

Mid Atlantic Region Port Security Workshop Report

Hunt Valley, MD – October 22-23, 2009



This page intentionally left blank

Copyright © 2010

By All Hazards Consortium

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or any information storage and retrieval system, without permission in writing from the publisher.

Requests for permission to make copies for any part of this work should be mailed to:

Mr. Tom Moran, Executive Director
All Hazards Consortium Program Office
7360 Guilford Drive, Suite 201 Frederick, MD 21704

Printed in the United States of America

Board of Directors
President
Evalyn Fisher
Philadelphia, PA



All Hazards Consortium
Program Management Office
7360 Guilford Drive, Suite 201
Frederick, Maryland 21704

Vice President
Andrew Lauland
Maryland

June 18, 2010

Secretary
Jackie Wasni
Motorola

Greetings from the All Hazards Consortium Board!

Treasurer
Robert Briggs
Delaware

It is with great pleasure that the All Hazards Consortium is able to announce the release of this Port Security Regional Workshop Report. This represents the sixth such regional report that establishes common agreement across our member states and urban areas on an important regional topic.

Millicent West
District of Columbia

The basis of this report was formed at our Regional Port Security Workshop in Hunt Valley, Maryland in October 2009. Seven states came together to discuss their current port security efforts and the role that maritime plays in their overall Homeland Security and Emergency Management efforts. Since that time, the port security representatives around the region have worked together to finalize this important document.

Joe Picciano
New Jersey

John Gibb
New York

Bud Mertz
Pennsylvania

This document represents another collaboration effort of the nine (9) consortium states and urban areas of Washington, D.C., New York City, Northern New Jersey, and Philadelphia with stakeholders from industry, higher education, non-profit and federal government partners. Going forward, this document will be used to help the states and urban areas in their planning efforts, grant activities and overall coordination efforts in important issues facing the region, including: information sharing; evacuation planning; communications interoperability; critical infrastructure protection / interdependencies; and, many of the future topics the AHC will be addressing in 2010 and 2011.

Christy Morris
West Virginia

Cheryl Wilkins
James Madison University

Dr. David Lindstrom
Penn State University

I would like to thank all our participants and partners who helped with this effort; many are listed in the report, but there are many hundreds of others who have helped with the Consortium's efforts over these past five years.

Robert Crouch
MITRE

Ira Tannenbaum
New York City UASI

I would particularly like to express our appreciation to our new partnership with the State, Local, Tribal and Territorial Government Coordinating Council's (SLTTGCC) Regional Partnerships Working Group (RPWG) and the Regional Consortium Coordinating Council (RCCC) who co-hosted this workshop with us. Their focus on regional Critical Infrastructure/Key Resource Interdependency issues will help regions across the country share information and benefit from this effort. We look forward to working together with them both in the near future.

Scott Di Giralomo
New Jersey UASI

Terrie Suit
Virginia

We are proud to release this important new document as we move the ball forward to improve protection for our citizens, increase awareness and enhance overall public preparedness.

Many thanks,

Advisory Committee
John Contestabile, Chair
Advisory Committee
Maryland

Joe Conrey, Chair
Critical Infrastructure
Protection WG
New Jersey

Executive Director
Tom Moran

Evalyn Fisher
Executive Director, Southeastern Pennsylvania Regional Task Force
President, Board of Directors
All Hazards Consortium

TABLE OF CONTENTS

1	Executive Summary	1
2	Summary of Panel Discussions	5
	2.1 State Perspective Panel	5
	2.2 Owners and Operators Panel	8
	2.3 Keynote Speaker	13
	2.4 Federal Perspective Panel	14
3	Findings and Recommendations	17
	3.1 Finding 1: The Port of the Future	17
	3.2 Finding 2: Essential Public-Private Partnerships	18
	3.3 Finding 3: Sustainability and Success of Regional Planning and Projects	19
	3.4 Finding 4: Full Spectrum Port Security	20
	3.5 Finding 5: “Coopertition”	21
	3.6 Finding 6: Information Sharing	22
	3.7 Finding 7: The Federal Grant Process: Investing in the Future	23
	Appendix A – Port Security Perspective Of The State of West Virginia.....	25
	Appendix B – Acknowledgments.....	27
	Appendix C – Case Studies / Solutions	29

I EXECUTIVE SUMMARY

The All Hazards Consortium (AHC) hosted the Regional Ports Security Workshop October 22-23, 2009 in Hunt Valley, Maryland, to bring together federal, state, local, and private sector stakeholders from across the Mid-Atlantic region, including North Carolina, the District of Columbia, Maryland, Virginia, West Virginia, Delaware, Pennsylvania, New Jersey, and New York, to discuss shared issues related to port security. The workshop was co-hosted by the State, Local, Tribal and Territorial Government Coordinating Council's (SLTTGCC) Regional Partnerships Working Group (RPWG); the State of Maryland and its host agencies; and private sector partners. Guests from the U.S. Department of Homeland Security (DHS) and regional port associations played a prominent role in panel discussions and participation. The workshop focused on a variety of topics designed to educate attendees on ports from a regional perspective and captured a "multi-state snapshot" of key topics to the region's ports (coastal and in-land) from several perspectives (e.g., federal, state, and private sector).

This Regional Report summarizes the general themes and outcomes of the conference, panel topics and discussions, and the consensus on issues developed during the course of the Workshop. In addition, this paper will chart a way forward for the region to collaborate on port security, including immediate action items for stakeholders, recommendations for dealing with current and future threats, and a blueprint for cooperation and partnership on shared issues of concern across the full spectrum of the public and private sectors. It is the hope of the AHC that this Regional Report can thereby help to educate a wider audience on developing port security issues, increase exposure for these topics, and provide recommendations that can help focus the work of the AHC member states and urban areas, private sector stakeholders, the federal government, and all other port security actors.

Port security topics and questions included in this paper:

- **Vision and planning:** How will stakeholders better secure the port of the future?
- **Governance structure:** What are the regional ports' unique roles and responsibilities and how are security concerns addressed and rectified in the current framework?
- **Funding:** How do ports engage in port security and UASI grant programs? What are some of the challenges with the funding and grant process and how can it be improved?
- **Economics & Operations:** What are possible funding sources for security improvements? How can ports increase regional cooperation in light of the traditional competitive nature of ports as a business exercise?
- **Cyber vs. Physical Security:** What information and physical security measures are being considered to increase port security? What opportunities for improvement exist?

- **Technology:** What are the key challenges facing port investments in technology?
 - **Information sharing:** How do organizations share critical information with federal, state, and local government, the private sector, and other groups?
- **Partnerships and Associations:** How do various organizations interact and collaborate in daily operations and what is the best mechanism for collaboration in emergency and post-disaster situations?
- **Existing efforts and accomplishments:** What are some of the best practices currently in use in the region's ports?
- **Opportunities for the future:** What are some of the common issues the Mid-Atlantic region can focus on and what is the best framework for doing so?

Findings

The extensive discussions generated by these topics crystallized in a number of clear findings that would be used to formulate helpful recommendations for port security. Although interstate cooperation on port security has increased in recent years, the workshop revealed that streamlining information sharing between states can be further improved. Additionally, much work remains to break down barriers to integrated interstate security planning and response. The main barrier to increasing this collaboration is the traditional competitive nature of the port industry, which hinders growth in cooperative port security measures. There must be a balance between competition and cooperation, and the Mid-Atlantic states and urban areas are determined to help strike that balance moving forward to assure the integrity of the region's ports as well as the public safety. The attempt to define this balance affects the full spectrum of port security, and it will permeate this paper's recommendations.

Recommendations

The Regional Ports Security Workshop identified seven (7) important findings in port security and generated discussion on recommendations for addressing these concerns in the near and future term. Section 3 of the report discusses each finding and the associated recommendations for action in detail. The seven findings and associated recommendations for action developed by the Regional Ports Security Workshop are as follows:

- 1) **The Port of the Future:** All current port security actions and planning must be pursued in anticipation of future threats and technological developments. The Ports Workshop outlined a range of issues likely to face the Port of 2030 to help generate necessary forward thinking in addressing both current and future challenges.
- 2) **Essential Public-Private Partnerships:** Public-private partnerships are essential for integrated security planning and effective levels of information sharing among private and public port security actors.

