwart such cyber threats while avoiding unnecessary interference with business processes. Additionally, the system must allow VPA to identify attempted cyber attacks for reporting to CBP (to help detect smuggling) and other Federal agencies. Total cost is estimated at $1 million for 2006, and considerable additional funding required to maintain the system's effectiveness in the future.

THE VIRGINIA PORT AUTHORITY RADIOLOGICAL MONITORING PROGRAM

Immediately after the September 11, 2001 terrorist attacks, VPA identified radiological and nuclear devices as a significant potential threat to its terminals, adjacent naval bases, The Port and the Hampton Roads region. VPA initiated planning for a radiological monitoring system and began meeting with radiation detection equipment vendors in November 2001 to identify appropriate systems for testing at the VPA terminals. The Department of Energy provided technical advice on radiological monitoring for VPA.

VPA also consulted with the U.S. Navy at Naval Station Norfolk, which had extensive experience with radiological monitoring and response procedures, and which was the first defense installation assessed in the Sandia National Laboratory's study of "unconventional nuclear threats" to U.S. military bases. Sandia's assessment of terrorist options for carrying out a radiological or nuclear attack in Hampton Roads provided valuable insight for VPA's planning.

Initial Goals, Research and Testing. VPA's initial goal was to protect The Port against radiological or nuclear attack. Placing radiation sensors at the entrance to the harbor was considered but quickly rejected because the technology available at the time would not provide reliable detection and the Port Authority Police lacked jurisdiction in the areas of the harbor where the sensors would be placed. The second alternative considered was a radiation monitoring system that would detect radiological or nuclear devices before they were offloaded from ships. This system included an initial test of radiation sensors placed on the spreader bars used to lift containers off vessels.

Testing of radiation sensors on spreader bars commenced in January 2002 and continued through June 2002. Those tests revealed that attempting to detect radiation in containers using sensors on the spreader bars of cranes was not feasible for three reasons:

1. Background radiation varied widely over land, water and vessels, making it difficult to set the system's sensitivity alarm threshold at a level that ensured reliable detection while avoiding excessive false alarms. Additionally, when radiation was detected, it was not possible to readily determine if the radiation source was in the container to be lifted or in an adjacent container.
2. None of the sensors tested proved capable of standing up to the shock and vibration of container handling operations. Excessive sensor failure rate made the cost of placing sensors on spreader bars prohibitive.
3. The development protocols for responding to the detection of radiation involved numerous operational issues that could not be easily resolved at the port level. Thus, even if the radiation monitoring equipment functioned properly, it was extremely difficult for VPA to develop effective procedures for dealing with detection of radiation in a container that was still on a vessel, especially since the Port Authority Police lacked jurisdiction over the vessel.

By October 2002, the Port of Virginia received a $1 million Port Security Grant and had already invested approximately $660,000 of its own funds to test and install radiation detection equipment. Because it was VPA's goal to deploy an operational system rather than conduct a long-term research and testing program, the failure of the tests of radiation sensors on spreader bars led VPA to initiate an alternative approach that could be implemented near-term.

Testing and Implementation of a Workable Solution. VPA determined that a viable alternative was to provide protection to the rest of the nation by monitoring containers for radiation *before* they departed the VPA terminals for shipment to their destinations around the country. A disadvantage of this approach was a lack of protection at the terminal itself. A container housing a radiological or nuclear device would arrive at a VPA terminal and not be detected until it passed through radiation monitoring equipment at terminal exits. However, it was determined that it was unlikely that terrorists would attack a container terminal with a radiological device. Given the enormous effort required to acquire the radioactive material, ship it to the United States undetected, and assemble a radiological dispersal device, such an attack probably would be reserved for higher priority targets guaranteed to cause a large number of casualties and psychological, economic and symbolic damage. The greatest risk was believed to be from inadvertent detonation of such a device at the terminal, or the terrorist group electing to "use it rather than lose it" upon learning that CBP had intercepted their attempt to smuggle it into the country. Hence, emphasis was placed on developing effective response protocols to these situations.

In November 2002, VPA began testing a radiation detection portal at one of its exit gates. This test was successful and VPA decided to deploy truck portals at all three of its marine terminals.

Concurrent with testing radiation detection equipment, in February 2002 VPA began working with U.S. Customs and Border Protection, the Department of Energy's Radiological Assistance Program, the Federal Bureau of Investigation and the Maritime Administration to develop effective response protocols. These discussions developed answers to questions such as who VPA should notify when radiation was detected, what agencies would respond, and who was responsible for placing a radiological or nuclear device in a safe condition and removing it for proper disposal. These discussions were later expanded to include state, regional and local agencies that would be involved in a radiological emergency. This was pioneering work—at the time, there was no Federal program in existence such as that being implemented by VPA, and thus there were no existing response protocols that VPA could turn to for guidance.

VPA's effort to develop response protocols culminated in CBP and VPA signing a Standard Operating Procedure (SOP) for response to detection of radiation—the first of its kind in any U.S. seaport. The SOP was developed with support from CBP's Laboratory Support Services (LSS) and the Department of Energy's Pacific Northwest National Laboratory. Initially developed only for the truck portals, the SOP was amended in November 2003 to include the rail portals as well.

Training and Practice Exercises. VPA recognized early on that extensive training and frequent practice exercises would be essential for effective implementation of the radiation monitoring program. Port Authority Police were trained in the use of the radiation detection equipment and procedures for responding to detection

of radiation. This training was required to meet CBP standards in order for the VPA radiation monitoring program to be certified by CBP and placed in operation. VPA held its first radiological emergency field exercise (FTX, also referred to as an "operations-based" exercise) on November 19, 2003. It exercised Federal, state and local first responders in the Hampton Roads region in basic procedures for responding to the detonation of a radiological dispersal device in a shipping container on a VPA terminal. It was an invaluable exercise for identifying equipment, training, procedural and communications deficiencies that needed to be addressed by the participating agencies. However, it did not fully exercise the VPA-CBP radiological SOP.

In December 2003, VPA pointed out the need for a follow-on exercise in a presentation on its radiological monitoring program to Federal officials from TSA and CBP, and state officials including the Governor's Assistant for Commonwealth Preparedness and his deputy. In January 2004, TSA proposed a tabletop exercise to familiarize Federal, state and local emergency management personnel and first responders with the VPA-CBP radiological SOP and to exercise the national response to detection of a radiological device in a seaport. Planning for this critically important exercise commenced in February 2004 but had to be suspended in June 2004 due to lack of funds.

On March 1, 2005, VPA received an ODP State Homeland Security Grant from the Virginia Department of Emergency Management to conduct the long-delayed tabletop exercise (discussion-based exercise) later this year. It will be held in conjunction with the Radiation Pilot Program Office (RPPO) multi-port radiological exercise so that national radiological defense efforts benefit from the VPA exercise as well.

The original plan for the VPA radiological exercise had envisioned a tabletop exercise in the Fall of 2004, followed by a major field exercise (operations-based exercise) in the Spring or Fall of 2005. The major field exercise will involve significant participation by Federal, state and local emergency management personnel and first responders. Because the tabletop exercise was postponed, the major field exercise has not been scheduled, but remains a high priority for the Hampton Roads region.

Documented Success. The Port of Virginia has been successfully employing radiological monitoring equipment since December 2002 and has led the nation in radiological monitoring at seaports. The radiation detection equipment ensures that 100% of all import containers leaving the terminal by truck are monitored and any detection of radiation is resolved before the container leaves the VPA terminal. In 2004, the VPA truck portals detected radiation in containers and trucks on over 1,000 occasions. All were resolved in cooperation with the CBP Port Director. VPA is currently in the final stages of testing and gaining CBP certification for a rail portal that will monitor containers departing NIT by train. In cooperation with CBP, the Port Authority Police has deployed radiation detection equipment to National Special Security Events such as the 2004 Republican National Convention and the 2005 Presidential Inauguration.

There is no Federal policy or regulation requiring any marine terminal operator to conduct radiation monitoring. VPA's current program was self-initiated well before there was a national program and no other port in the nation has done likewise. CBP is responsible for monitoring inbound cargo for radiation, and has a multi-year program to deploy radiation monitoring equipment at all land, sea and air ports of entry. Currently, VPA remains the only seaport in the country performing radiation monitoring on cargo entering the nation's interior.

LESSONS LEARNED FROM THE VIRGINIA PORT AUTHORITY EXPERIENCE

The Port of Virginia has enjoyed a long-standing, productive relationship with the Federal agencies on the front lines of port security—the Coast Guard and CBP. Both agencies are represented by outstanding, dedicated leaders in Hampton Roads—leaders who make a concerted effort to understand port and shipping industry concerns and constraints. This spirit of partnership and cooperation is vital for the success of the nation's port and cargo security efforts. CBP's C-TPAT program and the Coast Guard's Area Maritime Security Committees are prime examples of partnerships that work.

Inter-Agency Cooperation. Both CBP and the Coast Guard have recognized that measures to enhance port and cargo security must facilitate commerce, not hinder it. Unreasonably impeding the flow of cargo or increasing the cost of moving it through America's ports would cause unacceptable losses for America's factories and retailers in an era of just-in-time delivery. The thousands of containers entering the United States every day have replaced the warehouses of yesteryear. In fact, the stream of containers across the world's oceans could be viewed as warehouses in motion. Security measures that impede their flow or raise shipping costs would quickly destroy the spirit of partnership and replace it with an adversarial relation-

ship detrimental to both sides. Rather than support CBP and the Coast Guard, the port and shipping industries would be forced by economic pressure into a minimal compliance posture that could potentially make it much easier for terrorists to circumvent port and cargo security efforts.

CBP and the Coast Guard face additional challenges as well. Although both have received significant increases in funding and personnel since the September 11, 2001 terrorist attacks, they are still stretched thin and coping with significant equipment challenges. For example, the Coast Guard does not have the proper equipment to board and inspect vessels in all weather conditions, day or night. The result is that vessels must wait for conditions to improve before the Coast Guard can conduct its inspections. This delays vessel arrivals, disrupts the flow of cargo, and causes backlogs of ships awaiting berths at terminals. Like most ports, VPA relies on the Coast Guard for waterside security and it is essential that the Coast Guard be properly equipped to carry out that mission.

CBP also faces personnel and equipment challenges. One such challenge that has negatively impacted VPA is that CBP is forced to rotate its limited number of VACIS(r) cargo inspection systems among multiple ports and facilities. Although VACIS(r) is vehicle-mounted, it is not easily and quickly moved, causing cargo to back up on marine terminals awaiting the VACIS(r) machine for inspection of flagged containers. This delay not only threatens to degrade CBP cargo security efforts, but also negatively impacts ports, which must cope with the resulting congestion. A suspect container that must wait for days to be inspected is a latent threat to homeland security, which could potentially escape CBP's notice. The solution is to ensure that CBP has the resources it needs to conduct inspections in a timely manner without impeding the flow of cargo through America's ports. Congress must consider earmarking part of CBP's budget to ensure that adequate resources are dedicated to guaranteeing the security of the nation's seaports.

Port Security Funding Issues. With regard to the security of maritime facilities, the most obvious and important lesson that VPA can offer is that effective port security does not come cheaply. MTSA created a mandate for port authorities and port facility operators to implement extraordinary security measures. The Coast Guard Maritime Facility Security Regulations require stringent security measures for port facilities, with emphasis on perimeter security and surveillance, credentials and access control, and training and exercises. Implementing these security measures and meeting these mandates requires a significant financial commitment. In addition, failure to meet MTSA and Coast Guard standards can result in considerable fines or a ban on vessels calling on a non-compliant facility.

MTSA-mandated security measures are far beyond what the port industry would need to implement for the security of their own facilities based on a risk management approach. Clearly, the intent of MTSA is to protect the nation from terrorist attacks—both attacks facilitated by smuggling weapons of mass destruction through seaports and attacks intended to cripple the American economy by forcing large-scale closure of seaports. In short, the port industry has been mandated by Federal law to protect the nation against terrorist attacks.

Although Federal law placed significant responsibility for homeland security on the shoulders of the port industry, the Federal government has not provided the funding stream commensurate with the financial burden the port industry must bear to implement MTSA. VPA, like the rest of the port industry, has shouldered the financial burden to comply with the Federal mandate; however, this results in negative impacts for both the economy and the security of the United States.

The MTSA mandate and the financial burden it places on the port industry is unique in all of U.S. homeland security. The aviation and ground transportation industries have not been required to meet similar mandates. The safety of commercial aviation has been Federalized—the burden taken off the aviation industry—and over $11 billion spent for airline passenger screening and security. Unlike America's seaports, an international airport does not have to shoulder the financial burden of Federally-mandated security standards. Similarly, CBP bears full responsibility at land ports of entry for keeping terrorists and their weapons out of the United States. Private transportation operators—trucking and rail companies—have not been forced to bear this cost. For example, the Ambassador Bridge connecting Detroit Michigan with Windsor, Ontario is a major land port of entry and a critical link in the supply chain for the cluster of automobile factories around Detroit. Yet neither the auto industry nor the trucking industry has been saddled with the cost of providing security for this port of entry. Only the maritime port industry has been compelled, under threat of fines and Coast Guard sanctions, to bear the high cost of protecting the nation against terrorists.

This is not good for the port industry, the American economy or homeland security. The port industry is doing the best it can with the resources it has, but much

more remains to be done and it simply cannot be accomplished in a timely manner unless the Federal government is willing to fund a greater portion of the port security financial burden. The American Association of Port Authorities has recommended that funding for the Port Security Grant Program be increased to $400 million per year. VPA wholeheartedly supports this position. Security funding must be earmarked from the over $25 billion collected in customs revenues from duties and importation fees each year. These fees come largely from our nation's seaport operations. In Virginia alone, it is estimated that over one-half billion dollars in customs revenues were collected in 2004.

If the Federal government is not willing to pay for the level of security that it has mandated for the nation's ports, then it should rethink the security requirements imposed under that mandate. The current approach sets blanket standards and requirements for all port facilities, regardless of size, type, likelihood of being attacked or potential consequences of an attack. For example, a container terminal and a pier for loading or unloading cement must both implement the same measures as a liquefied natural gas (LNG) terminal. This blanket approach can only be justified by asserting that each and every port facility is equally likely to be attacked by terrorists and would generate the same consequences in terms of loss of life and loss to the American economy. The result of the blanket approach is that efforts are being made and costs are being incurred which contribute very little to homeland security.

There is an alternative approach that would enhance homeland security at much less cost than the current approach. Congress should direct the Department of Homeland Security (DHS) and the Coast Guard, by amending MTSA if necessary, to adopt a focused approach to port facility security. Under this approach, port facilities would be differentiated based on size, type, likelihood of being attacked and potential consequences of an attack, and the security standards they must meet would be tailored to their status based on these factors. Smaller facilities (those less likely to be attacked and those that would not result in catastrophic loss if attacked) would have less stringent—and less costly—security requirements. For container terminals, the emphasis would be on security measures that prevent smugglers from being able to circumvent CBP efforts to keep terrorist weapons out of the country. Port facilities that handle large quantities of explosive or hazardous materials, such as LNG, petroleum and chemical terminals, would focus on measures to prevent terrorists from gaining access to the terminals in order to cause catastrophic damage to storage and piping systems.

By permitting limited Federal funding to be focused on specific measures that will do the most to improve port security and relieve the port industry of having to implement—at great cost—measures that accomplish very little, this focused approach would achieve a greater level of homeland security at much less cost than the current approach.

Funding Sources for Security Operating Expenses. A second serious funding issue is that Port Security Grants can only be used to fund the procurement and installation costs of new security equipment and systems. Port Security Grants cannot be used to cover the increased cost of personnel, operations, maintenance and training resulting from compliance with MTSA and Coast Guard regulations. These costs must be borne solely by port authorities and port facility operators.

VPA's security program costs $6 million per year, which includes almost $1 million in overtime for the Port Authority Police—a cost difficult to avoid given the manpower-intensive security procedures mandated by the Coast Guard regulations. Prior to the MTSA mandate, VPA spent well under $4 million per year and enjoyed a decade without an incident of cargo theft on any of its terminals. This clearly illustrates the difference in cost between a security program designed to meet a port's crime prevention requirements, and a homeland security program designed to protect the security of the American people.

VPA is developing a long-range security budget that seeks to sustain compliance with MTSA and Coast Guard requirements in a cost-effective manner. VPA is also making an effort to meet MTSA exercise requirements at the least cost, such as by participation in Federal exercises and seeking State Homeland Security Grant Program funds for exercises that contribute to Commonwealth emergency preparedness as well as meeting MTSA requirements. However, despite these efforts to carefully manage security costs, VPA will still face increased costs for meeting Federally-mandated security requirements over the long term.

Currently, the only Federal support for annual operating expenses is compensation for overtime incurred when DHS sets Homeland Security alert Level Orange or higher; however, this compensation is not sufficient. Compliance with MTSA has significantly increased annual operating expenses, including maintenance of the high technology security systems required for effective compliance with MTSA,

training and exercise expenses, and all the personnel and other operating expenses incurred by ports for security.

Congress should work with DHS to amend the Port Security Grant Program to permit a portion of those funds to be applied to annual operating expenses for security. This is particularly important for port authorities like VPA, which are public agencies. Most port authorities, including VPA, require funding from tax revenues to supplement income from port revenues. This means that the added cost of MTSA requirements is a tax burden on states hosting ports—which are hard pressed to meet those costs—even though the enhanced security benefits all states.

A formula could easily be developed that permits port authorities to apply for grants to cover a portion of their annual operating expenses for security, based on the security enhancements they have been required to make in order to comply with MTSA.

In the near term, funds for capital investments in enhanced security equipment and systems should not be reduced to provide funds for annual security operating expenses: the vulnerabilities that must be corrected are too great. The best solution would be to determine the funds that port authorities need to help defray the annual cost of MTSA compliance and increase funds appropriated for the Port Security Grant Program. Over time, as capital investments in enhanced security systems and equipment begin to meet requirements, a larger portion of Port Security Grant Funds can be shifted to cover annual operating expenses for security.

Distribution of Security Grant Funds. The third major Port Security Grant Program issue arises from the manner in which available funds are distributed. As described above, VPA has only received about a third of the funds it needs to implement the security upgrades required for effective MTSA compliance. As a result, VPA has been forced to spend more of its own funds on port security than it has received from the Federal government. This is harmful for The Port of Virginia and the economy of the Commonwealth of Virginia. VPA has been required to divert funds to port security, which would otherwise have been invested in port development—bringing additional business to the port and increased employment in Hampton Roads and throughout Virginia.

The DHS Inspector General recently released a report that addresses the types of projects in other ports for which Port Security Grants have been provided. While not wishing to critique these projects, VPA is without question one of the Strategic Ports that has suffered from a lack of port security grant funds, or stated differently, a lack of Federal appropriations for our nation's security.

Consolidation of the Port Security Grant Program into the much larger Targeted Infrastructure Protection (TIP) Grant Program as proposed by DHS in its Fiscal Year 2006 budget request will not alleviate any of these problems. If anything, the TIP Grant Program will make it more difficult to receive grant funds because ports will be competing will all forms of ground transportation—rail, trucking and mass transit—as well as with other critical infrastructures such as the energy industry and chemical plants. Additionally, if DHS distributes TIP grant funds via the states, there is little likelihood that the formula used to allocate grants among the states will reflect port security requirements. This scenario would serve only to shift the competition for grant funds from the Federal to the state level, forcing port authorities and other port facility operators to compete with state agencies and local governments seeking TIP grant funds as a means of compensating for the overall 37% reduction in homeland security grants proposed by DHS in Fiscal Year 2006.

