**USCG** *(Cont. from 10)*

The brain, or information management center, for the Captain of the Port is the Sector Command Center-Joint (SCC-J). Within the SCC-J, there are cameras to view the port, and communication is conducted via marine radios. The SCC-J has nine different watch positions; seven of them are manned twenty-four hours a day, seven days a week, and 365 days of the year. The jobs the SCC-J watch standers complete are diverse and are the vanguard of port security. The Command Duty Officer (CDO) is a twenty-four hour watch position. During the watch period, the CDO is the direct representative of the COTP, and oversees the other eight individuals on the watch floor. Operational Unit Controller (OUC) is the first line of response for search and rescue cases, marine casualty cases (onboard commercial vessels), pollution spills, and suspicious/actual terrorist activity within the COTP zone of Hampton Roads. Two individuals man the OUC desk twenty-four hours a day, standing twelve hour watch shifts. This position is an essential part of the SCC-J. Just as the brain directs the muscles to move and react to various situations, the OUC directs Coast Guard assets from seven boat stations and five patrol boats, and coordinates between Federal/State agencies to launch for emergency situations. OUCs not only direct assets to launch, they also gather essential information and enter it into a central database to ensure the entire Coast Guard is aware of all known facts for each case. Two people stand the Communications Unit (CU) watch each twelve hour period. The CU watch standers monitor the Sector's marine radios for distress calls or other abnormalities that come across the radios. They then pass this information to the OUC who begins to prosecute the case. The Vessel Arrivals Desk (VAD) is manned seven days a week for nine hours a day. This position screens all commercial vessels coming to the COTP zone based on the information provided in the Notice of Arrival (NOA). Each vessel is evaluated based on its last ports of call, cargo, flag, nationality of crew, and size, and then, in totality, assessed and assigned a level of risk associated with its arrival to the port. Depending on the risk assessment, it may have to be boarded before entering, or it may transit without any further investigation by the Coast Guard. The VAD also schedules vessel examinations to ensure compliance of safety and security standards. The Situation Unit (SU) watch stander is stood by one person in twelve hour shifts and maintains overall situational awareness of all watch positions. The SU watch stander is responsible for double checking all commercial vessels that the VAD has evaluated to ensure accuracy, keeps track of all aids-to-navigation discrepancies within the COTP zone, and assists with the tracking of all radar contacts of commercial vessels either entering or transiting through the Port of Hampton Roads. The Enforcement Duty Officer (EDO) is in the SCC-J eight hours a day during the work week and is on call the remainder of the time. The EDO is the primary point of contact for drafting COTP orders that coordinate High Interest Vessels (HIV) movements. HIVs are vessels that wish to enter the Port of Hampton Roads, but due to some elevated level of risk require additional security measures prior to entry. The final position in the Command Center is the Sensor Manager (SM) watch stander. This position is staffed by United States Navy personnel who keep track of all vessels that wish to enter the Regulated Navigation Area within the Port of Hampton Roads. SM watch standers track vessels in the Port using Radar, Automated Identification System (AIS), and cameras that are strategically placed throughout the port. AIS is a required tracking system for all commercial vessel 300 gross tons or larger, and uses a radio transponder to provide a real time positions of vessels in the area. The SM watch standers work closely with the Virginia and Maryland Pilots to ensure all vessels entering/transiting through Hampton Roads comply with safety and security regulations and are cleared to enter/transit. The Coast Guard/Navy relationship is the reason that Hampton Roads is designated as a Sector Command Center-Joint, one of only four in the entire Coast Guard.

To truly experience the heartbeat of Hampton Roads, imagine working this actual scenario that a CDO experienced in the SCC-J.

On Thursday morning November 8, 2007 at exactly 0600 in the morning, as I entered the Command Center, the sliding glass door opened up from the

*(Continued on Page 17)*

**Hazardous Cargo** *(Cont. from 5)*

this step can include establishing handling procedures, conditions for unloading/loading cargo, and training requirements. Fourth, operators create a cost-benefit assessment of the damage and create action plans for the institution and maintenance of the safety plans. This proactive approach to hazard identification mitigates the effects and costs of such incidents.