- 3) **Sustainability and Success of Regional Planning and Projects:** Regional port security planning and projects must include frameworks to facilitate continued interstate cooperation and long-term sustainability of port security initiatives.
- 4) **Full Spectrum Port Security:** Port security must be addressed in an all-hazard, all-sources approach in order to quantify the full spectrum of threats facing ports, while taking into account the regional repercussions of a port incident up to and including complete closure.
- 5) **“Coopertition”:** Ports and states must strike an effective balance between security cooperation and business competition to safeguard regional port resources.
- 6) **Information Sharing:** Interstate information sharing must be increased and institutionalized through the creation of common standards, and operating procedures.
- 7) **The Federal Grant Process - Investing in the Future:** Enhancing the efficiency of the federal port security grant process will enable more effective cross-border collaboration.
- 8) **Coordinating & Leveraging Existing Efforts:** Effective port security efforts must be coordinated to reduce overlap and duplication of efforts and investments.

2 SUMMARY OF PANEL DISCUSSIONS

2.1 State Perspective Panel

The panel, moderated by Mr. Mike Fischer, Homeland Security Advisor, Maryland Department of Transportation (MDOT), brought together maritime security representatives from four All Hazards Consortium states to discuss their respective roles and responsibilities as well as their vision for the future of port security. Mr. Fischer began by asking representatives to discuss the governmental structure of port oversight in their states.

Ms. Noreen Cardinali, Section Chief, Office of Transportation Security, New Jersey Office of Homeland Security, noted that New Jersey runs all port security operations out of the Office of Homeland Security and Preparedness (NJ OHSP). The NJ OHSP serves as the hub for all port security initiatives including submitting and dispersing grants and formulating partnerships between the public and private sector. The NJ OHSP works closely with the U.S. Coast Guard (USCG) sponsored Area Maritime Security Committee (AMSC) to foster and strengthen partnerships between the state and the private sector port stakeholders. The NJ OHSP as part of the AMSC group, meet regularly to discuss risk assessments of critical assets, to identify vulnerability gaps, and to assess current capabilities against the approved DHS target capability list.

Mr. Ed Merkle, Director of Port Security and Emergency Operations, Virginia Port Authority (VPA), stated that in 1971 the Commonwealth of Virginia combined authorities of many disparate local ports to create the VPA. The VPA is a state-owned and controlled business and is responsible for all maritime safety initiatives in the Commonwealth. The VPA serves on its respective AMSC, which allows the Commonwealth to connect with federal and local partners as well as the private sector.

Mr. H.G. “Bud” Frank, Director of Security, Maryland Port Administration (MPA) detailed how the MPA is a modal component of the MDOT. In Maryland, all transportation security and emergency management, including port security, is coordinated and planned in a multimodal manner.

Mr. Herb Packer, Director, Ports of Pennsylvania (PennPORTS) discussed the challenges of maintaining focus on the importance of the ports to Pennsylvania when the commonwealth is not typically viewed as a maritime state. Pennsylvania is home to three vital coastal and inland ports. A separate USCG sector governs each port which makes it difficult to coordinate policy statewide. Mr. Packer noted that the AMSCs have been very useful in building relationships and how important those relationships are in the event of a crisis.

Mr. Fischer then moved the discussion to long-term planning and budgets.

Mr. Frank, MD stated that the MPA has an Executive Director who reports directly to the MDOT Secretary and the Maryland Ports Commission. The MPA’s planning process

does not focus on profit; rather it focuses on job creation and sustainability. Maryland utilizes a multi-year budget process that can pose problems because the State Legislature cannot increase, but may cut, the MPA budget.

Ms. Cardinali, NJ noted that New Jersey has been working to create an Area Maritime Security Risk Assessment (AMSA) based on the Maritime Security Risk Assessment Model (MSRAM). The AMSA will help determine whether an identified asset is critical enough for investment while simultaneously opening lanes of dialogue among federal, state, and local partners about counter-measures which should be employed. Ms. Cardinali closed by stating that, in her opinion, the best venue for regional security planning discussions in the ports of the future will be the Area Maritime Security Committee.

Mr. Merkle, VA detailed how the VPA has been working for years from a 2020 plan and has recently completed their 2040 plan. Key components of the 2020 plan include creating a partnership with Norfolk Southern to utilize double stack railcars to transport cargo from Virginia to Ohio while moving train tracks to avoid high-risk street crossings. The VPA is also collaborating with the U.S. Navy to create roadways to better control flow of traffic around naval bases and ports. Finally, the VPA is in the process of building the Craney Island Marine Terminal, which will be the largest and deepest terminal in the Nation.

Mr. Fischer then asked each panelist to describe the economics of their port operations. He asked how each state approaches port security and Urban Area Security Initiative (USAI) grants, and questioned how each is combating the economic realities of a recession.

Mr. Packer, PA noted that the recession has hit all state agencies but that it has been particularly hard for PennPORTS because their budget is wholly dependent on the federal grants programs for homeland security initiatives. PennPORTS does not have a line item in the Commonwealth's budget for the resources to apply for federal grants, so all resources spent applying for grants comes from the overall operations budget.

Mr. Merkle, VA noted that the federal grants program has been a great source of revenue for the VPA but that the distribution of funds has been problematic. The commonwealth is still awaiting the release of grants awarded for Fiscal Year (FY) 2007, which has backlogged the distribution of FY08 and FY09 grants. Mr. Merkle noted that in the future states would likely make the decision to follow the California model. California agreed to put up guaranteed state money (\$10 million) for the required match which in turn guaranteed the state more than \$30 million in Federal grants. The state's guarantee expedited the distribution of grants from the federal government.

Mr. Merkel noted that the states have trouble determining what the next investment should be; they do not want to get ahead of the market and currently don't have the facilities or resources to conduct their own research. It might be time for a state, or

multiple states coming together, to invest in research and development to help advise on how to spend the resources.

Mr. Frank, MD detailed Maryland's recently created public-private partnership to install Transportation Worker Identification Credential (TWIC) card readers in an attempt to make the public and private terminals consistent. The MPA also utilizes Baltimore UASI grant funds and encourages other states and urban areas to tap UASI funds for port security as ports are built into cities and are a vital aspect of the commerce of most major urban areas.

Echoing Mr. Merkle's concerns, Ms. Cardinali, NJ encouraged the federal partners to review the grants program and its distribution of funds. She expressed her concern that the current process hampers state efforts to harden and better secure the ports. Another problem is the short timeframe available to spend federal funds. Currently, once a state receives the grant money they have only 36 months to spend the money completely. This timeline prevents some projects from being started quickly due to the prerequisite to complete environmental impact studies, MOU executions, and/or complete other federal or state grant requirements before federal funds are released. She also noted that in the current economic climate, requiring states to match 25 percent of the grant amount is onerous and forces many port applicants to stop applying for grants.

The conversation then turned to interoperability in communications, information sharing, and cyber security. How are the ports in each state sharing information with local, state, and federal partners?

The VPA has made great strides in cyber security and interoperable communications in the past five years. In 2004, the port security team was very isolated from the information technology (IT) security team. The security teams now share one seamless network, which operates via fiber optic cable. The VPA still has outstanding issues with access (e.g., does the IT professional have the same level of clearance as the security guards?) but the teams are now working together to protect port assets, both physical and cyber. Since Hurricane Katrina exposed the problems of interoperability, the Commonwealth of Virginia created an interoperable statewide communications system that allows communications between fire, police, and emergency rescue systems.

Mr. Packer, PA noted that although cyber security is vital to securing the ports, there is still a need for improved physical security. He stressed that recent grants have moved from physical hardening to cyber security. The need for physical enhancements cannot be overlooked and should remain a funding priority. PennPORTS is working to enhance its information sharing with the private sector. Pennsylvania does not currently have an all-hazards fusion center, but one is planned and should be fully functional within a year.

Mr. Frank, MD noted that ports should remain competitive from the business standpoint but should not be competitive in security matters. He noted the Maryland Fusion Center has been a great resource for coordination of multi-modal and multi-sector situational

awareness. Maryland is working on a new vessel tracking system that will feed into the fusion center and be shared throughout the National Capital Region (NCR).