Radiological Monitoring. VPA has been conscientiously sharing its lessons with Federal agencies and other ports. VPA submitted a report to TSA in March 2003 covering the outcome of its extensive testing of radiation sensors and the operational issues identified during those tests. That report was followed by several briefings to various Federal and state officials in 2003 and 2004. The DHS RPPO was briefed on the VPA radiation monitoring program, response protocols and lessons learned in May 2004, providing RPPO with valuable insight for their two pilot programs in New York and Charleston. RPPO members and other Federal officials have visited NIT to inspect VPA radiation monitoring equipment.

Three lessons learned by VPA during its three and one-half years of testing and operational experience with radiological monitoring are particularly important. First, radiation monitoring is particularly difficult in the port and maritime environment. Despite the claims of suppliers, radiation equipment does not perform well in harsh environments when background radiation is highly variable, when radiological and nuclear devices must be distinguished from the numerous legitimate sources of radiation encountered every day, and when the manner in which cargo is shipped today—in sealed containers carried in large numbers on large vessels—offers ample opportunity for terrorists to shield and mask a radioactive shipment. Careful research and testing is required to make sure the right radiation detection

equipment is procured and that it is deployed and employed properly. Even the best equipment will fail if not placed in the right location or if not used properly for its intended purpose.

Second, effective protocols for responding to detection of radiation are critically important but difficult to develop. Response procedures are complex, involving a large number of Federal, state and local agencies. Additionally, the procedures for responding to detection of radiation in a shipping container are much different from other radiological emergencies because authorities have time to plan and execute precautionary measures in case efforts to disarm the radiological device fail and it detonates. For example, state and local authorities must decide whether a precautionary evacuation of residents near the terminal is warranted.

Third, radiological emergency exercises are crucial for protecting America's ports and port communities. If national strategy is to make every effort to halt terrorist radiological or nuclear devices in America's ports, then those ports should be given high priority in national exercise plans. For Hampton Roads, the VPA radiological monitoring program potentially increases risk to the Port's local communities. Port communities are literally on the front lines in the effort to protect America's heartland against the threat of radiological and nuclear terrorism. These communities must be ready for that threat, which can only be achieved through demanding training and exercises.

All of these lessons are applicable to every U.S. land, air and sea port of entry in which CBP will be monitoring inbound containers and cargo for radiological and nuclear devices. They also shed light on the challenges that DHS will face as it establishes the newly created Domestic Nuclear Detection Office to better coordinate the national effort to protect America against radiological and nuclear devices.

CONCLUSION

Security is clearly one of the most important issues facing U.S. ports now and in the future. Striking the right balance between the pursuit of commercial interests and the need to ensure the public's safety presents an enormous challenge to all stakeholders in the maritime industry—from citizens to businesses, shippers, railroads, truck lines, and ultimately to ports.

We believe that The Port of Virginia is among the ports that lead the nation in facilitating safe trade, but we are also aware that future ongoing security programs and needs will become a financial burden and will compete with expansion and development expenditures that are crucial to keeping commerce moving through the Port.

Security costs will certainly continue to rise, and it is critical that we work toward a common framework to address the issue of security-related expenses and ensure that security does not become a competitive issue between ports. The ship lines argue, and rightfully so, that charging them for security is unfair because the cost should be shared by cargo owners, truckers, rail carriers, stevedores and others who use ports. If you extend that logic, you see that the entire nation benefits from ports, even people who live thousands of miles away from the coast.

Federal Port Security Grants have certainly helped to improve port security, and we feel that additional funding in the future is appropriate and essential. Nonetheless, the fact is that Federal security grants will never cover all security costs incurred by ports, and until this issue is resolved, ports will continue to be put in an untenable position.

The Virginia Port Authority's experience with port security and radiation monitoring offers important lessons for enhancing U.S. homeland security. Much progress has been made enhancing the security of America's ports since September 11, 2001, but much more remains to be done. Now is not the time for complacency. As the leaders of the U.S. intelligence community testified before Congress last month, the terrorist threat to America is growing and it is not a matter of *if,* but *when,* they attempt to attack our nation with weapons of mass effect. America's ports are on the front line of the efforts to protect the United States against that threat. They take their responsibility seriously and are dedicated to doing the best they can to protect America. They have earned your support. I urge you not to let them down.

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

Mr. COBLE. We've been joined by the distinguished gentleman from Texas, Mr. Gohmert, and since only Mr. Scott, Mr. Gohmert, and I are here, we can probably have a second round, but we're going to have to go vote first. I think I'm going to go ahead and

ask my questions now. I think I can get my 5 minutes in before I go over there. I want to see how many votes there are going to be. I assume there's only one—one vote. So let me ask my questions, we'll come back, and I'll recognize Mr. Scott at that point.

Mr. Ahern, what resources and capabilities have been added by Customs and Border in order to reduce the vulnerability of ports and port facilities?

Mr. AHERN. What we continue to build upon is our layered strategy. As we look at increasing the security supply chain, we now have over 8,800 companies involved with C-TPAT and it's our determination that we need to get as deep as we possibly can in the supply chain, do verifications and validations in those environments. So that's part of the strengthening mechanism we're building upon our current program with Customs-Trade Partnership Against Terrorism. So we're building upon the existing layers that we have.

We're also looking at expanding beyond the current 34 ports that we have for the Container Security Initiative. As we take a look at—you know, we certainly rolled out initially to the top 20 megaports, making sure that we had over two-thirds of the Sea containers in those 20 ports. We then went to strategic locations and also locations where countries had the political will and the abilities to engage with us and support us in this binational program for container security.

As we look beyond the 34 ports, we now are down to the point where every one of the ports that remain that we would be targeting to deploy our resources is 1 percent—less than 1 percent of the universe of containers that come in from those locations. So we're now picking very specific and strategic locations based on threat and based on intelligence as we deploy there.

The other thing we're looking at now tagging as a part of this is global standards. Commisssioner Bonner, through the World Customs Organization, is challenging 164 members of the WCO to globalize the standards. We believe very strongly there should be one set of data elements required from carriers and from individuals involved with transmitting information to the Government agencies that would then have the ability to analyze that through a national targeting-type centralized targeting center, use expert-type rules as we build through the automated targeting system, and then make good risk-based determinations. We also believe countries involved with this should also have a similar supply chain type of security program, as well, to complement that.

Mr. COBLE. Mr. Ahern, are crew members of cargo vessels vetted against terrorist watch lists?

Mr. AHERN. We do have a program that we're actually working collaboratively with the Coast Guard where we're getting information in advance, electronically conveyed. I'm sure Rear Admiral Hereth would like to talk about the 96-hour rule and how we're getting it through the ENOA process.

Mr. COBLE. All right. Why don't you pick up on that, Admiral.

Admiral HERETH. Yes, sir. All the crew members for every foreign vessel that comes to the United States are vetted through the system against the databases prior to entry. As you know, there's a 96-hour notice of arrival requirement now on the books for all

vessels coming to the United States greater than 300 gross tons, all the large vessels. We vet all those crew members and take action. That information is passed to the local Coast Guard field unit for action as the vessel approaches the United States.

Mr. COBLE. I'll tell you, let's suspend right now. I've got a couple minutes left to go. We will return imminently, so you all rest easy in the meanwhile.

[Recess.]

Mr. COBLE. Okay, Admiral, you pick up where you were. We'll resume now. Or do you remember where you were?

Admiral HERETH. Yes, sir. I believe the question was on notice of arrival, and——

Mr. COBLE. Right.

Admiral HERETH.—we do receive vessel, cargo, and crew information 96 hours in advance, and all that information is vetted through a variety of systems and databases to look for anomalies. We work in conjunction with CBP, looking for any potential problems and then act on those problems at the local field operations level.

Mr. COBLE. Okay. Mr. Scrobe, by adding cargo crime to the Uniform Crime Reporting, how will that address this issue?

Mr. SCROBE. First of all, I think there would be much more accuracy and allow for better information and deployment of resources, there's no doubt about it. It would also give us a true number and be able to point out anomalies, like I said before, about where there may be terrorist activities involved.

Mr. COBLE. Mr. Keever, what areas do you see a need for improvement in strengthening the cooperative efforts among the Federal Government, local port authorities, and the private sector?

Mr. KEEVER. Mr. Chairman, I think what would strengthen that would be a steady Federal funding stream to ensure adequate funding for our nation's security at seaports.

Mr. COBLE. Let's see. My two colleagues are not here, so let me add one. I still have a little time left.

Admiral, let me come back to you. Since 2001, the Coast Guard has been a member of the intelligence community. Describe, if you will, how this membership has directly or indirectly supported the Coast Guard's port security efforts.

Admiral HERETH. Yes, sir, I'll be glad to. Let me just add one thing to what Mr. Keever said, if you would, Mr. Chairman.

Mr. COBLE. Okay.

Admiral HERETH. I'd like to just say that the relationships between the Federal agencies, State and local and private sector are key to preventing an incident on the waterfront and to ensure that there's good collaboration occurring on all the port authorities. We've established these Area Maritime Security Committees around the country. Presently, there's 43, one in each major port area around the country, and we think that's a powerful way in which to draw the stakeholders together to talk about security in their back yard and address vulnerabilities and address potential threats as they're changing.

Now let me jump over to your question, sir. The intelligence community membership of the Coast Guard is an absolute key in our mind. It feeds direct operational, actionable information directly to

our field operatives throughout the country so they can act on it and queue up resources in a way that allows us to deal with our limitations, but allows us to focus on the highest-risk targets, and those targets are constantly changing depending on the safety, environmental protection, and security challenges that face us.

And so it's really important that we have a good intel arm of the Coast Guard constantly focused on gathering information, staying connected to the intel community and all the members, and leaning on that direct access to information that we can then pump immediately out to our field operational commanders.

Mr. COBLE. I thank you, Admiral. My time has expired.

I recognize the gentleman from Virginia.

Mr. SCOTT. Thank you, Mr. Chairman. I'd like to ask all of our witnesses——

Mr. COBLE. Mr. Scott, if you'll suspend just a moment, I'm told that there will be another vote in about 30 minutes, so I think, if Bobby and Louie and I are the only three here, we may do another round. Go ahead, Mr. Scott.

Mr. SCOTT. Thank you. I'd ask all of our witnesses whether or not all of the ports—obviously, all of the ports don't have the same level of risk—whether or not the present formula allocates the funding for port security grants in an intelligent way.

Mr. AHERN. If you'd like, I'd begin first. I would first state that within Customs and Border Protection, we don't have any grant authority that we actually deal with State and local governments or port authorities for granting money.

But in answer to your question about the risk presented at different ports, I would tell you that certainly, we take a look at risk from a national perspective, and it's not necessarily the ports of arrival here in the United States, we believe, as far as—it's the origin of that supply chain and the beginning of that transit of cargo or seaborne containers coming into the United States. So we believe strongly that a lot of the emphasis should continue to be placed at the point of stuffing, at the point of lading in the overseas, and I believe it still needs to be complemented by a very strong port security structure here in the United States, as well, to make sure that we have good safe and secure environments when an offloading occurs of a container cargo vessel coming into this country.

Mr. SCOTT. Does anybody else want to comment?

Admiral HERETH. Yes, sir. I would just have to agree with you that we think that risk is the right dimension to focus on. Risk has a lot of variables, though, and all dimensions of risk need to be considered, not only the threat to a piece of infrastructure, but also the consequences of the loss of that infrastructure or the loss of that system, and so throughout the process, in our support to TSA that had original grant authority for port security grants and now our Office of Domestic Preparedness, we have supported that initiative, supported those initiatives, and supported the concept of risk-based approach to grants. Let me just stop there.

Mr. SCOTT. Mr. Scrobe?

Mr. SCROBE. Quite honestly, Mr. Scott, we don't really deal with grants or issues on this, so——

Mr. KEEVER. Congressman Scott, we have been the recipient of four grants and the process has served the Port of Virginia well.

The concern we have is that the existing, or the next round of grants has been delayed, and, of course, that delays us being able to implement the next phase of security, or level of security that we'd like to implement in Virginia. So the grant process has served us well thus far.

Mr. SCOTT. Mr. Keever, the seaports are pretty much left to their own device on security whereas airports and water patrol and borders get substantial underwriting from the Federal Government. Should ports have much more of the cost of security borne by the Federal Government?

Mr. KEEVER. Congressman, as I indicated, we have spent $22.4 million on security in Virginia. Half of that has been of our own money, the other half from grants. It appears that this is being handled somewhat differently than aviation and border crossings, and to have a steady funding stream from the Federal Government to provide for the adequate security at seaports, we think would be essential to ensuring the security of our nations. The burden has been placed squarely on the shoulders of the maritime security.

Mr. SCOTT. Well, and the port security grants can be used for procurement and installation purchases. Can you use it for personnel?

Mr. KEEVER. Unfortunately, it's only for the procurement of capital expenditures, and in Virginia, our cost of security has risen from $4 million annually pre-9/11 to over $6 million post-9/11, and those costs will continue to rise. It's very manpower-intensive, labor-intensive to continue to monitor these security levels that have been put in place, and that would be helpful if the grants could be modified to provide for the O&M costs of security.

Mr. SCOTT. So after you buy new equipment, you're pretty much on your own for the personnel, for the ongoing costs?

Mr. KEEVER. Absolutely.

Mr. SCOTT. Mr. Chairman, if we're going to have another round, I'd just defer now.

Mr. COBLE. We've been joined by the distinguished gentleman from California, Mr. Lungren. You are recognized for 5 minutes.

Mr. LUNGREN. Thank you very much, Mr. Chairman. I'm sorry I was late. We were at a briefing on the Homeland Security Committee about homeland security, and so now I'm here.

The panelists may not know it, but I used to represent two ports of Long Beach and Los Angeles, where I grew up. I've been gone for 16 years. I'm 400 miles away now, so I don't have those ports, but I still have an interest in those ports.

What strikes me as we go to all these homeland security briefings and meetings and exercises is we can't—we don't have enough money to do everything that we would like to do. And I've said before, when you try and do everything, you end up not doing anything very well. The ports seem to be a major concern that we have, I think rightly so. But now we come down to the question of paying for it.

Mr. Keever, what's wrong with the concept some have brought up that we sort of use a user fee, a per-container cost that would go directly into that security cost?

Mr. KEEVER. A uniform user fee across the board that could be applied at all ports would certainly be a concept that could be help-

ful in a Federal funding stream. One concern that we have is that not all cargo moving in and out of this country moves in containers. There are break-bulk and bulk and tanker vessels that carry, a variety of cargo that would have to be considered where some sort of a user fee would have to be applied uniformly without economically disadvantaging that type of commodity moving through the U.S.

Mr. LUNGREN. Mr. Ahern, are you allowed to venture an opinion on that?

Mr. AHERN. I would say it's probably safer for me not to comment on user fees and the—— [Laughter.]

Mr. LUNGREN. See, here's the problem. We've got a tough budget. We've got this. No one wants to give up what they already have. Everybody can point to the inadequacies we have in Border Patrol, what we are doing on the ports and so forth, and I'm trying to figure out, if we're really serious about this, how we go about paying for it because it's going to cost money.

Admiral, if you might respond to this question, what do we say to the average citizen about port security? I mean, I can't honestly tell anybody that even if we spent the entire Federal budget, we could ensure absolutely that we would have total security in our ports. The only way we could have total security in our ports is to get rid of the commerce, which sort of defeats the purpose but allows the terrorists to win by indirection what they can't win by direction. We rely on the commerce that goes through our ports. We're proud of it. The whole idea about "just in time" in our economy is predicated on the assumption that our ports are going to be open, working, and available to people.

So short of closing them down, I can't guarantee 100 percent. But what can we say? What can we—what could you tell me to say to some folks at my next town hall meeting when they ask me about the threat that is, the threat that remains to the United States with respect to our ports and what we are capable of doing in terms of applying some modicum of security to our ports?

Admiral HERETH. Yes, sir. I would pick up on your theme of—first of all, I think we deserve to be proud of a transportation system that provides such a huge benefit to the quality of life and our economic system of the United States, and then reflect on the fact that port security is something that we have to collaborate on. It's not one organization, one agency, one company that's going to solve all the problems and prevent an incident from occurring. And if we recognize the value of the system to the United States and emphasize that it's everybody's responsibility and that we have to collaborate on it, then I think we can explain the systems that are in place to do that.

We have put—an immense change has been laid out there and industry has responded very well past this first year law, this big implementation period of MTSA throughout the country. And actually, the international code now is implemented throughout the world. To put those new standards into place at port facilities on our vessels throughout the United States and throughout the world is a significant state of progress.

Couple that with the intense developments on the intelligence system looking for prevention of problems, looking at changing

threat streams so that we can respond and hopefully deter an act of terrorism before it occurs.

And then thirdly, I think part of the implementation of those systems, one of our threads of important must-haves was to develop a culture of security. So we now have security officers on vessels, in companies, and on facilities around the country. That's a whole network of eyes and ears out there of people that should be able to inform the intelligence system and the agencies about potential problems, and we get constant threat streams about pre-incident surveillance kinds of activities and other things that might be a concern that are brought into the system that we need to then be able to connect the dots and act and feed information out to those that own the infrastructure so we can better protect it.

So I think the good news is that we've done—we've taken a number of steps forward. We have a lot of people now that are charged with security responsibilities around the country. And if we work together as system, companies, organizations, and agencies, I think we'll have a good chance of preventing an incident in the maritime mode of transportation, and then underscoring how important that is.

Mr. LUNGREN. Thank you.

Mr. COBLE. I thank the gentleman.

I think we have time for a second round. Gentlemen, 2 days after 9/11—I may have told Mr. Scott this—a reporter asked me what my greatest fear was regarding a subsequent attack, and I'm sort of extending Mr. Lungren's comment. I said my greatest fear is that I fear that the next attack will be by water, harbor or port, and you four gentlemen are in a position, and hopefully we in the Congress are in a position to make efforts to make that less likely, but they're vulnerable by their very nature.

Mr. Scrobe, what voluntary steps has your industry undertaken to improve cargo security? I don't think we've touched on that yet.

Mr. SCROBE. Well, I think, Mr. Chairman, is that most importers and exporters, from the insurance perspective, and when we look at our importers and exporters, the first thing we ask them, are you C-TPAT compliant, which means that they have a working knowledge of what their system supply chain is all about. And I think most of the members within the ICSC do have that, and I think that was a major step moving forward. It gives more eyes to see what was going on at the borders and outside our country, which I think is the first step, like these gentlemen have mentioned before.

Mr. COBLE. Admiral, you've touched on this, but I'm going to give you a chance to do it more fully if you want to. Understanding that the Coast Guard has law enforcement responsibilities, what is its law enforcement role in protecting United States ports?

Admiral HERETH. Yes, sir. We see the Coast Guard as the nation's major maritime law enforcement agency, operating both all around the country and instituting protective measures on the waterfront throughout the maritime mode of transportation.