Within the hazardous cargo arena, numerous regulations complement facility operations and plans. One example is the International Maritime Dangerous Goods Code (IMDG Code) which establishes universal rules for maritime transport of dangerous goods. It includes protocols for packaging, labeling, classification, stowage, segregation and emergency response action for all interested parties including manufacturers, shippers, and intermodal transport providers and port authorities. It then becomes the port users' responsibility to adopt and follow such measures. However, most port safety protocols differ from port to port and local factors contribute to the disparities. These factors include individual jurisdiction of terminal property and the types and volumes of cargo handled, which in turn influence the activities performed on terminal property, combined with physical location issues from tidal changes, wind speeds, and temperatures. Core elements addressed by all safety procedures include the responsibilities of port authorities, terminal operators, and employees with regard to air pollution; transportation, storage and handling of harmful goods; proper equipment usage; maintenance and training policies; emergency and first aid plans; and general yard operations. For port authorities, failure to adopt, maintain, and update safe handling procedures can lead to employee illness claims and damage to infrastructure.

Direct and indirect costs resulting from worker injuries account for an economic loss between 4-5 percent of the Gross Domestic Product.[7] Direct costs include hospital-related expenses, physicians, drugs, health insurance administration and worker compensation costs, whereas indirect costs include loss of wages, costs of fringe benefits, employer retraining, workplace disruption costs (damages to equipment, tools and materials and required overtime), increased insurance premiums and loss of company goodwill.

The American Society of Safety Engineers (ASSE) states that indirect costs associated with safety failures can continue to impact organizations and are potentially 20 times greater than direct costs.[8] Negative publicity, an automatic result from workplace accidents and health scares, manifests a cost associated with the inability to attract potential employees. Other costs include workers' inability to reach productivity levels following a traumatic event, or the costs of counseling stemming from traumatic events. Therefore, by instituting a plan, the organization not only saves and improves productivity, but society perceives it as a well-respected corporate citizen.[9] Management organizations realize the negative impact of ignoring worker safety, which often translates into costly downtimes and high fines. Additionally, equipment malfunctions can result not only in worker accidents but also in delayed vessels and fewer vessel calls. For example, in January 2008, the Southampton Container Terminal experienced such delays and reduced productivity when a crane collapsed onto a berthed ship.[10] As a result, five cranes of similar design were pulled from quayside operations for inspection, thus necessitating over a dozen ships to reroute their cargo. The port experienced a 40% decline in business due to the down cranes. As investigations continue into the cause of the accident, the terminal loses business as ships and cargo are rerouted to neighboring ports. Therefore, ports and maritime facilities must assess their risk to such hazards by analyzing the types of cargoes, volumes of cargoes and handling methods to mitigate risks including spills, corrosion, and explosions that could seriously damage maritime infrastructure. ❖

[7] *Occupational Health.* (n.d.). Retrieved July 26, 2008, from the World Health Organization: www.who.int/occupational_health.
[8] Engineers, A. S. (2002). *White Paper: The Return on Investment for Health and Environmental Management Programs.*
[9] Russell, S. E. (2008). Port Workers and Safety. In W. K. Talley, *Maritime Safety, Security and Piracy,p. 20. London: Informa.*
[10] Porter, J. (2008, February 19). Ships steer clear of Southampton. *Lloyd's List*.

Legal Insights

# The Maritime Transportation Security Act of 2002

by Timothy P. Clancy, JD, Senior Program Manager, Cyber/IT

One of the most important pieces of federal homeland security legislation is the Maritime Transportation Security Act (MTSA). Passed by Congress in 2002, MTSA sets out a series of policies and procedures to better secure U.S. ports and waterways from acts of terrorism. This legislation and its corresponding regulations have had a dramatic and far-reaching influence on security practices across the complex international system of maritime transportation and commerce.

In the United States, government security responsibilities for the maritime sector — as in many CI/KR sectors — have been shared traditionally by a complex mix of Federal, State and local authorities. Port authorities are chartered primarily by State or local government entities and are a mix of private sector, quasi-government and government entities. Traditionally, seaports have been subject to limited federal regulation — such oversight and regulation was largely left to the States and localities.

The events of September 11 changed this regulatory paradigm dramatically. In the months following, there was a great deal of concern raised in Congress and internationally about the vulnerability of ports and waterways to potential terrorist attacks. As a result, Congress and the Executive Branch acted swiftly to radically alter port security practices.

MTSA and its corresponding regulations were central to this radical new era of U.S. maritime security. MTSA and subsequent homeland security laws established broad federal authority to regulate and police maritime activities in the United States both on land and in domestic waters.