In summation, Mr. Fischer asked each panelist to provide success stories and issues where more work is needed.

Ms. Cardinali, NJ stated the biggest recent success has been building trusted partnerships and relationships with a variety of federal, regional, and local partners. She cited the resiliency planning projects undertaken in the Delaware Bay and New York sectors, and the maritime domain awareness projects, as examples of stronger partnerships at the regional level. Issues which remain include allocating and distributing grant funds to assets in greatest need despite the cost share requirement, as well as assigning ownership responsibilities on large multi-disciplinary projects to shared users.

Mr. Packer, PA also commended the maritime domain awareness project and the work of the AMSCs in building and sustaining partnerships. He stated the largest issue facing PennPORTS is a planned government reorganization that could alter the chain of command for emergency response and homeland security in Pennsylvania.

Mr. Merkle, VA noted his agreement on the success of the AMSC while stating that Virginia has also been successful in creating a mass notification system. The notification system took lessons learned from the 2007 incident at Virginia Tech and implemented a system in the ports that relays critical information to employees. VPA is interested in working with other states on an information exchange regarding the mass notification system.

2.2 Owners and Operators Panel

Ms. Lisa Himber, Vice President, Maritime Exchange for Delaware River and Bay moderated a discussion among port owners and operators, which provided their unique perspective on what is working, and what needs to be improved, in port security. Ms. Himber noted that the panel represented a wide cross-sector of the maritime industry including two port authority operators, one port authority landlord, one private port operator, and one railroad operator at a port. To begin, panelists described their operations and sources of funding.

Mr. Kurt Ferry, Director of Security, Holt Oversight & Logistics, noted that Holt serves as marine terminal operators in Philadelphia and Gloucester City, New Jersey with services in container cargo and refrigerated cargo. Holt was recently designated a strategic port operator by the Department of Defense, allowing it to ship military cargo. He noted that a challenge facing private marine operators is the discrepancy of resources in emergency response. He stated private operators should have equal access to first responders and state emergency response assets.

Mr. Ed Merkle,¹ VA stated the VPA operates three marine and one inland terminal. The inland terminal is a truck depot in Front Royal, Virginia, which was built in an attempt to curtail business going to the terminals at the Port of Baltimore. Virginia International Terminals, Inc., (VIT) was incorporated as a non-stock, nonprofit corporation in 1981, to operate all the marine terminals owned by the VPA. VIT operates the state-owned ports through a Service Agreement with the Virginia Port Authority. The organizational structure of VIT provides it the ability to enter into contracts with union labor (prohibited by state agencies under state law), negotiate and enter into contractual relationships with ship lines and others while not being subject to the Freedom of Information Act (FOIA). This structure allows for more efficient flow of traffic at the marine terminals.

Mr. Louis Vitale, Maritime Security Coordinator, Port Authority of New York and New Jersey, noted that the Port Authority is unique in that it's a bi-state agency whereas the Executive Director and Chairman are political appointees by the Governors of New York and New Jersey and each Governor holds veto power over all regional infrastructure projects. Also unique is the full portfolio owned by the Port Authority, which not only owns six marine terminals but three major airports, and all bridges and tunnels connecting New York and New Jersey. The jurisdiction of the Port Authority (extending 25-miles around the Statue of Liberty) allows it to operate regionally between both states. However, of 170+ regulated maritime facilities in the Port of New York and New Jersey, the Port Authority is a landlord to only 7% of them. Since a security incident at one facility can affect the region as a whole, the Port Authority treats maritime security as a regional effort, not only concentrating within its own fence-lines.

Mr. Pat Hemphill, Port of Wilmington, Delaware, stated that the Port is a full-service deepwater port and marine terminal handling more than 400 vessels per year with an annual import/export cargo tonnage of more than four million tons and is the busiest terminal on the Delaware River. The Diamond State Port Corporation (DSPC), a corporate entity of the State of Delaware, owns the Port.

Ms. Himber then asked the panelists to describe the major challenges facing their respective companies/ports and/or how they plan for port security.

Mr. Merkle stated that the VPA is particularly concerned with the potential release or spill of a hazardous material (HAZMAT). To combat against a HAZMAT release, the VPA created a maritime emergency response network. The response network is comprised of 17 local fire departments that the VPA helps fund and provide equipment. In the near future, the VPA is looking to expand the team into incident response.

Mr. Vitale stated that the Port Authority coordinates its security activities through a five-year capital security plan. The plan is periodically updated by incorporating some action items identified by the AMSC. In furthering the planning effort the Port

¹ Mr. Ed Merkle represented both the state perspective and the owner operator perspective in his role with the Virginia Port Authority.

Authority periodically meets with the tenet security working group, which is comprised of the port facility tenants, to discuss incidents, trends, and best practices. In regards to the New York/New Jersey AMSC, it is unique in that it is not chaired by a representative from the USCG, but by a civilian who is elected by the stakeholders, essentially allowing for maximum participation of the stakeholders. The Port Authority Police Department also meets quarterly and participates on various task forces with federal, state, and local law enforcement partners to discuss current activities and initiatives.

Mr. Ferry noted that Holt Logistics and Oversight utilizes the AMSC recommendations for proprietary business development and continuity plans.

Ms. Himber then asked the panelists to describe their funding models and challenges posed by the current economic climate. Especially, how does each organization engage the Port Security and UASI grant programs?

Mr. Vitale noted that the Port Authority is a self-supported agency, in that it does not collect tax revenue, but relies on federal grants and collected revenue (e.g., tolls, property leases, etc.) to fund regional development projects. There are several challenges to the port security grant program, including the stringent spending caps and allowable construction costs. In today's climate, with increasing environmental legislation and permitting requirements, construction costs far exceed the \$1 million cap imposed under the grant. Mr. Vitale encouraged all ports to approach the grant program from a regional perspective and provided the example of the New York City Fire Department (FDNY) training facility for ship based fires; the FDNY had outgrown its training facility and used a regional grant to pay for a new facility. Similarly, the New York City Police Department (NYPD) applied to rebuild its docks that house 37 vessels (more than USCG Sector NY). Another issue with the grant program is the cost sharing requirements; the matching requirements are onerous in the current budget climate. Though initially intended for the private sector, with the port-wide benefit criteria, more public agencies are facilitating the proposals. In 2009, public agencies pulled back nearly \$60 million in proposals due to the cost share.

Mr. Hemphill stated that the Port of Wilmington is self sufficient through collected revenue of tariffs and rent.

Mr. Tony Dragani, Special Agent in Charge (SAIC), Norfolk Southern Rail Corporation (NS) Police Department stated that NS funding priorities are to improve capacity while becoming increasingly environmentally conscious. NS currently has three corridor projects that will require additional resources for increased security. A major challenge in planning for the railroad is how to balance and maintain the quick and efficient movement of customer's goods while handling the increasing demands and costs of security. NS has excellent working relationships with maritime exchange, and state and local decision makers. Mr. Dragani praised the NJ OHSP for their support in securing grants for NS and their security related projects. Mr. Dragani additionally discussed how NS shares information with federal, state and local law enforcement including several

fusion centers and the TSOC. NS has a police communications center based in Atlanta and is working to streamline internal information sharing. NS has a representative on the Railroads Joint Terrorism Task Force (JTTF) who serves as Rail liaison to the railroad industry and liaises with other JTTFs. Mr. Dragani agreed with Mr. Ferry on the need for private sector engagement in fusion centers and encouraged fusion centers and emergency operation centers to continue refining relationships and information sharing especially with the private sector as well as defining notification protocols.

Mr. Merkle stated that Virginia has recently stopped pursuing regionally based grants because of the problems with cost sharing and determining who is responsible for the operation and management costs of the completed regional project. Mr. Vitale seconded Mr. Merkle and stressed that cost share issues are the largest impediment to regional grants.

Mr. Ferry agreed and noted that the problems of cost share are not exclusive to the public sector. The private sector is reluctant to take resources out of the company's bottom line to pursue security grants. He also noted the challenge of keeping all parties involved and focused on regional port security. Something that might be mission critical to the private sector may not be regionally significant.