We have significant statutory authority in title 14 of the U.S. Code that gives us law enforcement authority. That's also recognized in a number of statutes, the Magnussen Act, the Ports and Waterways Safety Act that has now a security element to it, and,

of course, the Maritime Transportation and Security Act of 2002. So, yes, sir, we see ourselves as a law enforcement agency. We train people to those skills and we're out there every day.

Mr. COBLE. Thank you, sir.

The gentleman from Virginia?

Mr. SCOTT. Thank you. Admiral Hereth, you mentioned the 96-hour rule where the crew has to—you get the list of the crew. How do you know the names on the list are actually the names of the people on the ship?

Admiral HERETH. We check them out, sir. Part of our——

Mr. SCOTT. What do you mean? You check what out?

Admiral HERETH. When we receive the names, we—they're required to provide the name and passport number. All that information is vetted through against databases that we use in collaboration with a number of different agencies, law enforcement agencies and others, and then we have boarding teams that actually go on board those vessels as they approach the United States, and our control effort is centered around the implementation date around this first——

Mr. SCOTT. Let's say you verify the person has a passport and then you check the passport——

Admiral HERETH. Against that individual, and if it looks like the individual, that's what we're looking for. There is an initiative internationally to improve the biometrics and the documents that international seafarers use and we are fully supportive of adopting that as a new standard. We're trying to work out the biometric challenges, though.

Mr. SCOTT. Okay. Mr. Keever, you do a radiological check on all cargo that goes through. Do you get many hits?

Mr. KEEVER. Yes, sir, Congressman. This past year, in 2004, our radiological monitoring devices scored 1,000 hits, and while that seems fairly significant, we move approximately 20,000 containers through our gates weekly. So it's a small percentage of what goes through there. A number of those are hits that are non-cargo hits and CBP is not involved in that. We quickly move the containers out of the way for not to impede the flow of commerce. But we did receive about 1,000 this past year, yes, sir.

Mr. SCOTT. And was the cargo movement significantly impacted?

Mr. KEEVER. No, sir. We've developed standards to quickly move the affected container out of the flow, the traffic flow pattern, so that the other cargo can continue to move through, and we have some standard operating procedures in place with CBP if we receive a positive hit.

Mr. SCOTT. There's been a proposal to fold the Port Security Grant Program in the Targeted Infrastructure Protection Grant Program. Do you have any concerns about that?

Mr. KEEVER. We do, Congressman. By folding the Port Security Grants into the TIP would force ports to then compete with local, State, and other Government agencies for grant money and, therefore, make the available funds for ports diminished. So it would give us a lesser of a playing field.

Mr. SCOTT. Thank you. And I guess one final question, and whoever wants to answer it. With a port, you've got a lot of different agencies floating around. What are the various challenges in co-

ordinating activities with all of the different law enforcement agencies on the port and what do we do to make your life easier?

Mr. KEEVER. Well, I'll take a stab at that. We certainly have a good working relationship with CBP and Coast Guard. We have our own Virginia Port Authority police force that are sworn officers, as well as on the local level and the State level. The cooperation that exists through the Area Maritime Security Committee, as the Admiral referred to earlier, certainly has improved the communication among those agencies and we continue to do what we can to work together in a cooperative manner.

Mr. AHERN. I would add to that, also, as far as I would certainly go back to March 1 of 2003 when the Department of Homeland Security was created and we actually then had Customs and Border Protection, where we took all the different agencies that were operating within a port of entry, put them under a single leadership with single procedures so that when we do have changes in alert levels, we have the ability to have one organization responsible for that.

We also now have the other responsible agencies for port of entry—Coast Guard is one of our counterparts, certainly within the Department of Homeland Security. So we have better coordination just by our design and by our leadership. I think that's very critical.

There's been many entities involved with coordination of Port Security Councils as well as initiatives at our port, as well, for domain awareness.

Mr. SCOTT. Is there a satisfactory level of cooperation that we don't need—there's no problem for us to address?

Mr. AHERN. I think, certainly, there's always room to continue to improve, and certainly, we're still in a maturing process 2 years into our relationship in the Department of Homeland Security. But I would say it's not problematic. I think we've laid an excellent foundation we continue to build upon as we move forward in the future.

Admiral HERETH. Sir, let me just add that, again, underscoring the importance of the area committees to present a collaborative body in which all the stakeholders can meet and talk about security in their backyard is a very important theme to continue to foster and continue to focus our efforts around.

We're now in the process of mining best practices out of those area committees and intend to share those around the country, so I think it has to be viewed as a continuing process. We can't rest on our laurels. We've made good progress to this point, but a continuing discussion within those kinds of bodies is very important to making sure that we prevent an incident in the future.

Mr. COBLE. I thank the gentleman. The gentleman's time has expired.

Mr. Lungren earlier said that he'd been 16 years away from this place. The other day on the elevator, the operator looked at him and said, "Well, you haven't been riding my elevator in the last few months." [Laughter.]

Dan replied, "Well, I've only been away for 16 years." [Laughter.]

So I want to say to Dan, this Committee has missed you more obviously than the elevator operator has.

Mr. LUNGREN. I appreciate that. [Laughter.]

Mr. COBLE. I recognize the gentleman now.

Mr. LUNGREN. I thank the Chairman. I'm just glad she remembered who I was. [Laughter.]

And maybe I don't look that much older. I appreciate that.

Commissioner Ahern, can you tell me what the separation of ICE from CBP does to make you more effective with the ports?

Mr. AHERN. I would tell you that certainly we have a very strong relationship with Immigration and Customs Enforcement today, and we have principally the investigators there to follow up on crime or interdiction that actually occurs at the port of entry from an investigative standpoint. When the Department was created, certainly, an investigative arm did go to Immigration and Customs Enforcement. So we still do have a very strong relationship and a liaison between our two agencies and we're under one Directorate within Border Transportation and Security, as well.

Mr. LUNGREN. Isn't it kind of strange to have your investigators separated from your cops, to use an analogy to a police department?

Mr. AHERN. Well, that certainly is one point of view that was led to. Unfortunately, the separation that occurred on March 1——

Mr. LUNGREN. Well, I guess my question is, can you show me how that separation enhances the job that you do with respect to port security?

Mr. AHERN. If I could actually suggest that I defer answering that question until July of this year, because the Inspector General's Office will actually be doing a review of the ICE-CBP separation——

Mr. LUNGREN. I understand that, but I was just wondering if you could give me any idea that you have why it enhances our port security.

Mr. AHERN. I think——

Mr. LUNGREN. I mean, if you can't, that's fine, as well, but I'd just like——

Mr. AHERN. I think it's appropriate to wait for the July review to be concluded, sir.

Mr. LUNGREN. Okay. You started to answer this somewhat. Mr. Keever answered it. But Admiral, I'd like to ask this. One of my observations when I was Attorney General was the fact that there was at times a less than what I would consider to be a mutual respectful situation that existed between local law enforcement and the FBI, for instance. In some cases, it was good. In some cases, it was bad.

What is the level of cooperation that you have with local law enforcement? I come from a perspective in California where our ports have a distinct legal status. The Port of Long Beach, for instance, while the Port Commissioners are appointed by the mayor and the city council, the entity then is an independent entity that has some allegiance to the State as well as some allegiance to the locality and so they have, as you know, some of their own security, but there's also the City of Long Beach and there's the City of Los Angeles and there's the County of Los Angeles. If we were to have a major detonation in the harbor, it wouldn't just affect the port. It would affect the cities involved.

So what is the state of cooperation that you believe exists right now with your folks, the ports that you are directly working with, but the surrounding legal entities that you find yourselves involved with?

Admiral HERETH. Yes, sir. I would respond by saying I was Captain of the Port out in San Francisco in the Bay area during 9/11 and the relationship we had with local law enforcement and State law enforcement organizations was tremendous. I think it's only gotten better in the 2 years since I've left San Francisco, well, more than 2 years.

Mr. LUNGREN. Not because you left San Francisco Harbor. We wouldn't want to suggest that.

Admiral HERETH. The organizations that have been put together in terms of the Area Maritime Security Committee, the local exercise programs, the changes in some of the response protocols through the development of the National Response Plan and the National Incident Management System have all, I think, been favorable and fostered the development of a cohesive effort by State, local, and Federal law enforcement—State, local, and Federal law enforcement communities.

I would add that that's only going to continue to get tighter as we try to work for more defined prevention plans, whether it's a buffer zone protection plan around key infrastructure, and there's a variety of initiatives under HSPD-7 to do that. But it all suggests that the law enforcement communities have got to work together and lean on one another as they try to prevent incidents in a port area complex. There are many different players, as you know, that need to be involved in making sure an incident is prevented, and if something does happen, then a proper response from the law enforcement standpoint.

Most often, most of the port communities I've been at, and I've been stationed probably 10 years on each cost now, most of the port communities don't have all the resources they would like, and so the law enforcement communities have to band together to mount a proper response, in most cases, as you cascade on the resources and depending on the size of the incident.

The good news is we feel—the Coast Guard as an organization feels very comfortable working with the port communities on a broad variety of issues, and we've done that with our Harbor Safety Committees, our Area Pollution Response Committees, and now our Area Maritime Security Committees, and so it's a natural thing for us to reach out and pull in other agencies because we're resource limited, as many other agencies and organizations are, and so it's natural for us to draw into the mix and discussion with port authorities and local law enforcement authorities a game plan to help prevent incidents, and then if someone does happen, to be able to respond efficiently to one.

Mr. LUNGREN. Thank you, Admiral. I'm going to use that phrase that you used, "resource limited," when some people come and ask for different grants and programs. [Laughter.]

These last few weeks—that's a great phrase. I'm going to keep it.

Mr. COBLE. I thank the gentleman.

I thank Mr. Scott and Mr. Lungren for your input today. Gentlemen, I thank you all for your testimony. The Subcommittee very much appreciates it.

In order to ensure a full record and an adequate consideration of this very important issue, the record will remain open for additional submissions for 7 days. Also, any written questions that a Member wants to submit should be submitted within that same 7-day time frame.

This concludes the oversight hearing on law enforcement efforts at our ports of entry. Thank you for your cooperation, and the Subcommittee stands adjourned.

[Whereupon, at 4:26 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT CONGRESSMAN ROBERT C. "BOBBY" SCOTT

Thank you, Mr. Chairman. I am pleased to join you for this hearing on law enforcement efforts at our ports. The development of the Department of Homeland Security in the wake of the 9/11/01 tragedies brought about a shift of several law enforcement agencies from one department to another with changes and reorganizations of their responsibilities in some cases. There has also been a significant change in the responsibilities of federal law enforcement entities to communicate, coordinate and cooperate with state and local law enforcement entities. As a result, some confusion exists in the public, in the Congress and among the various federal state and local agencies as to where the oversight responsibility for these operations resides.

I am of the opinion that we should seek to clarify any such confusion by first asserting our jurisdiction over all federal law enforcement entities and then working with those entities to assist their coordination and cooperation with each other and with state and local law enforcement entities. So, I am pleased to join you in this first of a series of hearings we will be conduction in this regard, and commend your foresight and leadership in the matter.

I am especially pleased that we have Jeff Keever, Deputy Director of our Virginia Port Authority as one of our witnesses here today. Our ports are a vital part of the nation's economy, handling some 2 billion tons of freight each year. The Port of Virginia is the seventh largest U.S. port, in terms of general tonnage handled annually, and the second largest on the East Coast.

Operating alongside the nation's largest Naval base, and assisting the missions of the Defense Logistics Agency and the U.S. Transportation Command, security has always been job one for the Port of Virginia. Secure, smooth and efficient operations is not only critical to the deployment of our troops around the globe, but it is also why the port has maintained a robust annual growth rate of more than 9% over the past few years. As a part of its focus on security, the Port of Virginia checks 100% of the containers leaving the port with radiation detection and monitoring equipment before they leave the port on trucks. And as a result of its successful cooperative relationship with U.S. Customs, there has not been a theft at the port in about 8 years. That's quite a record of security when you consider that estimates of thefts from ports across the U.S. range as high as $30 billion annually.

Yet, despite the fact that our ports have risen to the challenges, their ability to continue to meet them in a world of changing threats and circumstances will depend in large measure on our assistance and support. I am concerned, Mr. Chairman, that we have not been as generous and diligent in supporting our seaports as we have with our airports and our land border crossings. It appears that we have left a much larger share of that responsibility to the ports themselves, compared to what we have done to assist our airport and border crossing operations.

I expect we will hear more about the details of what we can do from our witnesses. So, I look forward to their testimony and to working with you, Mr. Chairman, in clarifying the oversight responsibilities for the various federal law enforcement entities, and in strengthening our ports to do the vital job of securing and efficiently moving cargo and people. Again, I appreciate your leadership on these important matters. Thank you.

RESPONSE TO QUESTIONS FOR THE RECORD SUBMITTED BY COMMISSIONER JAYSON AHERN,U.S. CUSTOMS AND BORDER PROTECTION

1. Are the port facilities more secure since 9/11? What has CBP done since the 9/11 attacks to improve this security?

Answer: After the 9/11 attacks, CBP developed and implemented a defense-in-depth layered enforcement strategy. As part of this strategy, CBP developed numerous anti-terrorism and security programs and systems to identify and select high-risk cargo shipments, travelers, and conveyances. CBP understands that any single program or system can be defeated.

While we cannot physically examine all containers, we do review virtually 100 percent of all cargo shipments that arrive in the United States. This is possible through the 24-Hour Rule implemented by CBP in December 2002, which requires advance information for inbound vessel containerized and break-bulk shipments. The 24-Hour Rule, and later the implementation of the Trade Act of 2002, requires carriers to provide advance, electronic cargo declarations 24 hours before the cargo is laden aboard the vessel at a foreign port. Implementation of these regulations represented a significant change in the flow of information. This change allowed the United States to identify threats earlier in the maritime transportation process by being able to prescreen containerized cargo prior to being laden on board vessels destined to the United States.

Cargo manifest information provided to CBP is then reviewed electronically through the Automated Targeting System (ATS). Through ATS, CBP implemented threshold targeting which uses numerous rules that work in combination to vet shipment information from manifest and entry data, prioritize "unusual" shipments, and generate mandatory targets for shipments that exceed a specified score threshold. While the targeting rules primarily utilize historical shipment data to identify anomalies, all entities declared in the shipment data are also vetted against enforcement records.

Access to this data and the ability to vet it prior to lading supports another layer of CBP's strategy, the Container Security Initiative (CSI). Announced in January 2002, CSI is currently operational in 36 foreign ports—ports shipping the greatest volume of containers to the United States. CSI addresses the threat to border security and global trade posed by the potential for terrorist use of a maritime container. CSI proposes a security regime to ensure all containers that pose a potential risk for terrorism are identified and inspected at foreign ports *before* they are placed on vessels destined for the United States. CBP Officers are stationed abroad to work together with their host government counterparts. Their mission is to target and prescreen containers, utilizing the ATS and other available data, and to develop additional investigative leads related to the terrorist threat to cargo destined to the United States. Through the CSI, CBP is pushing our Nation's zone of security beyond our physical borders by working with nations from around the world to target, screen, and inspect high-risk containers that are bound for the United States.

After the events of 9/11, CBP began to leverage and expand existing industry partnerships. CBP developed the Customs-Trade Partnership Against Terrorism program (C-TPAT). C-TPAT aims at strengthening the international supply chain, from point of stuffing, through the CBP clearance process. Working in partnership with CBP, importers, brokers, carriers, port operators, and other C-TPAT members (partners) who initiate actions which further secure their supply chain receive measurable benefits from CBP, such as reduced inspections and expedited clearance times. C-TPAT members, now over 9,000, also report benefiting from the increased supply chain security by realizing more efficient supply chains, improved asset utilization, reduced total costs, revenue growth, and reduced pilferage.

To enhance our strategy at our borders, we have leveraged advanced non-intrusive inspection technology to examine a larger portion of the stream of commercial traffic while facilitating the flow of legitimate trade and travel. This technology includes large-scale, non-intrusive inspection imaging systems, radiation portal monitors, radiation isotope identifier devices and personal radiation detection devices.

With the help of these programs and systems, CBP officers can concentrate on searching for anomalies. The anomalies could range from discrepancies noted in the shipment information, irregular importer activity, discrep-

ancies in the density of a commodity, radiation emanations not consistent with the commodity, detection of irregularities within a container shipment, etc. Once an anomalous shipment is detected, our CBP officers can then physically search the shipment and determine whether the shipment has implements of terror or not.

2. What steps have been taken to increase coordination and cooperation with other DHS agencies, specifically the Coast Guard, to increase security of cargo arriving at US ports?

Answer: CBP has implemented several initiatives to increase coordination and cooperation with other DHS agencies, specifically the Coast Guard. These efforts include:

- Establishing agency liaisons at CBP's National Targeting Center (NTC) to streamline targeting efforts in homeland security. Agencies represented at the NTC include: Coast Guard, Transportation Security Administration (TSA), Federal Bureau of Investigation (FBI), Immigration and Customs Enforcement, and the Food and Drug Administration.
- CBP and Coast Guard have coordinated efforts to address industry in various forums to discuss port and cargo security. These forums include the Departmental Advisory Committee on the Commercial Operations of Customs and Border Protection and Related Functions, National Maritime Security Advisory Committee and various maritime conferences.
- CBP and Coast Guard have developed joint protocols and integrated operations such as targeting and conducting enforcement boardings in order to eliminate duplication of effort and leverage each other's capabilities and expertise. Critical U.S. Government work hours are now redirected and delays to industry have been reduced.
- CBP and the Coast Guard have been actively engaged in coordinating response protocols to address the threat of a nuclear or radiological weapon of mass destruction that could be smuggled into our country. CBP and the Coast Guard utilize a common radiological technical reachback (i.e., CBP's Laboratories and Scientific Services) to determine if a shipment contains illicit nuclear or radiological materials. This shared capability also provides for a thorough vetting of suspected shipments through both CBP's and the Coast Guard's information databases and watch lists.
- CBP and Coast Guard, with support from TSA, are conducting joint assessments of foreign ports to evaluate the port's level of compliance with International Ship and Port Facility Security Code (ISPS) requirements. During these joint site assessments, CBP addresses cargo security issues in CSI port operations or conducts site surveys of designated future CSI ports.
- CBP managers participate in the Coast Guard led Area Maritime Security Committees addressing port and cargo security measures and contingency planning.

DHS Agencies are also working in concert with the Department of Defense, in response to the National Security Presidential Directive - 41/Homeland Security Presidential Directive -13 (NSPD-41/HSPD -13), to develop a coordinated approach to securing the maritime domain which would assign specific responsibilities to appropriate agencies to ensure uniformity and avoid duplication.

Also in response to the NSPD-41/HSPD -13, CBP and Coast Guard, and other component DHS agencies, are working toward enhancing maritime domain awareness (MDA) and developing a common operating picture (COP) to better utilize information and maximize efficiencies and resources. Through MDA and COP, communication and coordination channels between CBP and Coast Guard are strengthened.

3. How would you describe the level of cooperation from the private sector thus far in implementing C-TPAT? What hurdles or obstacles need to be overcome in order to more fully implement the program?

Answer: Developed immediately after the 9/11 attacks, C-TPAT has grown from seven initial members to over 9,000 partners (members) as of April 2005, with an annual growth rate of approximately 3,000 new partners each year. The tremendous growth of the program is a clear indication of the significant level of cooperation from the private sector, and their commitment to partner with CBP to secure the international supply chain.