There is no question that the federal government has the power under the Constitution to assume this authority and responsibility. Security of navigable waterways in the United States has always been the responsibility of the federal government, carried out by the United States Coast Guard. The federal government also has the constitutional authority to regulate interstate and foreign commerce and consequently has wide powers to regulate port practices.

An important feature of the U.S. maritime and port security regime under MTSA is that it closely tracks to international port security standards. Also adopted in the aftermath of September 11, the International Ship and Port Facility Security Code (ISPS) was promulgated by International Maritime Organization (IMO) under the authority of the International Convention for the Safety of Life at Sea (SOLAS).

The ISPS Code is a two-part document providing measures and procedures to prevent further acts of terrorism which threaten the safety of ships and the security of passengers and crews. The ISPS Code is intended to provide guidance while allowing individual countries to adopt their own security measures and procedures based on the Code.

These international standards entered into force in July, 2004, the same time as many of the key provisions of MTSA. While ISPS is a mixture of mandatory regulations and voluntary guidance, however, MTSA makes all ISPS provisions mandatory and gives the Coast Guard and DHS strong authority to enforce MTSA provisions.

The goal of MTSA is to establish a more consistent security regime for ports across the U.S. to better identify and deter threats. The Act is built on a risk-based methodology and is focused on

*(Continued on Page 14)*

**Legal Insights** *(Cont. from 13)*

elements of the maritime sector that pose significant risk to life and property, such as tankers, large passenger vessels, offshore oil and gas facilities and other seaport facilities that handle hazardous materials or cargo. The legislation requires both vessels and port facilities to conduct vulnerability assessments. Vessels and facilities must also develop and implement certain security plans. These security plans may include passenger, vehicle and baggage screening procedures; security patrols; establishing restricted areas; personnel identification procedures; access control measures; and/or installation of surveillance equipment.

Another important aspect of MTSA is its provisions that encourage the sharing of information on threats and vulnerabilities across layers of government and the private sector. These provisions seek to shield certain sensitive and classified security information about critical port facilities from public disclosure. Indeed, as was discussed in the May 2007 CIP Report, these MTSA provisions were used as a template for similar information protection provisions in the Chemical Facility Anti-Terrorism Standards (CFATS) legislation. MTSA also created certain mechanisms at each port — Area Maritime Security Committees, for example — to include key private-sector port stakeholders as well as State and local law enforcement to enhance coordination and information sharing.

MTSA and its subsequent law, the SAFE Port Act, have not been without controversy. The implementation of the Act's requirements for a national maritime worker biometric identification card for access to vessels and critical port facilities has been contentious. DHS has begun enforcement of the new Transportation Worker Identification Credential™ (TWIC) requirement this month, while giving some ports in the South and West regions some leeway for full implementation of TWIC. Once TWIC is implemented, all port workers must display biometric TWIC credentials for unescorted access to secure areas of the ports.

MTSA is a landmark example of homeland security legislation. Crafted in cooperation and in concert with international security standards organizations, it swept away a patchwork security regime for the maritime sector. By making most international guidelines mandatory, the United States led by example in greatly strengthening maritime security practices globally. The Act has also had an impact on other CI/KR sectors: subsequent legislative attempts to more tightly regulate certain sectors have used MTSA as a template for a risk-based methodology and improved information sharing.

The Federal government has taken a much stronger role in regulating and policing the nation's ports and maritime transportation system since September 11. MTSA represents the core of this effort. ❖

NPS *(Cont. from 3)*

has been the subject of a thesis by Edward Pigeon, and work is ongoing.

The other effort consists of an analytic model called PORTZ whose purpose is to determine optimal dispatching rules. The queue is treated analytically in PORTZ, but only in equilibrium; that is, the delay is assumed to be indefinite. The intention is that WCPORT and PORTZ will be complementary, with PORTZ suggesting modifications to the dispatch rules of WCPORT, and with each serving as a verification tool for the other.