Ms. Himber ended the discussion on funding by noting ongoing discussions regarding the elimination of the fiduciary agent and cost sharing for the FY 2010 Port Security Grants Program (PSGP). She then pivoted the discussion to information sharing and communication interoperability. While noting that at least 40 businesses go into action when a ship comes into harbor, Ms. Himber asked each panelist to discuss their information-sharing environment. Questions included: with whom does your organization currently share information? What information are you sharing? How are you sharing it?

Mr. Vitale stated that the Port Authority is in the process of implementing a program called Blue Force Tracking, whereas law enforcement and first responder vessels will be equipped with encrypted transponders allowing for enhanced coordination among different agencies, and secure communication amongst participating vessels. A number of Port Authority personnel participate in various port-wide committees to further collaboration between the numerous agencies having a stake in the port.

Mr. Merkle referenced his previous comments on Virginia's statewide interoperability system while noting that the VPA pushes information out to its partners from its Port Command Center. The command center brings together all port information including fire alarms and other sensors and assimilates the information into a mass notification alert. The information is then shared with state and local operations centers. However, the system is not tied into the federal government due to the restrictions on the usage of federal grant money, which is used to fund the system.

Mr. Ferry stated that it is essential for the private sector to have representation at fusion and emergency operations centers.

Mr. Dragani declared that NS shares information with federal, state, and local law enforcement. NS has a police communications center based in Atlanta and is working to streamline internal information sharing. NS has a representative on the Railroads Joint Terrorism Task Force (JTTF) and he liaises with other JTTF's. Mr. Dragani agreed with Mr. Ferry on the need for private sector engagement in fusion centers and encouraged fusion centers and emergency operation centers to do a better job defining their protocols regarding the dissemination of information to the private sector.

Ms. Himber stressed that there should be increased cooperation and communication between AMSCs.

The conversation then pivoted to a discussion of the TWIC program. Mr. Hemphill noted that the Port of Wilmington was an original pilot program for full TWIC implementation and the port used that experience to assist other ports as the TWIC program was stood up.

Mr. Vitale described how the Port Authority linked the TWIC program with a previously established credentialing program named Sealink, which was a program used to facilitate access of truck drivers to a container terminal; it was therefore not created due to security concerns but for business needs. When TWIC was enacted, the Sealink database contained over 30 thousand registered truck drivers, who were added to a separate TWIC database. These two databases were then married so as to facilitate the suspension of a Sealink if a TWIC is found to be on the TSA Hotlist.

Mr. Merkle noted that 15 seconds is the ideal time for a truck to get through a gate at a port; anything longer than that will lead to bottlenecks and delays. To expedite truck throughputs the VPA linked TWIC credentials to their electronic gates, which allow credentialed drivers easy access through the gates while restricting all other drivers.

Mr. Ferry suggested that the states and region target grants and Memorandums of Understanding (MOU) to share Closed-Circuit TV (CCTV) video and data with local fusion centers and law enforcement. Mr. Dragani agreed and noted that NS has had some success sharing its CCTV feed with local law enforcement and has a grant awaiting processing that will add cameras to railroad bridges in Pennsylvania and New Jersey. Mr. Dragani stated that NS is committed to security but the states and locals must be mindful of ensuring that any security enhancements continue to facilitate commerce; they cannot get so focused on security that they inadvertently erect barriers to commerce and trade

Mr. Ferry noted that Holt is getting increasingly aggressive in pursuing grant opportunities and is heavily focused on training all employees on security and incident response. Holt is interested in seeing strong legislative action that requires certification for all port workers. Ms. Himber noted that Senator Frank Lautenberg from New Jersey is working on legislation that will create a certification for marine guards. She then

posed the question to the panel on what is working and what needs to be improved in port security?

Mr. Merkle noted that a model for the future could be Project SeaHawk. SeaHawk was a pilot program based in Charleston, South Carolina that included a Multi-Agency Intermodal Task Force, Intermodal Fusion & Analysis Center, Interagency Operations Center/Charleston Harbor Operations Center (CHOC) and an Intermodal Test & Evaluation Center. He encouraged that similar projects be created in ports throughout the nation. He also noted that the exercise and training grant programs are not well coordinated, and cited the example of fire departments receiving resources to complete duplicative training. Mr. Merkle strongly recommended coordinated regional exercises and training.

Mr. Vitale seconded Mr. Merkle's recommendation and noted that it should be a priority to reduce or eliminate redundant efforts. Within a single port, two terminals should not be competing for grant money for identical activities. If it has a port-wide benefit, it should be bid and executed jointly. He also stressed the need to combat complacency and educate the public on the importance of port security.

Mr. Ferry concluded the panel discussion by highlighting the need to encourage training and exercises while lamenting the lack of available federal resources to fund regional training. He stressed that regional training would reduce redundancy and help bring ports, competitive by nature, together to enhance security.

2.3 Keynote Speaker

Ms. Juliette Kayyem, the Assistant Secretary, Office of Intergovernmental Programs (IGP) at DHS began her remarks by noting her background as the former Homeland Security Advisor (HSA) for Massachusetts. She stressed that both she and Secretary Napolitano, having state government backgrounds, have taken state and local needs to heart and made them clear priorities at the department. This is evidenced by the strengthening of the role of IGP in DHS through the elevation of her title to the Assistant Secretary level and the office being folded into the Secretary's own office.

Assistant Secretary Kayyem discussed her review work for the Obama transition team on the role of intergovernmental affairs and their interaction with state and local actors. Her analysis highlighted that this priority had been sidelined by other department priorities and was lacking in transparency. In her words, the elevation of IGP has signaled the importance associated with the state and local perspective by the new administration. Her office provides the connection between the Secretary, and state and local partners nationwide. Assistant Secretary Kayyem stated that she sees regional consortia as a vital player in this process, bringing state and local ideas and concerns to the fore in DHS, while embodying a strong connection between DHS leadership and leaders in the maritime and transportation field.

She then discussed the status of the partnership between the department and states on fusion centers. In the future, she sees a role for DHS Intelligence and Analysis (I&A) subject matter experts (SMEs) at fusion centers across the country to assist in getting the private sector involved. In her opinion, facilitating information sharing with states and locals is the greatest concern as DHS moves into the intelligence arena. Moving information from law enforcement and other sources up the chain from the state and local level will be a primary concern for the near future. She noted that there is a governing board at I&A which is looking at fusion centers, and is working with state and local stakeholders and DHS to define private sector engagement. She acknowledged that there are unresolved questions regarding who can sustain private sector engagement, as well as how best to leverage fusion centers tactically, on a state-by-state basis. She expressed the need for IGP, I&A, and states to coordinate on how to “operationalize” the broader vision for fusion centers.

Assistant Secretary Kayyem ended her remarks by discussing her vision of IGP as the one stop shop for state and local stakeholders. She foresees her office as a vehicle to field questions from state and locals, and getting answers from the department’s vast and sprawling organization. Her biggest concern moving forward in this vein is how best to incorporate state and local issues and further engagement.

2.4 Federal Perspective Panel

The third and final panel brought together representatives from DHS, the United States Coast Guard (USCG), the Federal Emergency Management Agency (FEMA), and the U.S. Department of Agriculture (USDA). The panel was moderated by Mr. Patrick Twiss, Federal Preparedness Coordinator, National Preparedness Division Director, Region III, FEMA. Mr. Twiss began by stressing the importance of partnership between the government and the private sector in resiliency. Federal, state, and local governments have the ultimate responsibility to respond to incidents, but the private sector is crucial to all rebuilding and recovery efforts. He cited the example of the earthquake and subsequent tsunami that recently struck American Samoa. A major factor in getting the island back to functionality was collaborating with shipping companies to communicate with their employees. He noted that although all disasters are local, the economy is global, and a truly resilient country/region/locality requires an excellent public/private partnership. Mr. Twiss then asked each panelist to describe their operations in regards to port security.

Dr. Freeda Isaac, Director, National Center for Import and Export, Veterinary Services, Animal and Plant Health Inspection Services, USDA, stated that USDA port activities focus on safeguarding the nation from diseases that might be transmitted from imports of livestock and produce. USDA places officials at all major air and sea ports as well as at all land entries along the northern and southern border.