Moreover, C-TPAT members are conditioning contractual business relationships with service providers and vendors on participation and/or adherence to C-TPAT security guidelines, which is another strong sign of the level of cooperation from the private sector.

Staffing for this program was significantly increased in FY 2005 (120 new positions provided for conducting validations), which will allow CBP to conduct validations of all high-risk supply chains. CBP believes that the staffing increases and program adjustments made in FY05 (i.e., a modified validation approach that places emphasis on the importer and carrier sectors, maximizes resources and increases efficiencies) are sufficient to address the level of validations necessary of all high-risk supply chains.

4. How would you rate the success of the Container Security Initiative thus far? To what extent do you see it expanding to other overseas ports in the future?

Answer: To date, the Container Security Initiative (CSI) has been successfully implemented at 36 foreign seaports. The program has effectively extended our borders in regards to inspecting high-risk cargo destined for the United States. Prior to September 11, 2001, there was no program in place that applied the principals and security standards for maritime cargo that CSI employs today. Through CSI, a risk assessment is performed on every oceangoing container coming to the United States from a CSI port before it is loaded on a vessel. Additionally, CSI has been instrumental in enhancing port security. Through CSI, many foreign ports that previously did not utilize or possess non-intrusive inspection (NII) equipment now have either purchased their own NII equipment, or have access to such equipment. This has resulted in an increase in the effectiveness and efficiency of our targeting and examination process for inbound containers to the United States. Because of CSI, the probability of a terrorist organization exploiting the maritime environment to introduce weapons of mass destruction or disrupt the international supply chain is diminishing.

In addition to the current 36 operational ports, future CSI ports will be identified based on their strategic importance to international trade and volume of container traffic to the United States. Foreign ports with a large number of transshipped containers destined to the United, or ports located in countries with identified terrorists organizations, may be candidates for CSI expansion. CSI plans to be operational in 40 ports by the end of CY05 and 50 ports by the end of CY06.

5. Do you feel that CBP has adequate law enforcement authorities to adequately address the security needs of our Nation's seaports?

Answer: Congress has always empowered CBP Officers with broad border search authority. Under CBP or customs border search authority, searches of persons, conveyances, baggage, cargo, and merchandise entering the United States are allowed without a search warrant and without suspicion of criminality (see 19 USC 482, 1499, 1581, 1582). CBP Officers may routinely perform border searches to ensure compliance with all applicable laws bound of course by the reasonableness requirement of the 4th Amendment to the U.S. Constitution.

In addition to these authorities, CBP has been empowered by certain legislation that has enhanced our abilities to secure the seaports. For example, the Maritime Transportation Security Act of 2002 (MTSA) provides authority, in coordination with U.S. Coast Guard, to safeguard the public and protect vessels, harbors, ports, facilities, and cargo. Also, the Trade Act of 2002 ((PL 107–210) as amended by the MTSA of 2002) requires the electronic transmission of cargo information arriving and departing the United States for vessels (also includes air, rail and truck). The Enhanced Border Security and Visa Reform Act of 2002 required that electronic manifests for all vessel crewmembers and passengers be received by CBP up to 96 hours prior to arrival. These manifests are run against law enforcement databases, to include the terrorist watch lists.

6. Does CBP currently have adequate staffing and funding to ensure that 100% of hazardous cargo entering the United States is screened and intercepted when needed?

Answer: CBP employs a layered enforcement strategy to ensure that potentially dangerous merchandise does not enter the United States. Part of this strategy includes a requirement for key information on all cargo importations to be electronically transmitted to CBP prior to arrival at U.S. ports

of entry. The information is then screened by automated targeting systems and, if determined to be a potential threat to U.S. residents or commerce, the importation is subject to further review by CBP Officers. We are confident that our layered enforcement strategy effectively intercepts hazardous cargo entering the United States.

7. Please describe the level of cooperation that occurs between the federal government, local port authorities and commercial shippers to ensure the security of cargo entering U.S. seaports?

   A.Do you feel that it is adequate to address security vulnerabilities?
   B.What improvements can be made to bolster these cooperative efforts?

Answer 7: The tremendous growth of C-TPAT over the last three years is a strong indication of the private sector's commitment to partnership with CBP to secure the international supply chain.

- C-TPAT is not a regulatory program, but works through partnership with the trade community which leverages corporate strength and influence to push back security enhancements throughout the international supply chain, beyond the regulatory reach of the U.S. Government.
- Working in partnership with CBP, importers, brokers, carriers, port operators, and other C-TPAT members (partners) who initiate actions that further secure their supply chain receive measurable benefits from CBP, such as reduced inspections and expedited clearance times.
- As the program has grown and evolved, there has been a demonstrated need for more clearly defined, baseline security criteria as a condition of membership. After months of dialogue with the trade community, revised security criteria for importers were announced on March 25, 2005.
- The implementation plan is cognizant of concerns raised by the trade, and provides for a gradual, phased in approach to allow the trade additional time to enhance their security measures.
- Phase one pertains to the physical supply chain. Phase two relates to internal supply chain management practices, while phase three addresses business partner requirements.
- The Maritime Transportation and Security Act of 2002 (MTSA) required the establishment committees in our Nation's seaports to facilitate communication and coordination efforts of port stakeholders, including other federal, local and state agencies, industry and the boating public. These groups, called Area Maritime Security Committees, are tasked with collaborating on plans to secure their ports so that the resources of an area can be best used to deter, prevent and respond to terror threats. The USCG Captain of the Ports, acting as Federal Maritime Security Coordinators (FMSC), are responsible for developing Area Maritime Security (AMS) plans and establishing a local AMS committee.

The USCG, CBP, fellow federal, state and local representatives, and other maritime area partners participate on the USCG led AMS Committees to address maritime security issues. This coordination and cooperation is vital to our efforts to secure cargo entering U.S. seaports.

Answer 7 (A-B): While progress has been made, there is more work to be done:

- CBP will utilize a risk management approach and optimize all available resources.
- CBP will continue to work through international forums such as the World Customs Organization to implement a security framework that increases the security of the international supply chain.
- CBP will continue to work with other countries to internationalize the CSI principles and increase the amount of cargo, bound for the United States, that is inspected by those countries prior to departure.
- CBP will continue to work with the Department of Energy on the Megaports Initiative to provide foreign ports with radiation detection equipment.
- CBP will collaborate with the DHS Science and Technology Directorate in the development of an Advance Container Security Device and the Domestic Nuclear Detection Office in their research and development of radiation detection technologies.

- CBP will continue to strengthen its partnership with the private sector through C-TPAT, by sharing information with certified members more extensively, and developing more effective approaches to raising security standards, as well as facilitation benefits.

8. What nonintrusive technologies does CBP utilize to ensure that the stream of commerce is not unduly interrupted?

Answer: Non-Intrusive Inspection (NII) technologies deployed to our Nation's sea, air and land border ports of entry include large-scale X-ray and gamma-imaging systems as well as a variety of portable and hand-held technologies to include our recent focus on radiation detection technology.

NII technologies are viewed as force multipliers that enable us to screen or examine a larger portion of the stream of commercial traffic while facilitating the flow of legitimate trade, cargo and passengers.

As of mid-April 2005, CBP has 166 large-scale NII systems deployed to our Nation's air, land and seaports of entry. The systems include the Vehicle and Cargo Inspection System (VACIS), Mobile VACIS, Truck X-ray, Mobile Truck X-ray, Rail VACIS, Mobile Sea Container Examination Systems, and the Pallet Gamma-ray system.

CBP is also moving quickly to deploy nuclear and radiological detection equipment, including Radiation Portal Monitors (RPMs), Radiation Isotope Identifier Devices and Personal Radiation Detectors to our ports of entry. RPMs are very sensitive pieces of technology that allow us to seamlessly scan conveyances for nuclear and radiological materials.

9. How are CBP officers trained? Please describe the level and extent of this training.

Answer: Customs and Border Protection has established a comprehensive training plan for our officers. Carrying out the Nation's homeland security mission requires a workforce with necessary skills and proficiency to fight terrorist threats while effectively carrying out our traditional missions of interdicting drugs, intercepting illegal immigrants, and facilitating legitimate trade and travel. CBP was faced with the need to bring three distinct mandates together under the position description of one officer. The goal is to train the new CBP Officer to not only be equally competent in all of the former, individual areas of responsibility, but also to be better able to meet the expanded mission priority of anti-terrorism.

With the significant increase in the knowledge required for the CBP Officer, it was recognized that in order to not overwhelm the CBP Officers, it was necessary to develop a progressive roll out of training that allows officers sufficient time to assimilate the information into strong job task competencies, while building in sufficient personnel deployment controls to assure that the work was performed in a successful and timely manner.

The critical tasks required of the CBP Officer were identified and an instructional systems design approach was applied to build logic, simplicity, and progression into the training required to meet the wide diversity of duties performed by a CBP Officer. This diversity was further delineated as it relates to new hires as opposed to the incumbent workforce who were transferred from the legacy agencies.

From this perspective, training for new hires was divided into three major units: a 20 day pre-academy, a 73 day basic CBPI Academy at Glynco, Georgia and INPORT training which includes 37 modules of specific training to be delivered upon the students' return from the Academy, and prior to completion of their probationary period.

Training for all incumbent officers is ongoing. It incorporates many training methodologies to assist legacy officers in expanding their competencies within the new mission focus. The incumbent training also provides for in-service training of all officers on new or modified procedures or newly identified terrorist threats.

Currently, there are 37 different training modules being rolled out to cross train the front line CBP Officer and the Agriculture Specialists at air, land and seaports across the country. Twenty of these training modules are complete and available to the field in a variety of delivery methods. It is our goal to have the remaining 17 built and delivered to the field by December 2005.

Training has been built and will be delivered in structured stages so that training can be learned and absorbed before moving on to the next module. Cross Training will be delivered "just in time" based on operational needs of the agency. It is not our intention to roll out all training modules to all people, all at once.

There is a legitimate need to be sensitive to timing and delivery of training modules. Modules are staged based upon Headquarters ability to build quality training material and trainers, and the fields' ability to deliver the training as well as maintain effective port operations.

We are working towards creating an agency-wide law enforcement and national security culture, establish unified primary inspections at all United States ports of entry and conduct secondary inspections focused primarily on combating terrorism as well as the traditional missions inherited by Customs and Border Protection. To do this well and effectively, we have a built a comprehensive training plan to guide our efforts.

A very stringent 20-day pre-academy and 73-day basic academy training curriculum has been developed for the new CBP Officer. This training gives them the foundation that they need to work in the primary setting upon their return to the port, while also giving them a basic understanding of what occurs in the secondary environments. The ultimate goal is to train the new CBP Officer to not only be equally competent in all of the former, individual areas of responsibility, but also to be better able to meet the expanded mission priority of anti-terrorism. Their Academy training is then followed by a rigorous 2-year on-the-job training program with approximately 40-45 weeks (depending on environment - air, land or sea) of structured training courses. They are given training in stages in order to absorb it and be afforded time on the job to perform the duties and become proficient.

We do have several courses which we consider to be advanced training and they would include those that involve analytical capabilities and the counter-terrorism response units in our secondary areas. CBP is currently exploring the possibility of having additional areas and courses designated as specialized training classes.

10. What steps does CBP undertake that passengers and crew are adequately screened at seaport entries? Does CBP coordinate with the Terrorist Screening Center?

Answer: CBP rigorously screens watch list names from airlines and ships (both crews and passengers), destined to the United States transmitted in advance as mandated by law, through two systems, the Interagency Border Inspection System (IBIS) and Automated Targeting Systems (ATS). IBIS and ATS employ different algorithms to produce potential matches which require additional vetting either prior to or upon arrival.

Likely or positive matches are first coordinated with the Terrorist Screening Center (TSC), which serves as the government repository for watch list information, under HSPD-6, for the screening of names across all agencies of the United States Government. The TSC affirms the hit as a match, not a match or inconclusive. Both matches and inconclusive findings result in notification to the Counterterrorism Watch (CT Watch) at the National Counterterrorism Center (NCTC), which directs the Joint Terrorism Task Force (JTTF) squads around the United States. In a collaborative manner, decisions about both identification and admissibility are made between CBP and JTTF agents, though CBP alone exercises the authority to admit or refuse non-citizens at a Port of Entry (POE). Identification in advance, coordination with the TSC and CT Watch, and admissibility of all terror watch list cases at POEs are resolved through the CBP's National Targeting Center, which channels all field-level hits and maintains close communication with both TSC and CT Watch. In this way, there is a single CBP entity with awareness of all such hits at the more than 300 POEs in the United States, Canada, the Caribbean and Ireland.

11. Is there much overlap of responsibilities and duties with regard to port/cargo security between agencies in DHS? If so, is this overlap necessary? If so, why is the overlap necessary? If not, what, if anything, can be done to prevent this overlap?

Answer: Internally, CBP is addressing border unification and has implemented harmonized policies such as vessel boarding and the inspection of

goods and travelers. This allows for more efficient use of resources as the functionality of legacy agencies, immigration, customs and agriculture, is now being carried out through a single streamlined process.

In regard to overlap between DHS agencies, DHS continues to evaluate this issue. In the maritime environment, these roles and responsibilities will be further defined under the NSPD-41/HSPD-13.

12. Does each agency within DHS (or just CBP) have clearly defined responsibilities and duties in regards to port/cargo security?

Answer: Under the delegation of authority for MTSA of 2002, DHS has defined agency responsibilities for port/cargo security. The Coast Guard is the lead agency for waterborne/vessel and port facility maritime security issues. CBP is the lead agency for international cargo. TSA is the lead for Surface and Intermodal cargo security issues.

13. Is it possible to delegate some of your responsibilities and duties to other government agencies, especially at the state and local level, or perhaps even private agencies? Does C-TPAT impact DHS's delegation of responsibilities and duties?

Answer: CBP has unique border search authority and responsibility for the admissibility of goods and people arriving into the United States. This accountability is not something CBP would look to divert to other agencies or the private industry.

A voluntary, incentives-based program, C-TPAT works through partnership with the trade community, which leverages corporate strength and influence to push back security enhancements throughout the international supply chain, beyond the regulatory reach of the U.S. Government. In light of CBP's authority and responsibilities, this unique partnership is not one that could or should be delegated.

14. With regard to the trade act, how do you know the manifest data that is being transmitted to you 24 hours before shipment is authentic? Does CBP know the manifest data's point of origin? Does CBP know who is responsible for the manifest? Does CBP attempt to track any documents accompanying the manifest data?

Answer: The Trade Act requires that vessel carriers or automated Non-Vessel Operating Common Carriers (NVOCCs) provide CBP with an approved electronic equivalent of the vessel's Cargo Declaration (Customs Form 1302), 24 hours before the cargo is laden aboard the vessel at the foreign port. The current approved system for presenting electronic cargo declaration information to CBP is the Vessel Automated Manifest System (AMS). CBP has a multi-layer approach that involves the Automated Targeting System, Automated Commercial System and randomly selected vessel audits to validate cargo information with different enforcement processes. CBP electronically captures and retains the party transmitting the information to CBP by system identifiers and Standard Carrier Alpha Codes (SCAC) that are required in the transmissions. Automated parties are not required to have an office at each location of load to transmit that cargo information. In fact, most automated carriers have centralized office locations that are responsible for the transmission. There are many documents which make up a complete manifest in addition to the cargo declaration, which include: vessel entrance and clearance statements, ship's stores, crew effects, crew list, and customs and immigration forms which are presented at time of arrival. Vessel and cargo information is recorded in CBP systems.

15. Is there any warning system in place alerting the appropriate agency when any manifest or inventory data is altered?

Answer: The CBP automated systems track modifications and amendments to data that is transmitted. The automated system used by CBP also allows officers to mark cargo declaration information transmitted to CBP as reviewed. If the cargo information is changed after the review has occurred, the automated system will show the cargo information as not reviewed.

16. Can you use the automated targeting system (ATS) to preemptively try and find "high risk" cargo or known terrorists on board vessels? Do you do any kind of "date mining" with other government and private databases to try and preemptively prioritize cargo, ports, and personnel on board vessels?

Answer: The CBP Automated Targeting System (ATS) is designed to and does pre-emptively target high-risk cargo and known terrorists on board

vessels. The CBP cargo system collects electronic data from a variety of government and trade systems on all manifested cargo shipments. This is completed prior to the arrival of the vessel. Each shipment is risk-scored against the Terrorist Screening Center data base, law enforcement and violator data bases, as well as historical trade data. All high-risk shipments are examined by CBP Officers.

CBP continues to enhance its existing ATS program by leveraging ATS to integrate data elements from CBP systems and other commercial databases. CBP's cargo systems include commercial entry declarations, manifest, export, and enforcement databases. The CBP Passenger system includes all crew and passenger manifests via vessel (or aircraft) crossing the international border. Passenger and crew manifests are transmitted to CBP in advance of vessel arrival, and CBP works closely with the Coast Guard in assessing the risk posed by cargo vessel crew.

CBP uses this integrated data to risk assess and score existing cargo, crew, and passenger data. These scored events are evaluated against a pre-determined threshold to determine the intensity of CBP's interdiction. CBP also utilizes the Trend Analysis and Analytical Selectivity Program (TAP) to analyze and identify anomalies in trends and profiles of entry summary data. Based on operational risk assessment, comparison to historical crossing data, and matching against the Terrorist Screening Center data base and other law enforcement systems, an appropriate operational plan is developed and implemented.

17. How many private port facility operators are certified in C-TPAT? Approximately how many total private port facility operators are in the United States?

Answer: C-TPAT maintains statistics on a variety of enrollment sectors, but does not maintain the specific number of private port facility operators certified in C-TPAT. However, the following information is available: as of April 15, 2005, there are 26 certified Marine Port Authorities and Terminal Operators in the C-TPAT program.

CBP contacted the Federal Maritime Administration to obtain information on the total private port facility operators in the United States, but has not yet received that information.

18. How are federal funds currently distributed to ports throughout the United States? Any comment on Mr. Keever's suggestion that port security would be enhanced at a lesser cost by adopting a "focused" approach? According to page 23 of Mr. Keever's testimony, "under this approach, port facilities would be differentiated based on size, type, likelihood of being attacked and potential consequences of an attack, and the security standards they must meet would be tailored to their status based on these factors."

Answer: Federal funds are distributed through Port Security Grants (PSG) which are administered by the Office of Domestic Preparedness (ODP) branch of DHS. Seaports submit applications to be granted funds to enhance seaport security and these requests are reviewed by ODP. Seaports are presently differentiated based upon size, type and relative risk factors.

19. What are some ways you can secure our ports and cargo without an increase in funding or personnel?
    1. What about the creation of joint task forces to prevent duplication of responsibilities and duties by other agencies?
    2. What about delegating responsibilities and duties to other agencies; including local, state, and other federal government agencies, or even private companies?

Answer 19:

- CBP will utilize a risk management approach and optimize all available resources.
- CBP can continue to work through international forums such as the World Customs Organization to implement a security framework that will increase supply chain security of cargo in foreign countries.
- CBP can continue to work with other countries to internationalize the CSI principles and increase the amount of cargo, bound for the United States, that is inspected by those countries prior to departure.