Optimum port security will require collaboration between all key parties. MIST is addressing the collaboration requirements for maritime domain awareness and security. It is currently sponsored by the Naval Postgraduate School's MDSRP and the Department of Transportation's Maritime Administration (MARAD). MIST was stood up in the summer of 2008 as a prototype program to help the federal maritime domain awareness effort incorporate the input of the private sector into the sharing of maritime threat information. The National Maritime Security Policy, the Intelligence Reform and Terrorism Prevention Act of 2004, and the National Strategy for Information Sharing have all called for increased participation by the private sector in improving maritime domain awareness. The MIST effort supports this call for action by facilitating cooperation between local, private sector stakeholders and federal stakeholders. Leveraging the private sector to enhance information sharing could result in a potential increase of resilient response to emergencies and disasters affecting critical maritime infrastructure.

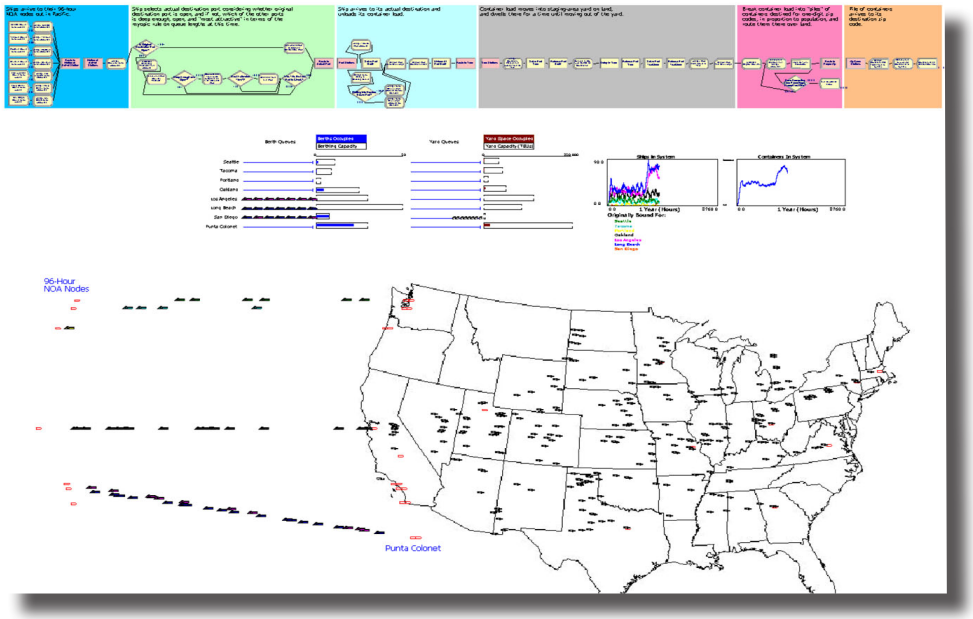


**Figure 2. Screenshot of Arena simulation logic model (top flowchart) and animation (bottom) of west coast container-port operations. At the time of this screen shot, both the ports of Los Angeles and Long Beach were closed, so vessel traffic was being diverted to other ports, mostly the proposed port in Punta Colonet, Mexico.**

Conceived as a multi-agency response, MIST worked closely in 2008 with the U.S. Coast Guard, MARAD, the Office of Global Maritime Situational Awareness (OGMSA), Global Maritime and Air Intelligence Integration (GMAII), Customs and Border Protection (CBP), and state and local government agencies to conduct a pilot workshop with private sector shipping at the Port of Long Beach/Los Angeles (LA/LB). The goal of the workshop was to prototype a process for uncovering private sector issues and solutions related to the sharing of threat information at the local level. The workshop was well received and provided actionable information regarding the general needs of the private sector. For example, the workshop delivered useful data about how to align private sector incentives with national strategy, leverage key local practices, streamline government interactions, collaborate with communities of interest, and improve information quality.

In May of 2009, MIST will look to address information sharing coordination and best practices in the Seattle/Tacoma maritime region. It will do so by replicating

*(Continued on Page 18)*

**Port Security** *(Cont. from 9)*

attack — instituting and installing measures that enhance resiliency, response, and rapid recovery. All of this contributes to port security while positively impacting the risk exposure to industry and those that insure them.

**The CHSF Grant Approach**

The Commonwealth Homeland Security Foundation (CHSF), using an innovative public-private approach, desires to contribute to the development and implementation of solutions that significantly improve the security of the commercial and military maritime port facilities in Hampton Roads against man-made or natural disasters. In particular, the protection and sustainability of the critical supply chain, intermodal facilities, and the workforce associated with the port region are key concerns.