Mr. R. James Caverly, Director of the Partnership and Outreach Division (POD), Infrastructure Protection and National Protection and Programs Directorate (NPPD), DHS, stated DHS has worked to create a strong public-private partnership. He noted

that there is a potential rift between fusion centers and emergency operations centers (EOC) and that states and locals need to coordinate homeland security and emergency management activities. The goal is to have one framework that the private sector can use in liaising with both fusion centers and EOCs; two-way information sharing is essential for emergency response and resiliency.

LCDR Michael DaPonte, Contingency Planning & Force Readiness Chief for Sector, Baltimore, USCG, noted that everyone in the room understood the role of the USCG in maritime security and expressed the Coast Guard's support of the public/private partnership spearheaded by the local AMSCs.

Mr. Twiss then asked the panelists to describe their agencies' roles in incident management, with particular attention to their role in command and control decisions.

Dr. Issac commented that the USDA serves as a partner in crisis management and will rarely take the lead in incident response; their purpose is to augment and support state response activities.

LCDR DaPonte noted that the USCG has a defined command structure and that it is the primary incident response agency of the federal government for all maritime incidents.

Mr. Caverly noted that DHS employs regional Protective Security Advisors (PSAs) who serve as the Department's on the ground representatives.

Mr. Twiss then asked the panelists to discuss challenges with the grants process from the federal perspective. He also asked panelists to highlight possible areas of improvement.

LCDR DaPonte noted that he was not able to answer all the questions previously raised regarding cost sharing, but stated that USCG recently finished appropriating grants from the supplemental stimulus, which did not have a cost-sharing requirement. He stressed the partnership of the Maryland Maritime Security Committee and encouraged all participants to be active in their local Area Maritime Security Committee (AMSC).

Dr. Isaac and Mr. Caverly noted that their respective organizations are not responsible for the distribution of grants specifically allocated for port security. However, Mr. Caverly encouraged the states to work together to pursue regional grants and commended the All Hazards Consortium for providing a forum for multi-state coordination.

Mr. Twiss then asked panelists to discuss how their organizations share information throughout the region, asking if they disseminate information vertically to the states and then down its respective chain of command or horizontally to several partners at once?

Mr. Caverly noted that DHS makes it a priority to share information with all relevant partners and that the DHS Information Sharing Environment (ISE) provides excellent flexibility to add partners based on the characteristics of the incident.

Dr. Isaac stated that the USDA works with the respective state health departments to share pressing information during an incident and shares response plans (e.g., pandemic influenza guidance) and continuity of operations (COOP) plans to all partners and stakeholders.

LCDR DaPonte extolled the virtues of the USCG supported information-sharing portal, HOMEPOR, and encouraged all participants to register and take advantage of its full functionality.

The conversation then moved to the regulations enforced by each organization. Lcdr DaPonte stated that the Maritime Security Act of 2004 mandated a shift to a more risk based approach to port security. The Act moved the maritime community to a performance based risk mitigation methodology. The methodology has been successful but can occasionally give the perception of inconsistent implementation. Although the progress has been substantial, he agrees there is room for improvement. The USCG is refining and constantly looking for better ways to define and measure risk.

Dr. Isaac stated that the USDA's regulations are not related to ports specifically, but are based on the risk associated with the imported commodity.

Mr. Caverly spoke about the TWIC program and the larger issue of credentialing and affiliate access. He said the problem is not technological but bureaucratic. While noting the government needs to do a better job of consolidating the numerous divergent credentials, the bigger question is how to create a system that allows for *ad hoc* access to a port (or any other incident) based on the individual incident circumstances.

At the conclusion of the panel, Mr. Eric Casey General Manager at Maersk Line, Limited announced that Maersk was collaborating with several non-profits to create a fleet of all-hazard maritime response vessels. Once complete, the vessels will have a fully integrated emergency operations center with dedicated satellite communications link and 9-1-1 services. The fleet's extensive services will also include a disaster casualty care system that includes hospital beds, pharmacy and a morgue, as well as water purification system, mobile emergency response system with roll-on roll-off capabilities and a fully stocked evidence lab. The vessels are being built in a collaborative effort and will be used for emergency response (e.g., Hurricane Katrina, Pacific tsunami response) as well as training and exercises. The ships are scheduled to be completed within 18 months.

3 FINDINGS AND RECOMMENDATIONS

3.1 Finding 1: The Port of the Future

Efforts made to protect our Nation's ports today must not only focus on solving current problems, but also anticipating and planning for threats and developments of the future. The Regional Ports Workshop included discussions on what the hypothetical port of the future will look like in order to frame the outcomes of the workshop in this progressive context.

The states and urban areas of the All Hazards Consortium will continue the vital work of discussing the port of the future to develop an ever-clearer outline of tomorrow's port security concerns to assist in the planning of today. This discussion must be a constant evolution to keep pace with technological innovation, the international business market, and the effect that both will have on shaping how our ports must operate securely and efficiently moving forward. The preliminary outline of the port of the future developed during the Regional Ports Workshop focused on the following trends and concerns as top priorities.

- Vessel traffic systems will become essential for law enforcement operations in port security and subsequently must be improved, standardized, and fully integrated into fusion centers.
- Technological advances must be routinely tracked and exploited by ports to ensure that developments such as smart sensors that track and independently adjust to malfunction or alert systems operators of problems are utilized to increase efficiency and security of operations.
- Human operators alone cannot track all information compiled by new systems. The port community must work to streamline its operations and maximize time with smart technology that can sift through the ever-increasing pool of security information derived from CCTV and online sources before passing along critical information in need of human analysis.
- Underwater surveillance is a significant capability gap in port security. It must be accounted for in the port of the future by mapping water bottoms and developing the means of countering underwater hazards through appropriate levels of research and development.
- Climate change and its environmental impact must be addressed to determine and plan for the possibility of rising sea levels and associated impacts on port security.
- Cyber security must play an equal role to physical security in safeguarding our ports. Stakeholders must monitor technological advances, such as social networking tools, and explore these tools for their utility in improving security as well as the possible threats they pose to port operations.
- The Port of 2030 must not be conceptualized in a purely physical context. Port security must be integrated in all port planning and addressed in a comprehensive and holistic fashion to utilize the most current technology to protect from both physical and cyber threats.

- Sustaining the regional dialog is a top priority.

As we work toward resolving the issues presented in this document, we must keep these concerns and developments in mind as the framework in which to find common solutions to shared deficiencies in security.

Recommendation 1A: Institute a continuing process for partnering with the DHS Science and Technology (S&T) Directorate's Borders and Maritime Security Division to facilitate dialogue on current and future needs of regional ports to develop clear concepts for the port of the future and influence the direction of research and development in the realm of port security to maximize returns on federal investment. Regional ports should explore ways to assist DHS S&T in this mission by volunteering to serve as pilot ports for new projects to increase close federal, state, local, and private sector coordination on these important security developments to ensure that all stakeholders are working together to ensure the most secure ports of future.

Recommendation 1B: Partner with DHS National Cyber Security Division (NCSD) to discuss how to secure Supervisory Control and Data Acquisition (SCADA) systems and cyber security networks in the most efficient and effective manner possible.

3.2 Finding 2: Essential Public-Private Partnerships

Stakeholder integration will be the key to securing our ports of today and tomorrow; public-private partnerships are essential to making integration a reality. The diverse stakeholders involved in port security, and the disparity in port operations from state to state, necessitate strong regional collaboration to:

- facilitate common standards,
- coordinate on planning for contingencies,
- develop common resources to be leveraged by all,
- coordinate and leverage public and private investments,
- respond to emergencies, and
- manage disasters.

The efficacy of these critical activities can be improved greatly through understanding and communication across state lines.

The states and urban areas in the AHC have led the way in bringing together these diverse stakeholders, and the dialogue of the Ports Workshop will go a long way in developing the personal relationships, knowledge base, and delineation of shared concerns and solutions. Public and private sector entities operate ports in AHC member states and urban areas. The participants of the Ports Workshop are a testament to this diversity of stakeholders.

On the most basic level, public-private partnerships exist to provide coordination between federal, state, local, tribal, territorial, and private sector stakeholders, all of whom connect to the daily functioning and security of any given port. It has proved difficult to streamline this coordination and integrate all into solid processes on issues from information sharing to planning procedures to the creation of common standards. This document addresses each of the issues individually, but it should be noted that they can only be addressed through full integration of stakeholders in functioning partnerships. The public and private sectors must be integrated throughout this process to maximize the comprehensive dialogue needed to reach full spectrum solutions on port security.