- CBP will continue to work with the Department of Energy with the Megaports Initiative to provide foreign ports with radiation detection equipment.
- CBP will collaborate with the DHS Science and Technology Directorate in the development of an Advance Container Security Device and the Domestic Nuclear Detection Office in their research and development of radiation detection technologies.
- CBP will continue to foster partnerships with the industry and continue to strengthen voluntary, incentive-based programs such as C-TPAT.

Answer 19 (1):

- CBP has various liaisons represented at the National Targeting Center (NTC) to streamline targeting efforts in homeland security. Agencies represented at the NTC include: U.S. Coast Guard, Transportation Security Administration, Federal Bureau of Investigation (FBI), Immigration and Customs Enforcement, and the Food and Drug Administration.
- CBP often integrates operations with the USCG to target high-risk conveyances and crew and conduct joint enforcement boardings in order to eliminate duplication of effort and leverage each other's capabilities and expertise.
- In order to increase security at U.S. ports, CBP and the Coast Guard have been actively engaged in coordinating response protocols to address the threat of a nuclear or radiological weapon of mass destruction that could be smuggled into our country. CBP and the Coast Guard utilize a common radiological technical reachback (i.e., CBP's Laboratories and Scientific Services) to determine if a shipment contains illicit nuclear or radiological materials. This shared capability also provides for a thorough vetting of suspected shipments through both CBP's and the Coast Guard's information databases and watch lists.
- CBP and U.S. Coast Guard, with support from TSA, are conducting joint assessments of foreign ports to evaluate levels of compliance with International Ship and Port Facility Security Code (ISPS) requirements. During these joint site assessments, CBP addresses cargo security issues in Container Security Initiative port operations, or conducts site surveys of designated future CSI ports.
- At the field level, CBP has representation on the Federal Bureau of Investigation's Joint Terrorism Task Force as well as other multi-agency task forces addressing maritime security issues at the state and local level.

Answer 19 (2):

CBP has unique border search authority and responsibility for the admissibility of goods and people arriving into the United States. This accountability is not something CBP would look to divert to other agencies or the private industry.

20. Please list your top three priorities in securing our ports and cargo? Can you envision a way to accomplish these priorities without additional funding or personnel?

Answer: CBP's top three priorities:

1) Increase CBP's ability to access and evaluate advanced electronic information on cargo, travelers and conveyances in order to accurately identify and interdict those that pose a high risk to our Nation's security.

2) Partner with Foreign Governments and Trade Industry - Align security practices and develop security frameworks with foreign governments and continue to build partnerships with industry to improve supply chain security.

3) Utilize and Explore New Technology - Utilize NII technologies as a force multiplier to enable CBP to screen or examine a larger portion of the stream of commercial traffic while facilitating the flow of legitimate trade and cargo. Also, continue to evaluate new technologies that will increase the efficacy of examinations, the security of the end-to-end supply chain, and to integrate information to enhance targeting efforts.

The following are ways in which CBP can support seaport security:

- CBP will utilize a risk management approach and optimize all available resources.

- CBP can continue to work through international forums such as the World Customs Organization to implement a security framework that will increase supply chain security of cargo in foreign countries.
- CBP can continue to work with other countries to internationalize the CSI principles and increase the amount of cargo, bound for the United States that is inspected by those countries prior to departure.
- CBP will continue to work with the Department of Energy with the Megaports Initiative to provide foreign ports with radiation detection equipment.
- CBP will collaborate with the DHS Science and Technology Directorate in the development of an Advance Container Security Device and the Domestic Nuclear Detection Office in their research and development of radiation detection technologies.
- CBP will continue to foster partnerships with the industry and continue to strengthen voluntary, incentive-based programs such as C-TPAT.

21. Does the type of container inhibit inspection in any way? If so, how? Would a uniform container requirement help ease the burden of inspection?

Answer: CBP continues to strive to enhance our inspection capabilities through the evaluation and adoption of emerging technologies. CBP is currently able to scan a container efficiently and is not inhibited by the type of container.

22. How often is a cargo vessel coming into the United States required to take a physical inventory of its cargo? After the cargo vessel takes a physical inventory of its cargo, is the cargo vessel required to report its findings to anyone?

Answer: CBP requires that all cargo on board a vessel destined for a U.S. port of call whether or not to be discharged in the United States be transmitted in the Automated Manifest System to CBP. CBP does perform random validations of cargo transmitted to CBP compared to the cargo being discharged at the port of call.

RESPONSE TO QUESTION FOR THE RECORD SUBMITTED BY REAR ADMIRAL LARRY HERETH, DIRECTOR OD PORT SECURITY, U.S. COAST GUARD

SECURITY ASSESSMENTS

QUESTION:

Port facilities and vessels across the nation were required to submit a security assessment and a security plan to the Coast Guard to identify aspects of each port facility and vessel that were deemed vulnerabilities by July 1, 2004.

(a) According to a report entitled Secure Seas, Open Ports some 9500 vessels have submitted assessments and plans earlier this year. Has that number changed? What is the number as a percentage of vessels doing business in our ports? Additionally, the Report states that 2500 facilities submitted both a security assessment and a security plan earlier this Year. What is that number as a percentage of port facilities in the United States?

(b) How do these assessments and security plans help the Coast Guard's law enforcement responsibilities?

ANSWER:

The Coast Guard has reviewed and approved security plans for approximately 10,900 vessels. This number includes all vessels required to operate under approved security plans in accordance with the Maritime Transportation Security Act (MTSA) including approximately 1600 additional vessels required to comply under the new regulations designating ammonium nitrate as a Certain Dangerous Cargo. MTSA applies to almost all ships carrying packaged or bulk cargo. The rule excludes most of the U.S small passenger vessels because the rule applies to only those that have Safety of Life at Sea (SOLAS) certificates and those carrying more than 150 passengers.

Over 3,000 facilities have submitted security assessments and plans and currently operate under approved Facility Security Plans. This number includes all facilities, including port facilities, required to operate under approved security plans in accordance with MTSA as defined in 33 CFR, part 105.

These requirements support the Coast Guard's law enforcement responsibilities by requiring the use of facility and vessel security plans as a strategy to reduce maritime risk by establishing separate measures and protocols focused on preventing transportation security incidents and improving response if an incident occurs. Vessel and facility security plans must identify the qualified individual having full authority to implement security actions and also detail provisions for establishing and maintaining

- Physical security
- Passenger and cargo security
- Personnel security
- Additional security measures necessary to deter a transportation security incident.

WHAT HAS THE CG DONE TO IMPROVE SECURITY SINCE 9/11

QUESTION:

Are the port facilities and coastal areas more secure since 9/11? What has the Coast Guard done since the 9/11 attacks to improve this security?

ANSWER:

Our port facilities and coastal areas are significantly more secure now than they were prior to 9/11. Since 9/11, we've made great progress in securing America's waterways, while continuing to facilitate the flow of commerce. It is a complicated effort with broad strategic implications. To execute this strategy, we continue to focus on the 4 pillars of our maritime security strategy:

- Enhance Maritime Domain Awareness (MDA),
- Creating and overseeing a domestic/international maritime security regime,
- Increasing/enhancing operational presence, and
- Improving our response and recovery posture.

These pillars guide our transformation of Coast Guard authorities, capabilities, and capacity, with an eye toward reducing risk and preserving an appropriate mission balance. There is no doubt that work remains, but there is also no doubt that we continue to improve maritime homeland security each and every day. Although certainly not all inclusive, a few examples follow:

Enhance global MDA

• Before 9/11 there was no mandatory ship-tracking requirement; the Coast Guard has since forged an international agreement to accelerate the requirement for *Automatic Identification System (AIS)* capability that went into effect in December 2004. Simultaneously, we have initiated a major acquisition project to implement nationwide AIS capabilities allowing for deployment of immediate capability including AIS shore stations in VTS ports, outfitting NOAA buoys offshore, and testing AIS receiving capability from a low-flying satellite. The Coast Guard's fiscal year 2006 budget requests $29.1 million to further deploy AIS capability throughout the U.S.

Create & oversee maritime security regime

• Before 9/11 we had no formal *international or domestic maritime security regime* for ports, port facilities, and ships - with the exception of cruise ships. Partnering with domestic and international stakeholders, including the International Maritime organization, a comprehensive domestic security regime (Maritime Transportation Security Act (MTSA)) and an international security convention (International Ship and Port facility Security (ISPS) Code) we established July 1, 2004. The Coast Guard's fiscal year 2006 budget fully supports continued enforcement of MTSA regulations and ISPS code.

• Deployed field intelligence support teams to better collect and disseminate maritime threat information.

Increase/enhance operational presence

• Since 9/11, the Coast Guard has implemented several initiatives that have considerably increased operational presence, enhancing the Coast Guard's ability to protect the U.S. maritime domain, and prevent terrorists attacking. Initiatives include:

- Established *13 new Maritime Safety and Security Teams,*
- Deployed over *80 new small boats (RB-S) and boat crews,*
- Provided *radiation detection capabilities* to our boarding teams,
- Acquired *15 Coastal Patrol boats (the Coast Guard's 110' and 87' Cutters) and 4 Patrol Coastals* (These are the Navy's PC-170s which were transferred to the Coast Guard. Patrol Coastal is the Navy equivalent to the Coast Guard's Coastal Patrol) to increase operational presence in our ports.

• The Coast Guard's fiscal year 2006 budget continues to invest in initiatives focused on improving the quantity and quality of Coast Guard presence including:

- Continued implementation of Airborne Use of Force for Coast Guard helicopters,
- Permanent establishment of an enhanced MSST,
- 14 additional RB-S allowances, and
- Continued implementation of the Deepwater program including production of the third national Security Cutter, and design of the first offshore Patrol Cutter.

Improve response & recovery posture

• Since 9/11, the Coast Guard has begun establishing *Sector commands.* Sectors streamline command-and-control, provide unity of command, and one-stop shopping for port stakeholders and will have long term positive impacts on Coast Guard response and recovery posture.

• The Coast Guard is currently deploying Rescue 21 to replace the existing outdated National Response System. Rescue 21 will serve as the Coast Guard's primary communications system and will greatly improve interoperability with other Federal, State, and local agencies for the Coast Guard's fiscal year 2006 budget request $101 million to continue deployment of the Rescue 21 system.

CARGO SECURITY COORDINATION

QUESTION:

What steps have been taken to increase coordination and cooperation with other DHS agencies, specifically CBP, to increase security of cargo arriving at U.S. ports?

ANSWER:

DHS operating elements have exchanged liaison officers to facilitate information sharing for critical processes including among the Coast Guard's (CG) Intelligence Coordination Center Customs & Border Protection's (CBP) National Targeting Center, enabling timely and effective information sharing and analysis of cargo and vessel targeting data. As part of this effort, the CG and CBP have worked to harmonize their advance information requirements such that the advance notice of arrival information for vessels and cargo is not redundant and allows both agencies to coordinate the identification and tracking of high risk cargo and/or vessels. Similarly, ef-

forts are underway to ensure that results from the Coast Guard's International Port Security (IPS) program are available and considered as part of cargo targeting practices. The IPS program visits foreign ports in order to assess port compliance with the International Ship and Port Facility Security (ISPS) code, share best practices and help raise global port security postures. The CG's IPS program is also leveraging partnerships with CBP's Container Security Initiative (CSI) in order to coordinate visits and assessment results and provide as comprehensive a picture as possible of foreign port security. At the local level, the Area Maritime Security Committees are the primary mechanisms for government agency cooperation and coordination on port security matters. The CG Captain of the Port and CBP Port Directors are prominent members of these committees. Each provides agency staffs to participate on subcommittees and workgroups that serve to coordinate cargo inspections, joint vessel boarding operations, information sharing, contingency planning, and security plan exercises.

Though the Coast Guard coordinates with ICE on many issues, cargo security is primarily a CBP function but not one of ICE's. ICE is a member of Area Maritime Security Committees and as such is involved in the overall security discussions.

BIGGEST CHALLENGES RELATED TO MARITIME HOMELAND SECURITY

QUESTION:

What are the biggest challenges you're facing related to maritime homeland security?

ANSWER:

The Coast Guard's overarching goal related to maritime homeland security is to prevent terrorist attacks within, or exploitation of, the U.S. maritime domain. Doing so requires a risk-based approach to identifying and intercepting threats well before they reach U.S. shores by conducting layered, multi-agency security operations while strengthening the security posture of strategic economic and military ports. Specific challenges to conducting these operations are:

Coast Guard Recapitalization

- Readiness of Coast Guard surface and air fleet is a continuing challenge. The Coast Guard lost 742 Cutter days (10% of fleet availability) in 2004 due to major equipment casualties; the 110-foot patrol boat fleet suffered 20 hull breaches in the last three years; cutters and aircraft employ technology from the 1960's.
- In 2004, the Coast Guard was forced to begin an immediate re-engining of its HH-65 helicopter fleet because of an increased rate of in-flight engine power losses (329/100,000 flight hours, while the FAA/Navy standard is 1/100,000 flight hours).
- Despite spending over 50% more than budgeted amounts on maintenance and repair of legacy assets, the major Coast Guard Cutter fleet is forced to operate with degraded operational capability nearly 60% of the time.
- Continued recapitalization of surface and air fleet through the Deepwater acquisition is critical to current and future readiness. Department of Homeland Security (DHS) submitted the Revised Deepwater Implementation Plan to Congress, on March 25, 2005, which updates the program to include critical post-9/11 mission requirements and important new capabilities: airborne use of force, Department of Defense (DOD)/DHS interoperability, and enhanced cutter interdiction capabilities.
- The Coast Guard's fiscal year 2006 budget proposes significant investments in recapitalizing the Coast Guard to ensure the Coast Guard is equipped to meet its mission demands. Initiatives include:
  - $966 million for the Deepwater program will fund production of the third National Security Cutter, design and long lead materials for the first Offshore Patrol Cutter, six legacy cutter mission effectiveness projects, continued acquisition of Vertical Unmanned Aerial Vehicles, and complete re-engining of the Coast Guard's fleet of operational HH-65 aircraft;
  - $101 million for continued nationwide deployment of Rescue 21 - recapitalization of the Coast Guard's national distress and response communications system;
  - $22 million to continue the replacement of the Coast Guard's aging and obsolete 41-foot utility boat fleet with the Response Boat-Medium; and
  - $39.7 million to replace deteriorating shore facility infrastructure necessary to support the Coast Guard's operational assets.

Coast Guard Operational Presence & Response Posture

- The Coast Guard continues to strive to increase operational presence and response posture to reduce the risk of a maritime terrorist attack and to improve the Coast Guard's ability to minimize impacts on the maritime transportation system in the event an attack occurs. The Coast Guard's fiscal year 2006 budget provides resources for several initiatives focused on enhancing Coast Guard operational presence and response posture including:
  - $19.9 million to arm Coast Guard helicopters at five Coast Guard air stations, significantly improving the Coast Guard's ability to stop maritime threats;
  - $10.1 million to enhance cutter boat response by replacing obsolete cutter boats and failing small boat davit systems;
  - $11 million for 14 additional response boat-small allowances and Liquefied Natural Gas screening personnel to improve presence in key U.S. ports; and
  - Reallocation of $20.8 million of base resources to permanently establish an Enhanced Maritime Safety and Security Team to help fill gaps in U.S. maritime counterterrorism capabilities.

Maritime Domain Awareness

- Maritime Domain Awareness (MDA) is absolutely essential to both maritime security and defense operations and is the lynchpin to identifying threats as early and as far from the homeland as possible.
- Absent actionable cueing intelligence information, we hope to disrupt terrorists' planning and execution of operations, thereby deterring attacks, stalling them, or affecting their timing. Effective and integrated intelligence information analysis and dissemination assists in focusing the right effort against the right threat in the right location(s).
  - Recognizing the impossibility of defending against every vector of attack, external and internal, to the 3.4 million square miles of U.S. Maritime Exclusive Economic Zone, we must improve our level of awareness and knowledge of all maritime activities. Only then will we be able to facilitate decision making and enable an early and effective response.
  - In response to NSPD 41/HSPD 13, the Coast Guard, on behalf of DHS, is leading the effort in concert with DOD to develop a National Plan for MDA.
  - The Coast Guard's fiscal year 2006 budget continues the Coast Guard's aggressive implementation of comprehensive MDA capabilities. Initiatives include:
    - $29.1 million to continue nationwide implementation of Automatic Identification System capability.
    - $5.7 million to deploy the Common Operational Picture throughout Coast Guard regional command centers;
    - $16.5 million to provide additional C130H maritime patrol aircraft flight hours and establish a forward operating location to increase aircraft time on-station; and
    - $7 million to improve radiological/nuclear detection capabilities in conjunction with the DHS Domestic Nuclear Detection Office.

RESOURCES & CAPABILITIES TO REDUCE PORT VULNERABLITY

QUESTION: What new resources and capabilities have been added by the Coast Guard in order to reduce the vulnerability of ports and port facilities?

ANSWER:

Before the events of 11 September 2001, the Coast Guard had limited mandatory ship-tracking requirements. Since then, the Coast Guard has led the international maritime community in accelerating the requirements for vessels to carry Automatic Identification System (AIS) equipment. These international requirements, along with more extensive domestic requirements, went into effect in December 2004. Simultaneously, the Coast Guard initiated a major acquisition project to acquire shoreside AIS capability to improve Maritime Domain Awareness (MDA). Initial efforts under this project have allowed the Coast Guard to deploy AIS shore stations in various major ports and other coastal areas, outfit offshore National Oceanic and Atmospheric Administration weather buoys with AIS, and develop AIS receiving capability from a commercial low earth orbit satellite.

Before 9/11, the Coast Guard had no formal *international or domestic maritime security regime* for ports, port facilities, and ships - with the exception of cruise ships. Through partnering with domestic and international stakeholders, both a

comprehensive domestic security regime and an international security convention are now in place. Both have been in force since July 1, 2004.

In addition, the Coast Guard has increased and enhanced its operational presence by:

- Establishing 13 new *Maritime Safety and Security Teams,*
- Deploying over 80 new small boats *(RB-S)* and boat crews,
- Providing *radiation detection capabilities* to boarding teams,
- Deploying *field intelligence support teams* to better collect and disseminate maritime threat information, and;
- Acquiring 15 Coastal Patrol boats and 4 Patrol coastal vessels.
- Upgrading sensors for command and control in New York, Boston, Miami, Charleston, Hampton Roads, and San Diego.
- Establishing a national maritime Common Operational Picture.
- Developing maritime asset tracking technology for federal, state, local vessels.
- Expanding information sharing between the Coast Guard, other DHS components, Department of Defense, and other federal, state, and local agencies.

Before 9/11, Coast Guard prevention, protection, and response activities were coordinated by multiple commands in a single geographic location. Since 9/11, the Coast Guard has begun combining Group and Marine Safety Office commands into Sectors to streamline the Coast Guard's command-and-control structure, provide unity of command, and one-stop shopping for port stakeholders, and enhance the Coast Guard's response and recovery posture.

To further reduce maritime risk, the Coast Guard:

- Established Area Maritime Security Committees
- Reviewed and approved security plans for approximately 3,000 facilities and over 10,900 vessels, and;
- Completed port security assessments at the 55 U.S. ports previously identified as militarily and economically strategic.

The Coast Guard's fiscal year 2006 budget proposes continued investment in reducing vulnerabilities within U.S. ports by focusing resources to further enhance MDA and increase operational presence and response posture; critical elements of the Department of Homeland Security's Maritime Security Strategy.