To this end, the CHSF plans to award a series of grants to its university consortium members — George Mason University, Old Dominion University, The College of William and Mary, The University of Virginia, Virginia Commonwealth University, and Virginia Tech — to identify, develop, and implement effective and affordable solutions to enhance port security and the associated critical supply chain.

The CHSF is appealing initially to industry located in Virginia or others with interests in the Hampton Roads port security to fund the initial strategy grant. This should include the insurance industry that has a distinct interest in approaches that reduce the exposure of the port and its associated industry to terrorist attacks.

The initial grant will focus on optimal strategies to secure the Hampton Roads port region in a comprehensive manner. In developing those strategies, the CHSF will employ the research and development capacity of its university consortium members to work with stakeholders in the Hampton Roads region — including all industry sectors, maritime and related, as well as Federal, State, and local government — to craft a range of viable strategies to address port security.

When this is accomplished, the CHSF will assemble all stakeholders to further refine and "down select" the most achievable strategy and begin the process of follow-on grants to focus on the specific application of optimal solutions, including best practices and technologies, to secure the port of Hampton Roads, its critical supply chain, intermodal facilities, and its workforce from disruption. In doing so, the CHSF will serve as a strategic match-maker between Federal and State dollars and funding from the private sector to deploy strategies in a coordinated public-private partnership, thereby leveraging the resources, talent, and insight of those entities with a major interest in the security of the Hampton Roads port.

The strategies that the CHSF envisions pursuant to the initial research should draw on selected top-level strategic objectives for maritime security as outlined in *The National Strategy for Maritime Security*, September 2005. They include:

1. Preventing terrorist attacks and criminal hostile attacks;
2. Protecting maritime-related population centers and critical infrastructure; and
3. Minimizing damage from attacks and ensuring expedient recovery.

**Conclusion**

The vulnerabilities, risks, and consequences of an attack on our vital ports and critical supply chain — particularly on the Commonwealth's premier resource in Hampton Roads — are real, present, and dangerous to our economic well-being. The need for a public-private approach offered by the CHSF is essential to the development of a comprehensive strategy incorporating the best practices and available technology to secure our critical supply chain in and near maritime port facilities. Government lacks the funding to secure the critical infrastructure that largely resides in private hands. Private industry cannot afford a disruption in the flow of the critical supply chain and neither can governments — at all levels — that depend on industry and business viability.

*(Continued on Page 18)*

**USCG** *(Cont. from 11)*

communications room, "Mr. Rooney, I hear Sector North Carolina talking to a cruise ship that is taking on water and just ran aground in the Inter-Coastal Waterway (ICW)!" I remember thinking it was going to be a very busy day for North Carolina! As I walked over to the Command Duty Officer desk, I heard a radio transmission on channel 16 from North Carolina, "Captain, how many people are onboard your vessel?" The master replied "65 both crew and passengers total." I remember thinking the master seems very calm and under control. As I continued my walk to the CDO desk, I heard Sector North Carolina request the vessel's GPS position. Immediately, I noticed position as the master passed it to North Carolina. My thoughts were once North Carolina gains control of the situation, I will call and offer assistance or support. Before I could sit down and log onto the computer, I heard Mr. Rooney say, "Sir, the position they just passed plots in our Area of Responsibility." I immediately got up and walked over to him, "Where?" He replied, "Pungo, Virginia Beach area of the ICW." My first thought was, "How in the world, are we going to get 65 people off of that ship?" My adrenaline started to pump and I wondered if the other watch standers could hear my heart beat. I looked at Mr. Rooney and said, "Call District and request a helo and direct Station Portsmouth to launch." I remember thinking we needed to get someone on scene and quick! I immediately returned to the CDO desk and initiated the Critical Incident Communications (CIC) conference for a major marine casualty. The conference call for the CIC brief included personnel from Coast Guard Atlantic Area and Pacific Area Command Centers, and Coast Guard Headquarters Command Center, located in Washington, D.C. I briefed the case, "This morning at 0600 a cruise ship hit an object and is taking on water in the Inter-Coastal Waterway in the vicinity of Pungo which is in Virginia Beach, VA. Once the master noticed that he was taking on water at a rapid rate, he deliberately ran the ship aground. At this time, the Inter-Coastal Waterway is partially blocked to commercial and recreational traffic and there are 65 people onboard including the crewmembers. We have launched Air Station Elizabeth City to deliver pumps, as well as Station Portsmouth to control vessel traffic. The master of the vessel reports no injuries and the vessel is stable at this time." The Headquarters Command Center replied, "Sounds good, I want another brief in thirty minutes." Immediately I hung up the phone and briefed my Chain of Command. I discussed the possibility of a possible terrorist attack. Utilizing the Captain's COTP authorities, I directed a safety zone be established around the vessel, sent Coast Guard personnel on scene to interview the master of the cruise ship, and notified the Navy, Air Force, and Army of the incident. Once the first of the Coast Guard assets from Station Portsmouth arrived on scene, I directed them to get the passengers and non-essential crewmembers off of the cruise ship and to establish a 200 yard safety zone around the vessel. Shortly, marine units arrived on scene from Virginia Beach, Chesapeake, and Virginia Marine Police. Station Portsmouth crewmembers interviewed the master of the vessel and determined that this incident was not a deliberate attack. For the safety of the public and first responders, the Inter-Coastal Waterway was closed by the Captain of the Port from Alligator River Swing Bridge in Tyrrell County, NC, to the Great Bridge Locks in Chesapeake, VA. Once the safe evacuation of all passengers and crew was complete, the focus shifted to containing and stopping the pollution and finally un-grounding and repairing the cruise ship. After three days of conducting pollution clean-up, temporary repairs were made to the hull of the cruise ship and the vessel was re-floated at high tide and towed to a shipyard for permanent repairs. Less than a day later, the Army Corp of Engineers discovered a large submerged object in the channel that the cruise ship struck causing the vessel to take on water.