The public and private sectors often address problems from different viewpoints, a fact which provides real opportunity to find fresh ways to solve problems when both groups are able to collaborate and plan together. The competitive nature of the private sector necessitates innovation and technological progress for market viability and survival. The public and private sectors are both however, constrained by finances, and are often forced to focus on immediate problems rather than carefully planning for the future and investing in R&D areas that could adapt to future needs. Public-private partnerships, and meetings such as the Ports Workshop, are vehicles for sharing current and future needs. Private sector development projects can use the input provided by these vehicles to work towards solutions for security gaps in the port of the future. The public sector and private sector must work together as full partners in port security in all stages of planning and operations.

Recommendation 2: Fully integrate and involve port owners and operators in their local USCG sponsored AMSCs. Encourage USCG to facilitate enhanced coordination among AMSCs and between AMSCs and external bodies (e.g. DHS S&T, FEMA).

3.3 Finding 3: Sustainability and Success of Regional Planning and Projects

Regional planning and projects on port security are an essential outgrowth of public-private partnerships. Regional partnerships such as the AHC provide the framework for states and urban areas, and both the public and private sectors, to address the myriad common concerns on port security. AMSCs are extremely valuable frameworks for collaboration on port security and should be fully utilized across the region.

The sustainability and success of regional partnerships are often dependent on public and private sector volunteers and require commitments of time and finances from states and urban areas in order to continue operations. States and urban areas must recognize the need for these partnerships and dedicate the required level of attention and resources for success. The difficulty of regional partnerships is often due to the issue of ownership; without clearly defined ownership of interstate problems, and assumption of responsibility, many important issues fall by the wayside until a disaster forces them back into the collective consciousness. Regional partnerships and organizations must

keep the momentum going on important projects and topics, but that requires the participation and time of an array of stakeholders.

Equipment shortfalls are another issue of shared concern for member states and urban areas. Regional planning and projects should include studying the feasibility of sharing information about available resources among states and urban areas, as well as sharing the resources themselves, which would be a cost-effective and as yet unrealized tool for maximizing regional gains with limited finances.

Recommendation 3A: Develop MOUs between member states and urban areas which can designate parties responsible for certain issues, and outline possibilities for shared resources and groups responsible for maintenance of shared equipment.

Recommendation 3B: Create a solid framework for Inter-state Disaster Training and Exercising whereby law enforcement, emergency response, and other port security actors from throughout the region can train together and develop processes for joint reaction to regional events.

Recommendation 3C: Formulate interstate/interagency plans and leader trees for response framework, reinstitution of powers, and continuity of operations, in the event of a disaster involving one or multiple ports.

3.4 Finding 4: Full Spectrum Port Security

Ports are regional lifelines facilitating international and domestic trade, transportation, and economic vitality. As such, it is essential that port security is addressed in an all-hazard, all-sources approach in order to quantify the full spectrum of threats facing every port, while taking into account the regional repercussions of a port incident up to and including complete closure.

A full review of the supply chain effects of port closures is necessary, to help determine a clearer picture of the criticality of ports to both the region and the nation. Even a cursory look at the possible effects of port closures shows:

- financial losses in the untold millions for the private and public sectors,
- an inability of labor resources to move within the affected port, and
- a public safety threat for densely populated metropolitan areas built around regional ports.

This however, is only the tip of the iceberg. Goods, services, and ultimately the lives and livelihoods of tens of millions of people are dependent on the port. The entire supply chain would be disrupted in the event of a port closure, let alone in the event of multiple port closures in the AHC state region. These supply chains stretch from international shores through our ports and into landlocked communities in the United States which are dependent on ports to transport goods for trade.

A review of the full spectrum of port security, including the supply chain that is reliant on port operations, is essential for the region, and ultimately the nation. There is a need to prioritize resources in a way that is consistent and relative to the broad threat posed to port security. A threat to one port is not an isolated security issue; it is a threat to the economic viability and public safety of an entire region. Federal and state allocation of resources and attention must be in accordance with this fact, and based on a comprehensive full spectrum review.

Recommendation 4A: Design a tabletop or functional exercise that focuses on the closure of a large Mid-Atlantic port and its potential impacts throughout the region. Consider the possibility of a FEMA sponsored regional exercise. The exercise could help focus on resiliency planning projects, recognizing interdependencies, to minimize port closure effects and ensure speedy recovery of essential activity by identifying critical operations necessary to port operations.

Recommendation 4B: Perform a study of the economic impact of the port industry in the nine-state region. This can be built on local and regional studies which may already exist, developing the data where they do not, and factoring overlap among the port areas included in the study.

3.5 Finding 5: “Coopertition”

Traditionally, ports have been incredibly competitive business enterprises. A certain level of competition is healthy and necessary for port operations in the reality of the business environment and private nature of many port facilities. Ports and states however must strike an effective balance between business competition and security collaboration to safeguard regional port resources. Deemed “*coopertition*”, this phrase adequately sums up a new approach in port security operations and interstate coordination on port security.

An enhancement of relationships and cooperation between interstate port operators could expose duplicative efforts, wasteful repetitive spending, and the deprivation of the collective best practices, which detract from an increase in overall port safety.

One glaring example of how competition can stymie interstate cooperation is in the case of the federal grant process. Competitive grants hamper regionalization and collaboration between states and urban areas by enforcing the notion of ports as competitors. DHS should instead look at a grant structure that would encourage cooperation.

Recommendation 5A: Continue interstate networking of port security officials to develop relationships that can foster increased understanding and common approaches to problems.

Recommendation 5B: Create a regional education and outreach initiative that illustrates the impact inadequate security practices can have on individual port

business operations, and the region as a whole, to encourage increased levels of cooperation.

Recommendation 5C: Encourage states and urban areas to develop an MOU to delineate security issues on which states and their ports can fully cooperate while maintaining their respective competitive edge and business viability.

3.6 Finding 6: Information Sharing

Information sharing is critical to port security, but there are still many barriers in place to its effective practice. Each state has different practices for its ports and different stakeholders responsible for port security. The Ports Workshop has accomplished much in spreading awareness through the AHC community of how partner states and ports operate, in order to facilitate communication between the necessary players. The first step in communication is the knowledge of whom to contact. The second step in communication is having a process by which partners can share critical information in a regular, timely and appropriate manner, a process which, to date, states and urban areas and the private sector have found elusive. A third step would be the establishment of common standards across state lines for:

- credentialing port security officials,
- telecommunications systems,
- determination of need to know, and
- mechanisms for pushing information over secured and unsecured networks to its proper audience irrespective of state lines.

The possible role of fusion centers must be addressed in this process. Co-locating federal, state, and local law enforcement and emergency response officials has gone a long way in streamlining information sharing between stakeholders. Incorporating the private sector into these centers would dramatically improve communications among port partners. In the same vein, regional collaboration would be enhanced through:

- exchange programs for employees,
- collocation of officials from different states and urban areas in fusion centers,
- the possible creation of interstate fusion centers, and
- the use of the same online systems based in fusion centers for properly cleared individuals to disseminate information.

Should all be explored as options to increase and institutionalize interstate cooperation? Regional fusion centers in New York and New Jersey should be explored as case studies for this type of integration.

Common standards can be accomplished through dialogue from meetings such as the Ports Workshop to inform partner states and urban areas of best practices across the region. The next step must be to take these best practices and then determine how to implement them in order to facilitate the smooth and steady flow of information to every

member state. It will require close collaboration between states and urban areas to come to terms with what standards every member state must meet as a prerequisite for receiving information, and subsequently what system each member state will use to share the information. The following recommendations will help to create the needed momentum

Recommendation 6A: Draft an MOU on clearance levels of port security personnel in neighboring states and urban areas to ensure port security operators are meeting common expectations and needs regarding operational security.

Recommendation 6B: Explore creation of virtual regional operations centers, which could facilitate real time interstate information sharing on port security planning from an interdependency perspective incorporating multiple states and urban areas and the private sector.