NOA ACCURACY

QUESTION:

Under 33 CFR 160; subpart C, all vessels entering a U.S. port or place must provide a notice of arrival (NOA) 96 or 24 hours, whichever is applicable, prior to entering the designated port or place. Any vessel that fails to provide an NOA within the timeframe specified in the NOA regulation will be denied entry into port. The NOA must include among other requirements: A list of crew including nationality and their primary position on board; the name of the owner and operator; and vessel cargo information (i.e. general description of cargo on board other than Certain Dangerous Cargo (CDC) and/or list and amount of CDC carried). What steps have been taken to ensure the accuracy of security information provided by vessels as it relates to Notice of Arrival data?

ANSWER:

To ensure vessels comply with the Notice of Arrival (NOA) regulation the Coast Guard (CG) developed a strict enforcement policy that directs that no vessel shall be permitted to enter the designated U.S. port or place until all required information has been submitted to the CG within the time frames stipulated by the regulation. Upon receipt of the NOA information, the CG's Intelligence Coordination Center (ICC) vets the information against various databases to determine any anomalies with regard to vessel, cargo and people. CG and U.S. Customs and Border Protection (CBP) officers at CBP's National Targeting Center also assist in the vetting process. Lastly, CG and CBP personnel verify the validity of people, cargo, and vessel information during at sea and dockside boardings. Since July 1, 2004, every vessel arriving from a foreign port has been boarded at least once to verify compliance with the International Ship and Port Facility Security Code and to check the accuracy of their notice of arrival.

DOES THE CG HAVE ADEQUATE RESOURCES FOR MTSA?

QUESTION:

Does the Coast Guard have adequate resources (personnel and funding) to continue enforcement efforts under MTSA?

ANSWER: The Coast Guard was appropriated approximately $101 million in fiscal year 2005 to implement the Maritime Transportation Security Act of 2002 (MTSA). The fiscal year 2006 budget includes an additional $31 million for annualization of MTSA work, providing the Coast Guard with the resources required to enforce MTSA on an annual, going-forward basis.

MDA ENHANCEMENT OF PORT AND VESSEL SECURITY

QUESTION:

It is my understanding that the Maritime Domain Awareness (MDA) provides information regarding the maritime environment that could adversely affect America's security, safety, economy, or environment. Does MDA provide intelligence and information for law enforcement efforts to protect our ports? What are the Coast Guard's MDA efforts that demonstrate how the different initiatives under MDA enhance port and vessel security?

ANSWER:

MDA, an effective understanding of anything associated with global Maritime Domain that could impact the security, safety, economy, or environment of the United States, is a critical element of the Coast Guard's maritime security strategy. The Coast Guard has a number of efforts implemented and in progress designed to improve the effective understanding of the maritime environment to support operational commanders in targeting operational assets toward identified potential threats. These efforts involve:

Improved partnering between federal state, local agencies and maritime industry - The Coast Guard leads and coordinates Area Maritime Security Committees in all major ports. In some ports, the Coast Guard already hosts or participates in interagency command centers; a concept of operations being considered for expansion. Additionally, the Coast Guard is designing technologies that will improve partnering efforts such as a web client that will share the Coast Guard's Common Operational Picture with other waterborne agencies as well as make other important information available to industry, and "blue force" asset tracking that will allow all enforcement vessels to be aware of each others location and to be tracked by the local command center.

Long Range Vessel Tracking - The Coast Guard is pursing several initiatives to ensure we are able to track vessels that are more than 24 miles from U.S. shores. These include developing a universal reporting requirement through the International Maritime Organization, agreements made directly with other seagoing nations regarding vessels registered within their states, obtaining intelligence and other information from the Department of Defense (DOD) and the national intelligence community, and working with DOD to explore and support new technologies that would provide improved capabilities. Additionally, we have contracted for a satellite to be launched in late 2006 that will carry an AIS (Automatic Identification System) receiver which will allow the Coast Guard to monitor the positions of cooperating major cargo vessels in both the Atlantic and Pacific oceans. The Coast Guard has also deployed AIS receivers on oil platforms in the Gulf of Mexico, contracted receipt of AIS data from vessel operations from the Aleutian Islands, and are deploying AIS receivers on offshore National Oceanic and Atmospheric Administration data buoys to enhance long range tracking capabilities.

Short Range Vessel Tracking - The Hawkeye port sensors and operations test bed that the Coast Guard is operating in Miami in conjunction with the Department of Homeland Security's Science and Technology directorate is one example of the progress made with short range tracking. Information gained through this prototype effort is being applied to improve operations at the 11 ports where existing surveillance capabilities exist including Vessel Traffic Systems, and to develop standards and criteria for implementation of surveillance in other port and coastal areas. Additionally, the Coast Guard has deployed AIS capabilities enabling the monitoring 70% of compliant vessels on international voyages. To further leverage AIS technology, the Coast Guard has initiated a major systems acquisition, the Nationwide AIS project, to install capabilities to monitor 100% of the nation's navigable waterways, transform the supporting infrastructure from a patchwork of ad hoc connections to a reliable network, and to add historic and enforcement information to vessel tracks before displaying them in the Common Operational Picture. The Coast Guard's fiscal year 2006 budget requests $29.1 million to continue deployment of the Nationwide AIS system.

Information Fusion - The Coast Guard has several efforts underway to improve our ability to correlate information from various dispersed data bases and across levels of security. These include improvements to automated features that are a part of our Common Operational Picture, a cooperative effort with the states to allow enforcement officials access to recreational vessel registration information, and a multi-year effort with the Naval Research Lab to automate an number of laborious and time consuming analytical functions.

Intelligence - The Coast Guard and Navy continue to build an effective joint intelligence partnership to enhance maritime domain awareness. The Coast Guard's Intelligence Coordination Center (ICC) is co-located with the Office of Naval Intelligence, which comprises the National Maritime Intelligence Center. The ICC's COASTWATCH gathers and analyzes information on ship notice of arrival reports on vessels, people, and certain dangerous cargoes approaching U.S. ports. Additionally, the Coast Guard operates Maritime Intelligence Fusion Centers under each Area Commander, providing actionable intelligence to operational commanders and agency partners. Field Intelligence Support Teams operate in 29 U.S. ports and have increased the collection and reporting of intelligence and information. Through its Coast Guard Investigative Service branch, the Coast Guard Intelligence Program participates in Joint Terrorism Task Forces, Organized Crime Drug Enforcement Task Forces, and joint agency operations to share intelligence information with other local and federal agencies.

These Maritime Domain Awareness initiatives will allow the Coast Guard to better screen the people, cargo and vessels operating in the maritime domain and to discern the legitimate from the illegal owners/operators of vessels. It will also give us the ability to detect, and interdict suspected targets further from our shores, reducing America's maritime risk.

EFFICIENCIES GAINED RELATED TO CUSTOMS LAWS

QUESTION:

What efficiencies have been gained by the Coast Guard in the performance of your duties relating to Customs laws since the standup of the Department of Homeland Security? How does the Coast Guard work with law enforcement agencies outside of the Department of Homeland Security to protect the ports and vessels?

ANSWER:

The Coast Guard, U.S. Immigration and Customs Enforcement (ICE), and the U.S. Customs and Border Protection (CBP) are improving law enforcement in the port through a variety of coordination initiatives. Officers of the Coast Guard, ICE, and CBP are all "customs officers" pursuant to the Tariff Act of 1930 and, as such, share unique search, seizure, and arrest authorities that enhance cooperative efforts. CBP's border search authority, combined with the authority of customs officers to carry firearms and to make warrantless arrests for any federal violation occurring in their presence, vests customs officers with the broadest law enforcement authority in the United States. Moreover, customs officers are authorized to stop vehicles, and board vessels and aircraft without a warrant to perform customs inquiries and border searches. ICE special agents also have the authority to seek and obtain search warrants, court orders authorizing the interception of communications, administrative summonses, and are authorized to conduct undercover investigative operations in the enforcement of law. Any merchandise or conveyance involved in a customs violation is generally subject to civil forfeiture and may be seized by customs officers without a warrant. Cooperative vessel arrival screening, joint boarding and investigations, coordinated cargo screening, and aerial patrol scheduling are examples of activities that create efficiency and effectiveness.

Since the stand up of the Department of Homeland Security, the Coast Guard has established 43 Area Maritime Security Committees, which serves as the primary mechanisms for government agency security cooperation and coordination in America's ports. Each committee is comprised of Federal, State, and local agencies, law enforcement and security agencies, and other key port stakeholders. The committees develop and maintain local area maritime security plans, which provide a framework for communication and coordination amongst all of the appropriate federal, state, and local law enforcement agencies to carry out port security missions.

Coast Guard Operational Commanders also coordinate Ports, Waterways, and Coastal Security (PWCS) law enforcement operations afloat and ashore, to the greatest extent possible, with appropriate international, federal, state, and local authorities. If a potential PWCS threat or incident appears to exceed the capability of available Coast Guard resources, the Coast Guard seeks assistance from appro-

priate services and agencies. In 46 U.S.C. 70119, Congress explicitly authorized any State or local government law enforcement officer who has authority to enforce State criminal laws to make an arrest for violation of a security zone regulation under the Magnuson Act, or a security or safety zone regulation under section 7(b) of the Ports and Waterways Safety Act, or a safety zone regulation prescribed under section 10(d) of the Deepwater Port Act of 1974 by a Coast Guard official authorized by law to prescribe such regulations if: (1) such a violation is a felony; and (2) the officer has reasonable grounds to believe that the person to be arrested has committed or is committing such violation. This authority has helped the Coast Guard leverage the capabilities and willingness of State law enforcement partners in order to help augment our collective presence within and around security zones.

ADEQUATE LEGAL AUTHORITY?

QUESTION:
Does the Coast Guard have adequate legal authority to provide the necessary security in our ports?

ANSWER:
Yes. The Coast Guard has the necessary legal authorities to ensure the security of our nation's ports and waterways. We are constantly examining our authorities, and when it is determined that changes are necessary in order to meet our maritime security responsibilities they will be proposed as part of new legislation.

ADEQUATE NBC WEAPONS TESTING EQUIPMENT

QUESTION:
Does the Coast Guard have adequate equipment to inspect cargo for nuclear, biological, or chemical weapons at sea? Does such mobile inspection equipment even exist? If so, how much does the equipment cost? How difficult would it be to have the Coast Guard inspect vessels at sea?

ANSWER:
The Coast Guard (CG) has deployed varying levels of equipment to aid in the detection of nuclear, biological, and chemical weapons. Each of these threats is unique and the capabilities to detect them vary according to the threat. Below is a summary of CG capabilities:

Rad/Nuc - The CG has some capability to detect, localize, characterize and identify radioactive/nuclear (Rad/Nuc) materials through the use of personnel portable search tools. The current CG program is summarized below:

- CG policy and procedures have been developed to provide guidance for conducting operations involving the detection of radiological and nuclear materials.
- Designed around the concept that during the course of conducting traditional missions, Maritime Inspectors and Boarding Team members wearing Personal Radiation Detectors (PRDs) may discover the presence of a radiation source.
- Certain trained members may further investigate by using hand-held isotope "Identifinders" to rapidly assess and classify the source. Information gained is transmitted to the U.S. Customs and Border Protection's Laboratory and Scientific Services to ensure proper diagnosis. If doubt still exists, Department of Energy Radiological Assistance Program teams are called to assist.
- When intelligence indicates an elevated threat, the Coast Guard has the ability to conduct wide area searches using RadPacks - radiation sensors, larger than the PRD, with increased sensitivity and range - carried in a backpack worn by a boarding team member. RadPacks decrease the time needed to search large ships.
- The Coast Guard's Radiation Detection Program increases our organic capability and is specifically designed for the maritime interdiction of radiological and nuclear materials.
- 1300 PRDs ($2,650 each), 250 Identifinders ($16,955 each), and 38 RadPacks ($30,100 each) have been distributed to the field.

Chemical - Current technology precludes detection of chemical or biological threats prior to release. CG capability to detect chemical threats is limited to post-release detection with portable equipment.

- Personnel Protective Equipment (PPE) provided to Maritime Inspectors and Boarding Team members includes GasAlertClips (detects oxygen deficient environments), GasAlertMicro (gas monitor tests for oxygen, carbon monoxide, hydrogen sulfide and lower explosion limit), and Hazmat Strips (alerts crews to potential presence of weapons of mass destruction agents).

- National Strike Force units possess various portable chemical detection instruments for air, liquids, and solids and the ability to respond to most chemical incidents (with appropriate PPE).

Biological - Available technology precludes detecting Biological threats prior to release. CG Strike Teams are equipped with the necessary PPE to operate in a contaminated environment.

Future Plans:

- The CG will continue to develop long-range, standoff radiation detection capabilities through research and development efforts coordinated with interagency partners.
- Fielding additional radiation detection equipment (identifinders and backpacks) in Fiscal Year 2005, with funds appropriated in prior years..
- Implement a maintenance and logistics support plan to support field personnel.
- As part of the DHS Domestic Nuclear Detection Office proposal, the CG's 2006 budget request includes an additional $7 million for improved Rad/Nuc detection capabilities, including:
  - Enhanced Rad/Nuc detection & response capability for Coast Guard Strike Teams, E-MSST (Chesapeake), and MSSTs (San Diego and New Orleans).
  - Equipping our 378-foot and 270-foot cutters with Specific Emitter Identification (SEI) equipment - improving vessel detection and identification capability.
- The Department of Homeland Security recently approved the revised the mission needs statement of CG Deepwater recapitalization project to provide for Chemical, Biological, Radiological, and Nuclear Equipment (CBRNE) capabilities among all our aircraft and major cutters. The reality of this change will begin in 2007 with the delivery of the first National Security Cutter equipped with stand-off detection capability and capable of operating for extended periods of time in contaminated environments.

DELEGATING AUTHORITY TO OTHER AGENCIES

QUESTION:

Is it possible to delegate some of your responsibilities and duties to other government agencies, especially at the state and local level, or perhaps even private agencies? Does C-TPAT effect the Coast Guard's delegation of responsibilities and duties?

ANSWER:

No. The Coast Guard has a mandatory duty, pursuant to 14 U.S.C. § 2, to carry out law enforcement and assistance duties and, among other things, to promulgate and enforce regulations for the promotion of safety of life and property at sea. Thus, the transfer of Coast Guard "responsibilities and duties" to other federal agencies (or private entities), as a general proposition, is not consistent with federal law.

Pursuant to 14 U.S.C. § 141(b), the Coast Guard has authority to request and receive law enforcement assistance from other government agencies under certain circumstances. However, the Coast Guard's law enforcement authority cannot be transferred to, or used by, an assisting entity. Accordingly, each entity providing assistance must do so within the bounds imposed by relevant federal law, and the entity's own legal authority and policy, which in certain circumstances may permit the assisting agency to enforce federal law. For example, in implementation of merchant mariner credentialing program, the Coast Guard is working with the Transportation Security Administration for interoperability between the Transportation Worker Identification Credential program and the merchant mariner credentialing.

The President, pursuant to the Magnuson Act and 33 C.F.R. § 6.04–11, authorized Coast Guard Captains of the Port (COTP) to enlist the aid and cooperation of federal, state, county, municipal, and private entities to assist in the enforcement of regulations issued pursuant to 33 C.F.R. Part 6. A request for assistance under 14 U.S.C. § 141(b) or 33 C.F.R. § 6.04–11, and the acceptance of it, have no effect on the assisting entity's existing law enforcement powers. In other words, the assisting entity's organic legal authority and policy will dictate the scope of assistance it may provide. No law enforcement power is implied with, or derived from, the request for assistance from the Coast Guard.

The Customs-Trade Partnership Against Terrorism (C-TPAT) is an initiative focused on self-security (by private firms) of the commercial supply chain. This initia-

tive does not afford a legal basis for the Coast Guard to delegate any authority, function or responsibility to any other federal agency or non-federal entity.

CROSS TRAINING WITH INTERNATIONAL AGENCIES

QUESTION:

Are you currently involved in any cross-agency training or training of international agencies with similar missions? Do you think it would be beneficial to send Coast Guard personnel overseas (and to other agencies within the United States) to assist in training?

ANSWER:

The Coast Guard's International Port Security Program (IPSP) participates with the Maritime Administration in providing IPSP Training to Latin American nations through the auspices of the Organization of American States. In addition, the program participates with the Transportation Security Administration in the Asia Pacific Economic Cooperation Forum in a similar fashion. IPSP Program personnel have also acted as instructors at International Maritime Organization (IMO) regional training sessions, and are investigating whether or not participation in the Secretariat of Pacific Countries (a regional body involving the small independent Pacific Islands) is feasible. The program is working with the U.S. Trade Development Agency to identify potential training for countries in Africa. This training is beneficial to maritime security worldwide and should be continued.

Furthermore, while not strictly training per se, the Coast Guard provides technical expertise in port security to U.S. Customs and Border Protection (CBP) in the Container Security Initiative port assessments, the Department of Energy in their Proliferation Security Initiative port assessments, and the Department of State in their Maritime Needs Assessments.

AUTHORITY TO BOARD VESSELS

QUESTION:

Can the Coast Guard board a vessel and do an inspection or do you first need some kind of indication of an illegal activity? What kind of factors indicating illegal activity are necessary before you may board a vessel at sea and do an inspection? In light of 9/11 and increased terrorist threat, do you feel at all burdened by this standard?

ANSWER:

No indications of illegal activity are necessary for a Coast Guard boarding because 14 U.S.C. § 89 [1] permits, *inter alia,* Coast Guard "commissioned, warrant, and

[1] 14 USC § 89 is the principal source of Coast Guard maritime law enforcement authority It provides:

A. The Coast Guard may make inquiries, examinations, inspections, searches, seizures, and arrests upon the high seas and waters over which the United States has jurisdiction, for the prevention, detection, and suppression of violations of laws of the United States. For such purposes, commissioned, warrant, and petty officers may at any time go on board of any vessel subject to the jurisdiction or to the operation of any law of the United States, address inquiries to those on board, examine the ship's documents and papers, and examine, inspect, and search the vessel, and use all necessary force to compel compliance. When from such inquiries, examination, inspection, or search it appears that a breach of the laws of the United States rendering a person liable to arrest is being, or has been committed, by any person, such person shall be arrested or, if escaping to shore, shall be immediately pursued and arrested on shore, or other lawful and appropriate action shall be taken; or, if it shall appear that a breach of the laws of the United States has been committed so as to render such vessel, or the merchandise, or any part thereof, on board of, or brought into the United States by, such vessel, liable to forfeiture, or so as to render such vessel liable to a fine or penalty, and if necessary to secure such fine or penalty, such vessel or such merchandise, or both, shall be seized.

B. The officers of the Coast Guard insofar as they are engaged, pursuant to the authority contained in this section, in enforcing any law of the United States shall:

(1) Be deemed to be acting as agents of the particular executive department or independent establishment charged with the administration of the particular law; and

(2) Be subject to all the rules and regulations promulgated by such department or independent establishment with respect to the enforcement of that law

C. The provisions of this section are in addition to any powers conferred by law.

petty officers . . . at any time [to] go on board . . . any vessel subject to the jurisdiction or to the operation of any law, of the United States."

SECURING OUR PORTS WITHOUT INCREASING FUNDING

QUESTION:

What are some ways you can secure our ports and cargo without an increase in funding or personnel?