However many similarities there are between the human body and the SCC-J, there is one major difference: The SCC-J is not given time to recover from a long exhausting case, but must rebound instantly to be ready for the next maritime situation and response. The SCC-J must balance all port information and maintain maritime domain situational awareness at

*(Continued on Page 18)*

**Port Security** *(Cont. from 16)*

Insurance companies know, as they experienced after 9-11, that a major disaster confounds their ability to offer insurance products to businesses. This cooperative public-private partnership venture proposed by the CHSF to identify the right strategy to secure our ports is the best way to ensure that our security requirements for critical supply chain are addressed.

Moreover, when the Federal Government takes note of the commitment of this public-private venture, they will see the efficacy of the concept and will be more likely to bring Federal dollars to the application of effective solutions.

In the end, the CHSF approach to this problem provides a "win-win" strategy for both the public and private sectors while, most importantly, making it all the more difficult for our enemies to disrupt the economic viability so essential to our way of life. ❖

* *L. Scott Lingamfelter is the President of the Commonwealth Homeland Security Foundation (CHSF). After 28 years of active service with the U.S. Army, he retired as a Colonel in 2001. That same year, he entered another phase of public service as an elected member of the House of Delegates of the Virginia General Assembly, where he currently serves on the Appropriations Committee, the Education Committee, and the Militia and Public Safety Committee.*

**NPS** *(Cont. from 15)*

the workshop process from LA/LB, enhancing the social network tool hosted by MARAD on MarView, and completing a field study to capture "a day in the life" of a facility security officer working in the private maritime industry as it relates to information sharing. The notion of MIST is that a better understanding of the private sector network and perspective on maritime security, paired with a more solid bridge for communication and collaboration with government, will result in a more resilient port environment.

This article highlights only a small sampling of the more than 25 different Maritime Defense and Security Research Programs currently on-going at NPS. In addition, the MDSRP publishes a monthly e-newsletter, the SITREP, which is a collaborative venue to highlight not only NPS research, but maritime-related research of all agencies, research labs, industry, and other stakeholders interested in Maritime Defense and Security issues. If you wish to receive the SITREP, or have any questions regarding this article, please contact Ms. Rita Painter at rpainte@nsp.edu. ❖

**USCG** *(Cont. from 17)*

all times. The Operational Commander uses the SCC-J as a command and control platform to coordinate missions to achieve operational effectiveness and strive to guarantee port safety and security. ❖

### Upcoming Conference Reminder


The CIP is co-hosting, with the Security Analysis and Risk Management Association (SARMA), the 3rd National Conference on Security Analysis and Risk Management from June 16-18, 2009, in Arlington, VA.