Recommendation 6C: Create an MOU between states and urban areas and the private sector regarding a mass notification system for states and urban areas outlining what information should be immediately shared across state lines and the best process for dissemination.

Recommendation 6D: Coordinate with DHS to develop protocols for fusion center integration, including best practices and standard operating procedures (SOPs), which can facilitate information sharing between states and urban areas.² Encourage DHS to allow linkage between fusion centers and state and local programs.

Recommendation 6E: Encourage all eligible to register and utilize a secure maritime community portal (e.g., HOMEPORT, HSIN-CS).

3.7 Finding 7: The Federal Grant Process: Investing in the Future

The Regional Ports Workshop developed a broad consensus on the need for improvement of the Port Security Grant Program (PSGP). The grant process should be structured to account for the full spectrum of port security and ensuring the fair distribution of resources based on an accurate calculation of risk to the region as a whole rather than to individual ports.

The AHC member states and urban areas should encourage FEMA to explore opportunities to apply for grants as a region to solve common problems by developing shared solutions.

Recommendation 7A: The AHC member states and urban areas should develop formal lines of written communication with FEMA documenting shortcomings of the current grant system and suggesting a formalized collaborative process in which FEMA and member states and urban areas can work to improve these issues.

² Refer to AHC Mid-Atlantic Region Fusion Center Workshop Report for more recommendations

Recommendation 7B: Strongly encourage FEMA to alter the PSGP to remove or reduce the cost sharing requirements, streamline distribution of funds and expand the period of performance from 36 months to 48 months.³

Recommendation 7C: Institutionalize a regional multi-state grants workshop under the leadership of FEMA to educate states and urban areas on grant opportunities and lead the way in applying for grants as a region rather than as individual states and urban areas to ensure accurate resource allocation.

Recommendation 7D: Encourage and provide the means for developing partnerships and personal relationships among the port owners and operators and UASI directors to encourage collaboration and potential UASI funding of port security initiatives. Allow private sector port operators located in UASI districts to apply for UASI funds.

³ In FY 2010 the cost sharing requirements have been lifted.

APPENDIX A – PORT SECURITY PERSPECTIVE OF THE STATE OF WEST VIRGINIA

On January 13, 2010, Mr. Patrick Donovan, Director of the West Virginia Public Port Authority (WVPPA), who was unable to attend the workshop, provided his perspective on port security and the topics discussed at the workshop. Mr. Donovan noted that the WVPPA is structured differently than its neighbors Kentucky and Ohio. The WVPPA is a state agency of the West Virginia Department of Transportation. The WVPPA is controlled by a Board of Governors whose members are appointed by the Governor. The charge of the WVPPA is to develop “the potential of intermodalism by combining highway, rail, and water transportation infrastructure to maximize overall economic advantages to business, industry, and the citizens of West Virginia.”⁴

West Virginia is responsible for 422 miles of navigable waterways along the Ohio River system and has over 300 private terminals. The majority of the product moving up and down the waterways is coal, with petroleum and petrochemicals also constituting a large percentage of traffic. The Ohio River system is divided among the Marine Safety Unit (MSU) Huntington and the Marine Safety Office (MSO) Pittsburgh. The WVPPA is based out of Charleston, the State Capital, and is thus much closer to MSU Huntington. So in effect, James McCarville, Executive Director of the Port of Pittsburgh Commission, helps coordinate the security efforts for the West Virginia waterways covered by MSO Pittsburgh.

Mr. Donovan raised the issue of proper coordination between neighboring states as the main challenge facing the WVPPA. When dealing with the Commonwealth of Kentucky the WVPPA works with the State Police or a private terminal operator, while for the state of Ohio it must collaborate with the Ohio Watercraft Division. Regional coordination would be streamlined and more effective if it was standardized among neighboring states in the region. There is also a lack of coordination between the U.S. Coast Guard (USCG) and U.S. Army Corps of Engineers (USACE). The USCG is responsible for MSU Huntington (422 miles of navigable waterways) but the USACE statistical port district for the Port of Huntington Tri-State is only 199 navigable miles. The geographical definitions don’t dovetail and can subsequently lead to great confusion.

The Huntington AMSC has been very effective in securing MOUs across jurisdictions. The Port Security Plan addresses primary responsibility for response and recovery. The criticality of the inland water system is based on dams and locks; if there is a failure of a lock or dam, you lose navigation and commercial transportation. There is a need for enhanced marine domain awareness of the inland waterway system. Awareness has been hampered by a lack of understanding about the criticality of the inland system for commerce, as well as water intake.

The WVPPA is working on addressing a shortage of railroad intermodal terminals and multimodal terminals to facilitate supply lines to and from WV ports. Mr. Donovan noted that the WVPPA worked with Norfolk Southern to secure 90 million dollars of federal funding for the Heartland Corridor Rail Project that will allow for double-stack railcars

⁴ West Virginia Department of Transportation Website <http://www.transportation.wv.gov/Pages/Agencies.aspx>

from the eastern seaboard to Ohio. West Virginia is in the process of clearing 26 tunnels to allow for double-stack access. West Virginia is also building an inland port terminal in Pritchard that will be modeled after the Front Royal Inland Port run by the Virginia Port Authority (VPA).

The WVPPA has worked closely with the Ohio Department of Transportation in an effort to declare the Ohio River System a federal marine highway corridor. There is currently a loose federation of regional port authorities and planning agencies and if the area receives the designation as a marine highway corridor it will band together in an effort to secure regional grants and other federal resources.

Marshall University National Maritime Enhancement Center is working to develop a maritime situational awareness tool. There have been issues with private companies reluctant to share any information that might include proprietary data, such as the location of their barges.

Mr. Donovan stated that another potential issue is a conflict between the Captain of the Port and state agencies. The Captain of the Port can singlehandedly stop previously agreed upon and funded initiatives. Enhanced coordination between the USCG and the state agencies is essential to successful regional coordination.

The conversation then pivoted to information sharing. Mr. Donovan supported the ongoing efforts to create information sharing systems, especially password protected, ring down information blasts, but worries about creating stovepipes. It is unclear whether the system being created in West Virginia will work in conjunction with a system in New Orleans or Ohio; issues such as these must be addressed in planning for a more streamlined port system in the future.

The WVPPA has also had issues coordinating with FEMA on the Port Security Grant Program (PSGP). Funding from FY2007 has not been disbursed and Mr. Donovan noted that the program would be better run if it was coordinated by the USCG and not FEMA.

West Virginia is working to build a port-wide, secure, web based management tool that accesses real time data and coordinates all CCTV feeds as well as all other transportation data and visualizations to port operators. Mr. Donovan expressed a desire to share the data with neighboring states and the Captain of the Port. The WVPPA has also succeeded in physically hardening critical assets with new fences and camera feeds.

Finally, Mr. Donovan stated the WVPPA is working with the City of Charleston Police Department to receive a grant to secure underwater explosive training along the Canal River.

APPENDIX B – ACKNOWLEDGMENTS



Special thanks to the U.S. Department of Homeland Security and SRA International, Inc. for providing resources and support for the preparation of the workshop and the development of this white paper.



SRA International, Inc. and its subsidiaries are dedicated to solving complex problems of global significance for government organizations serving the national security, civil government and global health markets. Founded in 1978, the company and its subsidiaries have expertise in such areas as air surveillance and air traffic management; contract research organization (CRO) services; cyber security; disaster response planning; enterprise resource planning; environmental strategies; IT systems, infrastructure and managed services; logistics; public health preparedness; public safety; strategic management consulting; systems engineering; and wireless integration.