(a) What about the creation of joint task forces to prevent duplication of responsibilities and duties by other agencies?

(b) What about delegating responsibilities and duties to other agencies, including local, state, and other federal agencies, or even private companies?

ANSWER:

(a) The Coast Guard maximizes the effectiveness of its operational efforts through a risk-based approach to identify and intercept threats before they reach U.S. shores; through layered, multi-agency security operations nationwide, and through partnership with port officials and the private sector. The Coast Guard is employing this risk-based approach, including the emphasis on close coordination with other agencies and stakeholders, at the international, national, regional, and local level. These partnerships include maritime industry organizations, such as the International Council of Cruise Lines, the Passenger Vessel Association, and the American Waterways Operators. The Coast Guard also has a maritime community watch program called Americas Waterway Watch (AWW) designed to help citizens report suspicious activities. While personnel and other costs are incurred in establishing and maintaining AWW and the various other agency and industry partnerships, the resource demands are small relative to the benefits gained.

The Coast Guard also coordinates public and private maritime security efforts through Coast Guard led port-level Area Maritime Security (AMS) Committees. These Committees provide a forum for bringing the perspectives and capabilities of member organizations together to ensure that risks are identified, prioritized, and addressed while continuing to facilitate the safe and efficient flow of commerce. The primary purpose of AMS Committees is to develop an AMS Plan that will serve as a framework for communication and coordination among port stakeholders. These committees support formal coordination arrangements, such as the Joint Terrorism Task Forces developed and led by the Federal Bureau of Investigation. The committees also provide an avenue to organize task forces to conduct security related missions such as joint vessel boardings and other operations.

(b) The Coast Guard, as the lead Department of Homeland Security agency for maritime security, shares many port security responsibilities and duties with other federal, state and local law enforcement agencies as well as public and private stakeholders. This is consistent with the Maritime Transportation Security Act of 2002 (P.L. 107–295) which places primary responsibility for protection of privately owned port infrastructure on the owner/operator and requires owners of regulated vessels and facilities to conduct vulnerability assessments and produce individual security plans. Some private companies are hiring professional security services to assist with plan development, access control, security patrols and physical protection services. These responsibilities and duties are outlined in the AMS plan and coordinated through specific sub-committees of the AMS Committee. Further, the Coast Guard has agreements with a number of states detailing how each party will support the other's maritime law enforcement missions, including state and local enforcement of Coast Guard established safety and security zones. While the Coast Guard cooperates on port security with others as appropriate, the Coast Guard is not authorized to delegate its responsibilities, duties, or law enforcement authority to any other individual or organization, whether governmental or private.

TOP 3 CARGO SECURITY PRIORITIES

QUESTION:

Please list your top three priorities in securing our ports and cargo? Can you envision a way to accomplish these priorities in securing our ports and cargo? Can you envision a way to accomplish these priorities without additional funding or personnel?

ANSWER:

The top three priorities in securing America's ports and cargo are improving threat identification, reducing the vulnerability to terrorist acts, and mitigating the potential consequences of an actual terrorist incident.

The Coast Guard has taken, and continues to take action to address these priorities and further our collective national security interests. Through the provisions

of the Maritime Transportation Security Act, the commencement of critical security programs such as Maritime Domain Awareness and the Integrated Deepwater System, and implementation of the Coast Guard's maritime security strategy, America's ports and cargo are becoming less vulnerable to acts of terrorism. Continued investment in these programs through full support of the Coast Guard's fiscal year 2006 budget, and strong interagency cooperation to further these efforts is critical for their success.

The Coast Guard maximizes the effectiveness of its operational efforts and existing resources through a risk-based approach to identify and intercept threats before they reach U.S. shores; through layered, multi-agency security operations nationwide, and through partnership with port officials and the private sector. These partnerships include maritime industry organizations, such as the International Council of Cruise Lines, the Passenger Vessel Association, and the American Waterways Operators. The Coast Guard also has a maritime community watch program called America's Waterway Watch (AWW) designed to help citizens report suspicious activities.

The Coast Guard also coordinates public and private maritime security efforts through Coast Guard led port-level Area Maritime Security (AMS) Committees. These Committees provide a forum for bringing the perspectives and capabilities of these organizations together to ensure that risks are identified, prioritized, and addressed while continuing to facilitate the safe and efficient flow of commerce.

While personnel and other costs are incurred in establishing and maintaining AWW, AMS Committees, and the various other agency and industry partnerships, the resource demands are small relative to the benefits gained.

The Coast Guard continues to guide its efforts by implementing policies, seeking resources, and deploying capabilities through the lens of our maritime security strategy. However, continued risk reduction to America's ports and cargo is contingent upon Coast Guard readiness and capacity. Without these building blocks, implementation of maritime security strategies will not be sustainable.

RESPONSE TO QUESTIONS FOR THE RECORD SUBMITTED BY PETER SCROBE, MEMBER OF INTERNATIONAL CARGO SECURITY COUNCIL

1.) Yes, through education and training programs, specifically with the US Merchant Marine Academy (USMMA) - Global Maritime Transportation School (GMATS) and various seminars.

2.) The ICSC through seminars, conferences, and training w/USMMA GMATS.

3.) It varies based on industry groups and requirements associated therewith. Many believe we are headed in the proper direction, but much more needs to be accomplished.

4.) Enhancing the CSI program and continuing to push our borders overseas. Also, there is need to utilize existing technology (such as VACIS type) and other similar type equipment. Better allocation of resources and funding thereof. Incorporate risk management approach with minimum standards included.

5.) It is believed that among "friendly" nations, there is a mutual cooperation to provide necessary security, but still requires our (US) presence. On the private sector side, the ICSC has recently opened a European Chapter which appears to be growing steadily.

6.) Again, there is a need for the US to continue pushing out our borders. Continue to work on processes and phase in technology for support (more than one form of technology may provide the necessary requirements).

7.) The potential of a WME. There is, in my opinion, the need for constant vigilance and all parties pertaining to the Supply Chain continuing to focus on and upgrade security. This question should also be addressed, in more detail, by members of the Carriers and Port/Terminal personnel.

8.) We believe it has brought a greater awareness to all parties in the "Supply Chain". The C-TPAT document should continue to be strengthened to further enhance the process.

9.) Original figures in the early '90's, ranged from $3–10 billion in losses domestically and has steadily increased to the numbers indicated today. There have been studies completed by the FBI, Rand Group (for the hi-tech industry - o/o/a 1995) and the FIA Study (2000 - funded by NCSC and Brown & Williamson) which assisted in, in part, to qualify the numbers. There must be a data base to record cargo crime to better get a true handle on the severity, where the losses are occurring, the type product(s) being stolen and the ability to properly allocate resources (funding as well as manpower).

10.) Clearance by being C-TPAT certified, unfortunately, doesn't control port and terminal congestion. Although it may allow for document clearance, it doesn't get the shipment "out the door" any quicker.

11.) A Multi Jurisdictional Task Force (MJTF) is one that is made up of various law enforcement personnel, such as the TOMCATS of Miami, FL. The TOMCATS, MJTF consists of: Miami Dade, FBI, C&BP, FDLE, DEA, etc. and is headed by Lt. Edward Petow of the Miami-Dade Police Dept. It provides for greater cooperation, sharing of information, and the ability to respond to any situations that might arise. In addition, this group offers educational programs within the state of FL., as well as to other law enforcement agencies throughout the country and has been attended by overseas law agencies, too. The TOMCATS are thought of, by numerous individuals, including this writer, the template for establishing a MJTF.

12.) The Tallahassee Summit was held for the second year, by Sheriff Ed Dean, and attended by Gov. J. Bush, local and state officials and, as well, by the private sector, government and law enforcement sectors from around the country. At that Summit, there was a "National Security White Paper" drafted and approved by all that attended. Please advise if you need a copy of this document.

13.) It is, in my opinion, that an increase in spending for enhanced security is unavoidable.

1. a Multi Jurisdictional Task Force will supplement those agencies already working.
2. it is possible, in my opinion, provided the responsibilities are spelled out. There will, most likely, be costs associated therewith.

14.) A.

1. continue expanding our borders.

2. better allocation of existing resources (including funding) and technology, such as (x-ray type equipment), etc.
3. better communication and sharing of data amongst law enforcement, government and the private sector.

B. No, in my opinion, there is always a cost associated with any measures/equipment to be implemented, however, with better sharing of data and resources, the allocation of necessary resources would save time, cost overruns and duplication.

15.) To my basic knowledge and understanding of VACIS type equipment - no.

16.) To my understanding, through CSI, shipments are recorded and the container information and units are checked as they go on board. If there are any additional inventories performed on board, I would recommend contacting port/terminal and/or carrier personnel for additional details.

RESPONSE TO QUESTIONS FOR THE RECORD SUBMITTED BY JEFF KEEVER, DEPUTY EXECUTIVE DIRECTOR, VIRGINIA PORT AUTHORITY

1) In your testimony you mention that "in 2003, the Bureau of Economic Statistics reported that The Port of Virginia plays a part in over 180,000 jobs, with salary and wages in excess of $5 billion." Understanding the importance our Ports play in our economy, what do you believe would be the effect on our economy if one of our ports suffered a terrorist attack? Would it be a local effect or national effect?

A: The effect on our economy of a terrorist attack on one of our ports would depend on five factors: the specific port that was attacked, the nature of the attack, the government response to the attack, the shipping industry response to the attack, and the public reaction to the attack.

- The specific port that was attacked. Obviously an attack on a major port will have greater impact on the nation's economy than an attack on a minor port. If the port that was attacked primarily serves a regional market, the direct economic impact will be largely limited to that region.
- The direct consequences of the attack. This could vary widely, in both scope and duration of the consequences. The worst case would be an attack with a nuclear weapon, which could result in the loss of a port for years. But even an attack that did not use any type of weapon of mass destruction could close a port entirely for weeks to months, such as by sinking a large vessel or dropping a bridge span to block a shipping channel. An attack on a large oil terminal or other large petrochemical facility could cause significant damage and economic loss. Terrorists might also attack a port facility in order to cause mass casualties in the surrounding community through release of a large quantity of hazardous chemicals. But terrorist attacks on many other types of port facilities would not cause catastrophic consequences.
- The government response to the attack. If the Federal government were to react to an attack on a port in the same way it reacted to the 9/11 attacks - that is, by shutting down all U.S. ports until the government could verify that no other ports were threatened - the loss to the American economy would be devastating. The economic loss resulting from the Federal government closing all ports in response to an attack would be orders of magnitude greater than the direct economic loss resulting from the attack itself. Clearly, Federal policy should be to minimize the impact of a single attack on the rest of the maritime transportation system and thus minimize the economic damage resulting from Federal policy.

The same phenomenon could happen on a smaller scale within a port if an attack on a single facility were to result in the Coast Guard shutting down the entire port. In a large port the overall economic loss from closing the entire port would be much greater than the direct economic impact of the attack on a single facility.

The manner in which state and local agencies respond to an attack on a port can also impact the resulting economic loss if they impede rapid recovery from the incident. Minimizing the impact of an attack on a port - thus denying terrorists the satisfaction of causing widespread, lasting economic loss - requires a concerted effort by government agencies at all levels, working in close partnership with the maritime industry, to rapidly restore normal operations in the affected port.

- The shipping industry response to the attack. The shipping industry's goal is to keep cargo moving as expeditiously as possible. In an era of just in time delivery, their customers demand no less. If a port suffers an attack, they will divert cargo to other ports. At a minimum, this will cause loss to the economy of the effected port. But it could cause wider loss if the diversion of cargo causes delivery delays and backlogs at other ports. The worst case would be if an attack on a single facility in a port causes a loss of confidence in the security of all the other facilities in that port, causing shipping to be needlessly diverted to other ports.
- The public reaction to the attack. If a terrorist attack on a port were to result in significant loss of life in the surrounding community, the public and their elected officials could well demand assurances of protection against further attacks that would be difficult to meet. This could delay recovery from the attack and cause broad disruption of maritime transportation should such public concerns become a national issue.

2) Your written testimony states that "the Port Authority Police, sworn law enforcement officers of the Commonwealth of Virginia, have been highly effective at preventing crime on VPA's three marine terminals." What is the law enforcement function in securing ports?

A: The law enforcement function in securing ports is similar to the role of law enforcement in homeland security in general: to deter, detect, prevent and respond to terrorist attacks. They ensure that only authorized individuals enter the terminals, and prevent theft or pilferage of shipping containers and other criminal acts on the terminals. They provide security procedure and threat awareness training to all persons working on the terminals. They maintain compliance with the Coast Guard Maritime Security Condition (MARSEC) currently in force. Although many of the functions could be performed by security personnel who are not sworn law enforcement officers, there is an inherent advantage to having a dedicated police force serving the port authority. Sworn law enforcement officers have much greater authority to control movement and behavior of persons on the terminals, including as a last resort use of force (in compliance with Commonwealth of Virginia policies on use of force by state law enforcement agencies).

3) According to your testimony, "Although CBP is responsible for implementing US-VISIT, CBP will require support from Port Authority Police . . ." Could you explain the type of support the police will provide?

A: First and most importantly, the Port Authority Police deny terrorists opportunities to circumvent U.S. Customs and Border Protection (CBP) immigration control procedures. That is, they prevent individuals from departing vessels via the terminals unless they have been properly cleared by CBP. This is a critically important function that every port facility must carry out because CBP does not have sufficient agents to post a 24-hour guard around all of the ships that call in U.S. ports every day. This is an excellent example of the manner in which the port industry has been compelled by the Maritime Transportation Security Act (MTSA) to perform a wide range of functions to protect the nation as a whole from terrorist attacks.

The Port Authority Police also provide logistical and administrative support to CBP, including office space and parking on the terminals. CBP has not yet informed the port industry of the details on how US-VISIT will be implemented at the thousands of port facilities that receive vessels from overseas, but it undoubtedly will impact port facilities in some way and certainly will not relieve them of their responsibility for preventing individuals on ships arriving from overseas from CBP immigration control procedures.

4) Where is the Port of Virginia in its implementation of its upgrades to comply with Federal SAFECOM interoperability standards? Please explain the importance of interoperability to port security.

A: The Port of Virginia is still in the early planning stages of upgrading its communications system. It is our intent to request a Round Five Port Security Grant to fund this upgrade, which will be costly and thus beyond out means to accomplish in a timely manner.

VPA priorities for enhancing its security program have been driven by the overriding requirement to achieve and maintain compliance with MTSA and the Coast Guard Maritime Facility Security Regulations (33 CFR, Chapter 1, Subchapter H, Part 105). Neither MTSA nor the Coast Guard Maritime Facility Security Regulations require compliance with SAFECOM, which was launched more recently and had not produced authoritative, comprehensive standards that could be acted upon prior to 2005.

VPA has identified a need to upgrade its aging communications system, which is hard pressed to meet the greatly increased Port Authority Police communications requirements resulting from MTSA and the Coast Guard Maritime Facility Security Regulations. One of the priority requirements in planning for the communications system upgrade is to enhance interoperability with the Federal, state and local agencies with whom the Port Authority Police work on a daily basis and in emergencies. To achieve that, we are closely following the strategic plan and interoperability standards being developed by the Virginia's Commonwealth Interoperability Coordinator and the opportunities to integrate Port Authority Police communications into the Statewide Agencies Radio System (STARS), led by the Virginia State Police. Both of these Commonwealth of Virginia programs are guided by SAFECOM, which will ensure that the Port Authority Police attain the required level of interoperability with Federal and local agencies as well.

5) Please describe the cooperative security efforts the VPA uses to ensure that the stream of commerce is not unduly interrupted.

A: There are many cooperative efforts that contribute to enhancing security without unduly impeding the flow of commerce:

- Providing office space on the terminals for CBP agents.
- Operating radiation portals that in other ports are operated by CBP and sharing specialized radiation detection equipment with CBP.
- Briefing arriving vessels on VPA security procedures.
- Providing training on VPA security procedures to persons requiring access to VPA terminals.
- Designing entry and exit control procedures to avoid traffic backups at terminal gates.

Many of these examples may appear to be small matters, but collectively they make a big difference in the flow of commerce.

As I stated in my testimony, some of the most serious impediments to the flow of commerce are caused by the inadequate resources provided to CBP and the Coast Guard to accomplish their missions. This results in vessels being delayed entering port while they await Coast Guard boarding and inspection, and containers piling up on the terminals while they await CBP inspection. Such delays are costly for shippers and their customers, and ultimately represent a drain on the American economy. No one questions the need for such security measures, but the agencies that execute them must have the resources they need to carry them out without impeding commerce.

6) Does your office regularly interact and share information about shippers and cargo with other port authorities?

A: The Port Authority Police does not have jurisdiction over cargo other than its responsibility to prevent theft and pilferage while it is on the terminals. CBP is responsible for preventing contraband from being smuggled into the country and would be the agency responsible for sharing law enforcement information related to shippers and cargo with other agencies.

If the Port Authority Police have suspicions about a shipment, or are informed of anything suspicious about a shipment by an individual working on a terminal, after securing the area, they notify CBP. This has actually happened and in at least one case that we know of resulted in CBP intercepting a shipment of illegal drugs. It would be CBP's responsibility to share information related to that incident with other port authorities. The Port Authority Police would not do this because they do not have the comprehensive information gathered by CBP and U.S. Immigration and Customs Enforcement in their investigation of the suspect shipment.

7) You said in your testimony on page 5, "VPA's guiding principle for security is that a state port authority has a higher level of responsibility than a private port facility operator," how so? What kind of effect would increasing a private port facility operator's responsibilities have on the private port in terms of cost? Is it possible to increase the private port facility operator's responsibilities without increasing funding to that private port facility?

A: A state port authority has a higher level of responsibility than a private port facility operator because a state port authority is accountable to the citizens of the state and their elected officials for protecting their investment in the port and meeting their expectations for the port's performance. That means ensuring that the port contributes to the state's economy through robust growth in its port business and striving for maximum efficiency and productivity. It also means having an effective security program, both to protect the lives of the state's citizens and to prevent a terrorist incident from interfering with commerce through the port. Very importantly, it means striking a careful balance between growth and productivity on the one hand and security on the other. Neither can be pursued at the expense of the other - the citizens for whom the port authority is a public servant deserve no less.

Increasing a private port facility operator's responsibilities would, at a minimum, increase the cost of that facility's security program. The amount of that increase would depend on the nature of the increased responsibilities. It could also impede the flow of cargo through a terminal, thus reducing that terminal's productivity and competitiveness. It could cause problems with labor relations if a private company is tasked to perform quasi-governmental or quasi-law enforcement functions with questionable statutory authority. Similarly, it could incur significant liability risks that would not be incurred by a government agency. All of these problems illustrate the need to draw a clear distinction between security measures that a private port

facility operator should have in place as prudent business practices, and the much more extensive security measures required by MTSA intended to protect the nation from terrorist attacks. Effective homeland security is a daunting task even for the Federal agencies that exist for that specific mission; attempting to shift their responsibilities to private port facility operators that are not capable of carrying out those tasks would only result in serious deterioration of port security.