**Confirmed Keynote Speakers include:**

- Mr. Peter F. Verga, Principal Deputy Under Secretary of Defense for Policy
- Ms. Tina Gabbrielli, Director of the Office of Risk Management and Analysis, U.S. Department of Homeland Security
- Mr. Roger W. Cressey, President of the Good Harbor Consulting Group and former Director for Transnational Threats on the National Security Council

For additional information, to include Agenda, Early Bird Registration (ending May 1st), Sponsor and Exhibitor prospectus, please visit http://sarma.org/events/pastevents/3rdannualconferenc/.

### Release of Paper on Regional Risk Analysis

Complementing CIP's efforts on risk, to include co-hosting the Security Analysis and Risk Management Association's annual conference and past publication of a risk monograph, CIP recently posted a paper on its website addressing the topic of regional risk analysis. Authored earlier this year by Liz Jackson of the Federal Emergency Management Agency's Office of National Capital Region Coordination (NCRC), William McGill of The Pennsylvania State University, and Chris Geldart of the URS Corporation and former Director of NCRC, "Regional Risk Analysis: A Coordinated Effort" discusses the analysis of homeland security risk in a multi-jurisdictional environment and offers insight on key considerations of strategic risk analysis. The paper abstract is below.

*Risk assessments are being conducted more frequently as localities seek to enhance their preparedness and mitigate and manage risk with regard to all-hazard events. In the National Capital Region (NCR), a risk analysis was recently conducted that built on previous assessments and further contributes to a regional risk picture. This paper describes the development of the 2008 NCR Strategic Hazards Identification Evaluation for Leadership Decisions (NCR SHIELD) regional risk analysis, which includes both a risk assessment and strategic approach to risk management. It begins with a discussion of the difficulties that must be overcome to ensure executive decision makers align their thinking and pursue a common goal of assessing regional risk to inform their decision-making processes and, in turn, how they mitigate and manage risk at the strategic level. The paper concludes with information on the conduct of NCR SHIELD and outlines a stakeholder-engaged process for further developing a multi-jurisdictional approach to risk management.*

The full paper is available on the CIP website at http://cip.gmu.edu/research/Regional_Risk_Analysis.php.

**Transportation** *(Cont. from 7)*

international maritime commerce. The total estimated cost of this closure was $500M - $1B.

**Section II: Trade Resumption/ Resiliency Plan (TR/RP) - Building Resiliency into the MTS**

Examples such as the 2008 Hurricanes and the Mississippi River oil spill previously discussed illustrate the importance of immediate response and recovery operations to support an effective recovery of the MTS. It also illustrates the role that contingency planning plays in preparing for these high-consequence events. Considering the economic costs and the unpredictable nature of waterway and port closures, it is of vital importance to the economic security of the United States that alternatives to this transportation segment are analyzed and appropriate response and planning doctrines developed.

A security program focused on layered initiatives, programs, and cooperative work with stakeholders throughout the international supply chain provides the greatest flexibility and support to reduce the chances of a breach in the security network. A holistic supply chain strategy can help reduce the risk of disruptions at the marine ports, or even while the vessel is at sea where it can be vulnerable to pirate attacks or other incidents prior to reaching its destination. An important component of a holistic risk management framework is the development and implementation of a Trade Resumption/Resiliency Plan (TR/RP), as well as other strategic risk management plans and response and recovery programs.

The TR/RP is an important component of the DHS Port Security Grant Program (PSGP) that is designed to identify initiatives that would aid the preparedness of regional port communities by adding resiliency in the basic systems that support port commerce and trade. The TR/RP supports and complements other strategic maritime regional planning activities, including the Area Maritime Security Plan (AMSP), the Area Contingency Plan (ACP), and the Strategic Risk Management Plan (SRMP) and others as highlighted in the figure below.

The goal behind these initiatives is to build resiliency into the MTS by identifying gaps in security, authorities, capabilities, capacities, competences and partnerships across the security continuum of awareness, prevention, protection, response and recovery. These efforts can enhance the system's ability to operate under normal conditions, and improve its capability to address a Transportation Security Incident (TSI) or an Incident of National Significance (INS).