SLTTGCC

In order to bring together critical infrastructure and key resources (CIKR) protection experts from the private sector and all levels of government, the Department of Homeland Security established the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC). The SLTTGCC functions as a forum for state, local, tribal, and territorial government representatives to engage with the federal government and the CIKR owners and operators within the Sector Partnership Framework, to achieve the homeland security mission of protecting the nation's critical infrastructure. The SLTTGCC's Regional Partnership Working Group (RPWG) was formed to facilitate and encourage the creation of multi-state governmental consortiums focused on CIKR protection. For more information see http://www.dhs.gov/files/committees/gc_1177096698216.shtm

RCCCC

The Regional Consortium Coordinating Council (RCCC) was established in 2008 to bring together established regional entities into a unified forum for coordination with DHS and the established DHS CIKR sector framework. RCCC goals include:

- *Promoting and fostering protection and resilience efforts*
- *Developing a national policy framework for regional infrastructure protection, prevention, deterrence, response, recovery, and longer-term restoration*
- *Providing the foundation for regional cross-sector collaboration*
- *Fostering the development of risk-based protection and mitigation measures to enable measurable progress towards robust security and disaster resilience*
- *Enhancing the education and awareness of critical infrastructure interdependencies*

For more information see http://www.dhs.gov/files/committees/gc_1186441153885.shtm

Thanks also to our other workshop sponsors and All Hazards Consortium partners:



APPENDIX C – CASE STUDIES / SOLUTIONS

Regional Ports Workshop Case Study:

Mobile Port Emergency Operations Center

Client:

Port of Houston Authority, Texas

Challenge:

The Port of Houston faces a number of threats from both natural and potential man-made disasters. Its proximity to the Gulf of Mexico makes it a target for hurricanes every year. They needed to address continuity of operations issues especially with their Class 5 Emergency Operations Center (EOC), as over 220 million tons of cargo moved through the Port in 2009. This Port impacts a variety of people and systems including supply chain for food/fuel/textiles of the Gulf States, 785,000 jobs, and over \$118 billion in annual business. The Port is ranked first in the United States in foreign waterborne tonnage (14 consecutive years); first in U.S. imports (19 consecutive years); second in U.S. export tonnage and second in the U.S. in total tonnage (19 consecutive years).



Solution:

After months of effort, The Port of Houston Authority refreshed their mobile EOC, referred to as the Mobile Coordination Center (MCC). The MCC is a semi-tractor trailer rig with dispatcher stations, a command center, *next generation* Hosted IP Telephony, Satellite Communication for voice, data and video, all managed and maintained by Verizon Business, complemented by annual Health Checks for quality assurance.

The mobile EOC will operate daily as a training facility and for public service and awareness. In time of emergency, the MCC will mobilize and relocate to ensure the unimpeded transportation of cargo, protection of the Port facilities, corporate partners, and surrounding communities, state, and nation.



Application:

The Port of Houston Authority's MCC is mission ready. The MCC is a mobile asset in the communications and emergency response arsenal of the Port Police Department. The MCC is the self-sufficient extension of the Port Coordination Center, the Port's on-site communication coordination and response facility. The MCC enables the Port of Houston Authority Police Department to maintain business as usual performance from remote locations.

Result:

Port security officials and staff will benefit from this solution by improved security and response times to help prevent loss or harm from threats to health, welfare, and assets; increased resiliency in Port operations to help expedite the flow of commerce; improved coordination with state/local/federal government stakeholders, and continued operations and service to the private sector partners.

Regional Port Workshop Requirements/Recommendations Achieved:

Based on the regional findings outlined in this first AHC Regional Port Workshop Report, the following recommendations have been or will be achieved by this solution:

1. Improved security and response times by the Port of Houston Authority Police Department
2. Increased resiliency in Port Emergency Operations
3. Ongoing protection of the Port facilities, corporate partners, and surrounding communities, state, and nation

For More Information: Please contact Pam Doiron, pamela.doiron@verizonbusiness.com, 713.888.7536



Regional Ports Workshop Case Study:

Multi-State Maritime Domain Awareness/Information Sharing

Clients:

US Navy, US Air Force, State of Delaware, State of Maryland

Challenge:

The US Air Force needs to protect their fuel supply chain for Dover Air Force Base. This supply chain involves the receiving of fuel at an off-shore terminal at Port Mahon in the Delaware Bay area. Additionally, the USAF needs the cooperation of the State of Delaware's Fusion Center to help monitor and communicate with the appropriate state and federal agencies that are part of this regional effort.

Solution: **"SureTrak"** is a state-of-the-art, fully integrated, multi-sensor, data acquisition and display system developed by CSC for the U.S. Navy. **SureTrak** receives, integrates and processes data from a variety of remote sensors including surface surveillance radars, air surveillance radars, GPS transponders, AIS receivers, infrared/closed circuit television cameras, and environmental noise monitors. **SureTrak** has been deployed at numerous military facilities in the U.S. (including Maryland's Pax River facility) and is fielded in several African nations as part of the Regional Maritime Awareness Capability (RMAC) program.

Application: CSC is developing a new mobile surveillance system for the state of Delaware. Information collected by this system will be shared between the USAF and the Delaware Fusion Center via a new **SureTrak** web services module. This secure GIS based web technology, also known as **Omni Track**, will increase the visibility of vessels, structures, and other assets across a wide geographic area by integrating data from multiple inexpensive, secure sensors into a single picture so that authorities can analyze, decide and respond to situations faster and alert others in the region to the situation at hand.

Result: State and federal authorities in two states are provided with real-time sensor information, increased visibility and awareness, and improved security and response times through distribution of sensor data via secure web connections to the authorized personnel/agencies and the Delaware Fusion Center.

Regional Port Workshop Requirements/Recommendations Achieved: Based on the regional findings outlined in this first AHC Regional Port Workshop Report, the following recommendations have been or will be achieved by this solution:

- 1) Improved maritime domain awareness through data sharing via secure web portals
- 2) Reduced costs by leverage existing systems and investments across the region
- 3) Increased collaboration by helping to formalize partnerships that share resources and data
- 4) Greater participation by regional Fusion Centers in the information sharing process

For More Information: Please contact Joe Anderson at 301 737-5708 jandersoniii@csc.com



Regional Ports Workshop Case Study:

Multi-State Maritime Information and Intelligence Sharing

Constituents: States of DE, NJ and PA, four public port authorities, multiple private terminal owners/operators, shipping lines and agents, importers, brokers, warehouse operators and trucking companies.

Challenge: In order to process vessels and cargoes moving through Delaware River ports as safely, securely, and efficiently as possible, vast amounts of information must be shared among many private and public partners in the transportation and cargo supply chains. Information needs range from cargo descriptions, quantities, weights, points of origin and destination, importer/consignee data, and cargo release status, to vessel sailing history and crew/passenger names and documentation information, just to scratch the surface. The challenge is to provide a standard electronic interchange to ensure partners have timely accurate access to the information while minimizing the need for each to develop redundant data management systems.

Solution:

Maritime On-Line® (MOL) is a multi-faceted maritime information and intelligence system. Operated by the Maritime Exchange for the Delaware River and Bay, a non-profit association, MOL is a suite of applications including historic, current and projected ship movement schedules, cargo manifesting, an advance notice of vessel arrival system including crew manifesting, and real-time vessel/tug tracking via an Automatic Identification System display. Data is warehoused at the Exchange and made available via on-line inquiry or file uploads/downloads. Detailed information about the individual modules of the system is available at http://www.maritimedelriv.com/Ops/maritime_online.htm.

MOL was developed in partnership between the Maritime Exchange, the private sector business community and the three states. The Delaware River Port Authority provided the initial capital, and operating costs are currently funded via a combination of subscription fees and state financial support. The Exchange has also received federal funding, through the Port Security Grant Program. In turn, the Maritime Exchange allows access to the system at no fee to state, municipal, and federal agency employees who have a right and a need for the information.

Results: Today, over 1,500 individuals at over 400 businesses, organizations and state/federal agencies use the system for both daily operational needs (e.g., resource allocation, risk analysis, etc.) as well as long-term planning and trends assessment. It provides the most cost-effective mechanism for the private sector to meet federal reporting requirements and offers a single portal for critical information, greatly streamlines communication and information processing, and is scalable such that new features are added when identified.

Regional Port Workshop Requirements/Recommendations Achieved: Based on the requirements and recommendations outlined in this first AHC Regional Port Workshop Report, the following recommendations have been or will be achieved by this solution:

- 1) Improved maritime domain awareness through data sharing via secure web portals and secure data transfer
- 2) Reduced costs by leveraging investments across the region
- 3) Increased collaboration by bringing data users together with data providers to design the system and formalizing partnerships to share resources
- 4) Facilitation regulatory compliance and enforcement

For More Information: Please contact Lisa Himber at 215-925-2615 or lisa.himber@maritimedelriv.com.