The manner in which MTSA has been implemented over the last two years shows that it is possible to increase a private port facility operator's responsibilities without increasing funding to that private port facility. But the port industry's experience with MTSA clearly shows that doing so is highly undesirable, even counterproductive. Imposing statutorily mandated security requirements - requirements that must be complied with under threat of severe sanctions for non-compliance - without providing the funding needed to effectively implement MTSA does not produce effective port security. Overall, the port industry is struggling to do the best it can to bear the burden of the unfunded mandate imposed on it by MTSA, but this can hardly be described as wise national policy. MTSA was passed to protect the entire nation from the potentially widespread consequences that could result from a terrorist attack on the maritime transportation system. In the realm of national defense, the financial burden of protecting our nation from foreign aggression is placed on the nation as a whole. In the realm of homeland security, the financial burden of protecting commercial aviation from terrorist attacks and preventing terrorists from exploiting land transportation to enter the United States is placed on the nation as a whole. Only the maritime industry has been forced, under threat of sanctions, to bear the cost of protecting the nation from terrorist attacks.

8) Please list and describe the type of responsibilities and duties entrusted to your port authority police? Do these responsibilities and duties overlap with any other agency - public or private - at VPA?

A: MTSA assigned the Port Authority Police responsibilities and duties similar to those of law enforcement in homeland security in general: to deter, detect, prevent and respond to terrorist attacks. But those responsibilities and duties are on top of a broad range of responsibilities similar to those of corporate security organizations that protect their businesses against criminal acts. Port Authority Police responsibilities and duties include, but are not limited to:

- Ensuring that only authorized individuals enter the terminals. This consists of perimeter security, access control at gates, and a credentialing and badge system.
- Preventing theft or pilferage of shipping containers and other criminal acts on the terminals. This consists of verifying that containers departing the terminals have been properly cleared for release and monitoring the terminals for indications of criminal activity.
- Preventing all types of criminal acts on the VPA terminals, such as robberies, burglaries vandalism and other such crimes - similar to the responsibilities of local law enforcement agencies.
- Providing security procedure and threat awareness training to all persons working on the terminals. This is required by MTSA and the Coast Guard Maritime Facility Security Regulations.
- Maintaining compliance with the Coast Guard Maritime Security Condition (MARSEC) currently in force.
- Conducting drills and exercises as required by MTSA and the Coast Guard Maritime Facility Security Regulations.
- Supporting CBP cargo and immigration operations on the terminals.
- Maintaining compliance with supply chain security requirements of the Customs-Trade Partnership Against Terrorism (C-TPAT).
- Maintaining compliance with Commonwealth of Virginia emergency preparedness and continuity of operations requirements for state agencies.
- Conducting routine public safety functions similar to those of local law enforcement agencies, such as traffic control and responding to accidents. The Port Authority Police also have mutual aid agreements with the police departments of the cities in which VPA terminals are located, which enables them to assist with emergencies near the terminals (such as traffic accidents on the busy roads outside the terminals).

These Port Authority Police responsibilities and duties overlap with those of a number of public agencies and private companies, but only because such overlap is dictated by MTSA and other Federal and state policies. For example, the Coast

Guard, the Virginia State Police, the Port authority Police and the respective local Police Department all have law enforcement jurisdiction on VPA terminals. In practice, though, these agencies are not conducting redundant operations on a day-to-day basis. And in a major terrorist incident such overlapping jurisdiction could well be an advantage in responding to an emergency with sufficient resources. There is also overlap with private companies that have facilities on the VPA terminals. Like VPA, those private facility operators must comply with MTSA and the Coast Guard Maritime Facility Security Regulations. The VPA Director of Security has worked closely with the facility security officers of those private facilities to coordinate and align their plans and procedures with VPA's in order to achieve an effective overall security posture and minimize redundancy.

One of the potentially most serious areas of overlap is in the responsibilities of federal agencies in the event of a major terrorist incident on a marine terminal. VPA has had to address this in the course of developing response procedures for detection of radiation in a shipping container by the VPA radiation monitoring system. The question is who is in charge, or who takes the lead among Federal agencies? At least eight Federal agencies can point to statutes or policy documents that give them responsibility for all or part of a terrorist-related radiological emergency on a port facility: CBP, the Department of Energy, the Coast Guard, the Department of Homeland Security (DOE response teams are supposed to be placed under DHS control), the FBI, the Maritime Administration (MARAD), the Environmental Protection Agency (EPA), and the Federal Emergency Response Agency (FEMA). At the working level, local representatives of these agencies make it clear that they will focus on their specific responsibilities and not engage arguments over who has overall control of the situation. That is reassuring, but does not resolve the issue. The response to a radiological emergency can be complex, causing the response procedures of these various agencies to conflict with each other and requiring an authority that understands these diverse response plans to resolve procedural issues. Additionally, all of these agencies have headquarters that could well take a different view of who is in charge and override the collegial approach of their on-scene representatives. The solution is a Federal policy document that resolves this issue; but neither the National Response Plan (Including its radiological emergency annex) nor the National Incident Management System provides definitive guidance.

9) What are some ways you can secure our ports and cargo without an increase in personnel?

A: I can only speak to VPA's experience. We have attempted to achieve MTSA compliance without an increase in Port Authority Police personnel. This is driven by funding: we simply cannot afford large increases in personnel and the Federal government is not willing to fund them, even though it was Federal law that mandated the requirements we are trying to meet. Some of the security requirements imposed by MTSA and the Coast Guard Maritime Facility Security Regulations are extremely manpower intensive, such as the requirement for random vehicle and bag checks at entrance gates. VPA has attempted to leverage technology wherever possible to reduce manpower requirements so that Port Authority Police personnel can be reassigned to MTSA tasks for which there is not a readily available technological solution. For example, installation of a closed circuit television system for perimeter surveillance reduces the requirement for police officers on perimeter patrols, making them available for other duties. Another example is to achieve as much automation in access control as possible, thus reducing manpower requirements at the terminal gates. Our goal would be fully automated, unmanned gates, but the Coast Guard Maritime Facility Security Regulations currently do not permit this. We will be working with the Coast Guard to achieve minimum manning on our gates consistent with MTSA security requirements.

1) What about the creation of joint task forces to prevent the duplication of responsibilities by other agencies?

A: VPA is a member of the FBI's Tidewater Joint Anti-Terrorism Task Force and the Coast Guard's Area Maritime Security Committee. Duplication of responsibilities has not been a serious issue for VPA because Port Authority Police jurisdiction is limited to the VPA terminals. For example, the Port Authority Police does not have boats patrolling the harbor, which is the responsibility of the Coast Guard, the Virginia Marine Police and city police departments. Wherever overlapping responsibilities across Federal, state and local agencies exist, joint task forces or other cooperative approaches to coordinating their efforts toward the common goal of effective port security would certainly be called for.

2) What about delegating responsibilities and duties to other agencies; including local, state and other federal government agencies, or even private companies?

A: VPA itself does not have authority to delegate its port security responsibilities and duties to other Federal, state and local agencies. Our goal is to have effective working relationships with those agencies and to ensure that all of our security and emergency response plans are synchronized and mutually supporting. Please see my answer to question 7 above concerning delegation of responsibilities to private companies. Although VPA has contractors that assist it with various aspects of its security program, it has not delegated any of its port security responsibilities to them. VPA is accountable to the Coast Guard for compliance with MTSA and the Coast Guard Maritime Facility Security Regulations, and would face drastic sanctions for non-compliance. This strict regulatory environment precludes delegation of responsibilities.

10) Please list your top three priorities in securing our ports and cargo? Can you envision a way to accomplish these priorities without additional funding or personnel?

A: My top three priorities for securing America's ports and the cargo passing through them would be as follows:

- Fund all port security requirements imposed on the port industry by MTSA and the Coast Guard Maritime Facility Security Regulations that are designed to protect the nation from terrorist attacks; in other words, all requirements beyond those that a prudent business would take to protect itself from normal criminal activity. The port industry does not have the resources required to protect the nation. We are willing to carry out our responsibilities to the best of our abilities, but the Federal government must live up to its responsibilities for homeland security as well.
- Provide the Federal agencies responsible for port and cargo security, especially CBP and the Coast Guard, with the resources they need to carry out their missions. I have the utmost respect for the hard working men and women of these two agencies. They are doing the best they can with the resources they have, but they are stretched thin and face a significant challenge carrying out their responsibilities without impeding the flow of commerce.
- Enhance the management of the Port Security Grant Program. Develop a more rigorous allocation system that ensures funds are provided for purposes that provide the greatest enhancement to port security, rather than the current practice of spreading grants as widely as possible. Preserve the positive aspects of the current Port Security Grant Program, such as the evaluation of grant proposals by experts in the Coast Guard, CBP and MARAD, and continue to provide the grants directly to port authorities, port facility operators, and other state and local agencies directly responsible for port security. Because the Port Security Grant Program supports implementation of a unique statutory requirement imposed on a single industry, do not merge port security grants with other grant programs that are not tied to implementation of statutory mandates, which would greatly increase the competition for scarce grant funds and thus exacerbate the financial burden that has been placed on the shoulders of the port industry. Similarly, the Port Security Grant Program should not be treated in the same manner as grant programs supporting state and local first responders. The allocation procedures used for those programs are not appropriate for an industry governed by a statutory mandate, and would result in loss of the expert review process now in place. Amend the Port Security Grant Program to permit a portion of those funds to be applied to annual operating expenses for security. Compliance with MTSA has significantly increased annual operating expenses, including maintenance of the high technology security systems required for effective compliance with MTSA, training and exercise expenses, and all the personnel and other operating expenses incurred by ports for security.

The only possible way to reduce, or avoid future, costs is to update the CFR 105 requirements to a more "tailored" made requirements - a risk based approach. For instance, a predominately container facility, such as VPA, compliance should be against regulations based on the threat and vulnerability to a container facility. E.g., Significantly reduce the requirement for vehicles inspection entering the facil-

ity. [A container facility sees a high number of "tractor-trailers" are required within the regulations to inspect the cab, yet leave the 40 feet of cargo "un-inspected" due to a practical way to accomplish.] Where a petro-chemical facility might be prudent to have a higher standard, as one might argue the threat or vulnerability to the petro-chemical facility is entering vehicles.

11) Does the type of container inhibit inspection in any way? If so, how? Would a uniform container requirement help ease the burden of inspection?

A: This question should be directed to CBP for a complete answer. VPA does not inspect containers and would only open one in an emergency, such as suspected or actual release of hazardous material or some other emergency in which opening a container would be necessary to protect human life. Containers are already standardized in terms of dimensions and construction for maximum efficiency of intermodal transportation. There is one type of container that presents unique challenges: marine portable tanks (tanks build to the same dimensions as regular shipping containers). I recommend that you ask CBP about the challenges of inspecting for contraband hidden in a marine portable tank full of the various liquid cargoes carried in them.

12) How often is a cargo vessel coming into the U.S. required to take a physical inventory of its cargo? After the vessel takes a physical inventory of its cargo, is the cargo vessel required to report is findings to anyone?

A: This question should be directed to the US Coast Guard and CBP for a complete answer. VPA does not have the authority to direct such a physical inventory and has no knowledge of a vessel destined for a VPA terminal ever having been directed to conduct such an inventory by the Coast Guard or CBP. I also recommend that you refer this question to the International Cargo Security Council, the Chamber of Shipping of America, the Intermodal Association of North America, the Maritime Security Council and The Waterfront Coalition. I am sure they would tell you that conducting a physical inventory of the cargo in hundreds of containers on a vessel would be impossible and that the master of a vessel has no responsibility for verifying that the contents of the containers matches the shipping documents for those containers.

STATEMENT SUBMITTED BY THE RETAIL INDUSTRY LEADERS ASSOCIATION

On behalf of the Retail Industry Leaders Association (RILA), we welcome the opportunity to submit written comment for the record for this important oversight hearing on port security. Safe and secure seaports are an important element in building efficient and technologically advanced supply chains that can move cargo quickly to distribution centers, stores, and factories across the nation. Any delays can seriously disrupt the supply chain and harm the U.S. economy.

The Retail Industry Leaders Association (RILA) represents the nation's most successful and innovative retailer and supplier companies—the leaders of the retail industry. Retail is the second largest industry in the U.S., employing 12 percent of the nation's total workforce and conducting $3.8 trillion in annual sales. RILA's retail and product supplier companies operate 100,000 stores, manufacturing facilities and distribution centers in every congressional district in every state, as well as internationally. They pay billions in federal, state and local taxes and collect and remit billions more in sales taxes. They are also leading corporate citizens with some of the nation's most far-reaching corporate social responsibility initiatives.

RILA and its members have played a critical leadership role in shaping supply chain security efforts. From partnering with U.S. Customs & Border Protection and the Department of Homeland Security to testing different pilot projects, RILA and its members are committed to ensuring the safety and security of their supply chains not only to protect their cargo, but also their customers and the individuals associated with the movement of their cargo.

Since the tragic events of September 11th, a great deal of work has gone into improving the security of the supply chain. What we ask members of Congress and the Administration to understand is that the supply chain is a very complex system and that variations exist among companies and between industries. While there have been a number of initiatives and regulations put in place since September 11th, there is still a lot that needs to be done.

Members of Congress and the Administration must realize that there is no "silver bullet" solution when it comes to supply chain security. There is no one technological or procedural solution that will magically make every supply chain safe and secure from infiltration. RILA strongly believes that the layered approach that the government is currently using is the best way to prevent a terrorist attack within the supply chain - and we urge Congress to continue on this wise course. There is of course a role for technology but it needs to be integrated carefully into the system and must be consistent with international standards. If a particular technology cannot work worldwide, then it cannot work effectively in our international supply chain. Technology should be reliable and result in virtually no false positives or false alarms. Even a 1% failure rate could be disastrous.

SECURITY ACTIONS TO DATE

As members of the subcommittee are aware, there have been a number of regulations and programs that have been put into place to increase supply chain security. U.S. Customs and Border Protection (CBP) along with the U.S. Coast Guard have taken the lead on a number of these efforts.

CBP is now enforcing both the "24 Hour Rule" and the "Trade Act" which require the submission of manifest information in advance of cargo arriving in the U.S. For ocean bound cargo, the information must be submitted before the container is even loaded onto the vessel at the foreign port. These new regulations have enabled CBP to better utilize information and better identify "suspect" cargo through its Automated Targeting Center.

In addition, CBP has also developed a number of new programs through partnerships with the trade community as well as foreign Customs agencies. The Customs-Trade Partnership Against Terrorism (C-TPAT) was the first true private-public partnership to enhance supply chain security. Many of RILA's members were the first to join the C-TPAT program and helped to develop the program. Many of these same companies continue to work with CBP to further enhance the C-TPAT program. CBP has also been partnering with RILA members and other C-TPAT members to test "smart box" technology, container security devices and the collection of advanced trade data.

CBP has also worked with foreign Customs agencies through the Container Security Initiative as well as working to develop an international framework for supply chain security through the World Customs Organization.

CBP has many other tools at its disposal including the use of non-intrusive inspection technology such as the Vehicle and Cargo Inspection Systems (VACIS) and Radiation Portal Monitors which are being deployed at ports nationwide.

The U.S. Coast Guard is now responsible for enforcing the Maritime Transportation Security Act (MTSA) as well as the International Maritime Organization's International Ship and Port Facility Security (ISPS) Code. In fact, the U.S. Coast Guard was instrumental in the development of the ISPS Code, which closely resembles the MTSA. These new regulations call for increased security at port facilities as well as ocean vessels.

While CBP and the Coast Guard have taken the lead on supply chain security and port security efforts, there are other agencies that are involved as well. The Food and Drug Administration is now enforcing the Bioterrorism Act (BTA), which protects the nation's food supply from a terrorist attack.

FUTURE ACTION

There is still a great deal of work that needs to be done on supply chain security. However, this cannot be done overnight. As stated earlier, the supply chain is a very complex system that companies continuously seek to refine and improve. Cargo security legislation and regulations should include a thorough analysis and recognition of commercial implications including the potential impact of delays and congestion on the national economy. RILA believes that there are several issues that Congress should consider as it moves forward with initiatives to secure the global supply chain.

Container Inspections

Many in Congress have talked about the physical inspection of 100% of cargo containers. RILA strongly believes that 100% physical inspections are not necessary or economically viable. Physically inspecting every box is simply impossible. Members need to consider infrastructure issues such as marine terminal congestion, warehouse space shortages, trucking demands and highway congestion.

Such an approach would result in an enormous increase in congestion at U.S. seaports and have a tremendously negative impact on the U.S. economy. Rather, a more effective approach would be for CBP to continue to focus on inspecting 100% of the cargo that is deemed suspicious by the National Targeting Center.

Balanced Policy

Policy developed by the Department of Homeland Security, Congress or other agencies should balance the need for security and the need to allow the free flow of legitimate commerce. Security requirements should not become a barrier to trade.

Technology

There is no single technological solution for supply chain security. The government should not rush to require the use of "smart containers" or "electronic seals". These technologies are still extremely expensive and are not yet 100% accurate. Technology should *not* be considered as the only solution. It should be considered as a part of the overall strategy. Successful security includes a multilayered approach. We know of few if any technologies that have been independently tested by entities that do not have a conflict of interest in selling such technology. No only does the technology need to be reliable but because of the expense we need to ensure that the technology considered will improve the probability of detecting a security risk (i.e. WME or WMD). By way of example, if you could design a foolproof container door intrusion device, all the terrorist would have to do is cut a hole in the side of the container for purposes of placing a bomb inside. An operation such as this might only take 20 minutes or less depending on the expertise of the bad guy. We need to ensure that the money we spend provides more than simply "feel good" measures.

Government Coordination

There needs to be a better-coordinated approach not only between federal government agencies, but also those at the state and local level. If an incident occurs, everyone needs to be on the same page as to how to respond. In addition, Congress and the Administration need to ensure that the various agencies involved in homeland security do not duplicate ongoing efforts.

Likewise, each country has an interest in ensuring that the global supply chain is kept safe. A major terrorist incident in the U.S. will not impact just one port or one city or even one country. The impact will be felt around the globe.

Therefore cooperation among governments is important. But government's active collaboration with the private sector is extremely critical. Supply chain security is

simply too complicated for the public sector to tackle the problem without partnering with private industry. This is a good example of the whole being greater than the sum of its parts.

Business Continuity/Contingency Planning

There is a need for the Administration to focus on business continuity/restoration plans in the event of a terrorist attack. To date, most of the attention has been on prevention. Now there needs to be an equal focus on the steps that will be taken to keep the global supply chain operational in the event of an attack. The trade needs to know who is in charge, how they will make decisions, whether and which segments of the supply chain will be closed and how those decisions will be communicated to the trade. One of the terrorist's main goals is to disrupt the world economy. Therefore, it is imperative to have plans in place, which will reduce the disruptive effects of any terrorist incident.

CONCLUSION

A great deal of work has been done over the past two years to ensure the safety and security of cargo entering and leaving U.S. ports. There are still many areas for future work. However, through partnerships with U.S. government agencies such as CBP and through increased partnerships with their suppliers, both merchandise and transportation providers, RILA's members have accomplished a great deal to ensure the security of their supply chains. They are continuing to learn what works and what doesn't around the world. These lessons must be taken into consideration as new regulations and policies are discussed.

We thank the subcommittee for the opportunity to submit written testimony for the record and stand ready to continue to work with both Congress and the Administration on improving the security of U.S. ports and the global supply chain. If you have any questions, please contact Jonathan Gold, Vice President Global Supply Chain, or Paul T. Kelly, Senior Vice President, Federal and State Government Affairs.

○