As Figure 1 below highlights, following a TSI or an INS, performance of the port (i.e. measured by container throughput or other productivity measures) will be impacted during the immediate response stage as well as in the early recovery stages. Response and immediate MTS recovery is usually led by government entities, such as the U.S. Coast Guard's efforts previously mentioned, with the assistance of the private sector and begins within 1-3 days of the event and last for 90 days or longer. Resumption of trade is primarily a function of the private sector who

*(Continued on Page 21)*

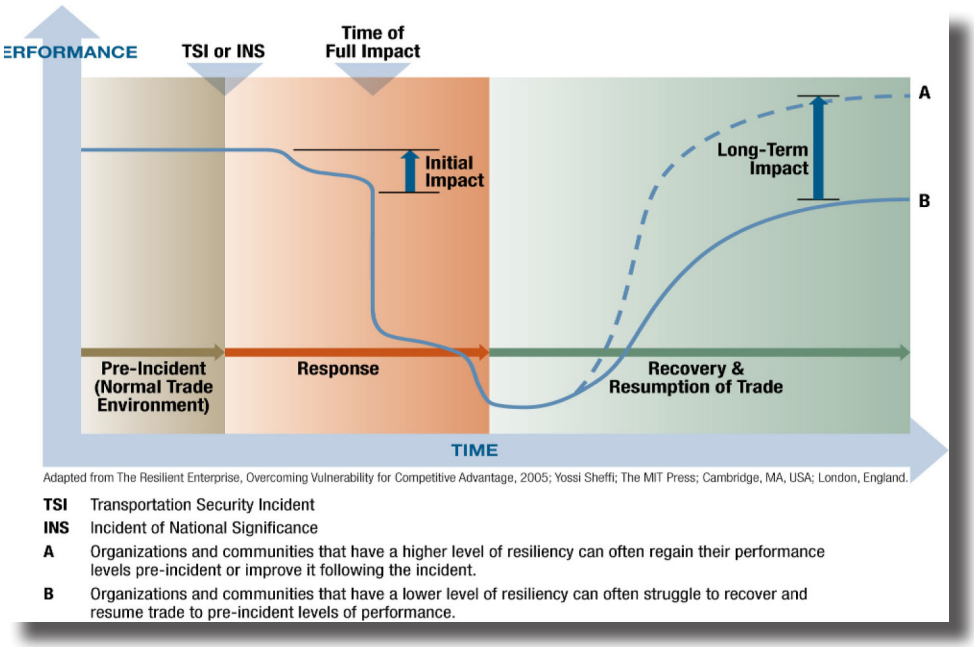


**Figure 1. Conceptual Framework for Response and Resumption of Trade Following a TSI or INS**

**Transportation** *(Cont. from 20)*

own most of the assets and can take months to years.

**Section III: The Experience of the Lower Mississippi River (LMR)**

Evidence of the implementation of this national strategy can be found in the planning work recently completed in the Lower Mississippi River (LMR). The Ports in the LMR[5] are a critical gateway for imports and exports for the United States, especially for food products, petroleum products, and chemicals. To increase the resiliency of the LMR MTS, which extends from Baton Rouge to the Gulf of Mexico, the LMR Ports joined forces to form the Port-Wide Strategic Security Council (PSSC). The PSSC has launched some important initiatives to increase its preparedness position and collaborate on security grant applications. One of the activities the PSSC has commissioned is a Trade Resumption and Resiliency Plan (TR/RP) to identify gaps in the current LMR operating environment and to identify respective capital investments and initiatives that can help to address the critical institutional and planning, waterway, and landside issues in the region.

With the support of DHS, the Ports of the LMR, and others across the U.S., are increasing coordination with regional, local, and federal agencies and the private sector to enhance its capabilities to protect the MTS. Under the leadership of the U.S. Coast Guard, local law enforcement agencies, and other key sector stakeholders, it is also enhancing system-wide situational awareness and communications capabilities to detect, deter, mitigate, respond, and recover from disruptive events such as the ones discussed in this article or other high consequence events.

As the nation prepares to implement the American Recovery and Reinvestment Act 2009 Projects, it will be important for the MTS stakeholders to continue to coordinate closely so that competing demands don't distract resource allocation and attention from the critical infrastructure and key resources essential for trade and the economic well-being of our nation. The focus for future transportation investments needs to be on smart infrastructure that leverages technology and adds redundancy, capacity, flexibility, and control into the transportation system to ensure the nation's competitiveness, as well as safe and secure supply chain operations. ❖

**Figure 2. Ports of the Lower Mississippi River (LMR)**


[5] The LMR Ports includes the Port of South Louisiana, Port of New Orleans, the Greater Baton Rouge Port, the Plaquemines PHT District, and the St. Bernard PHT District.

The Center for Infrastructure Protection works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1