U.S. Department of Homeland Security

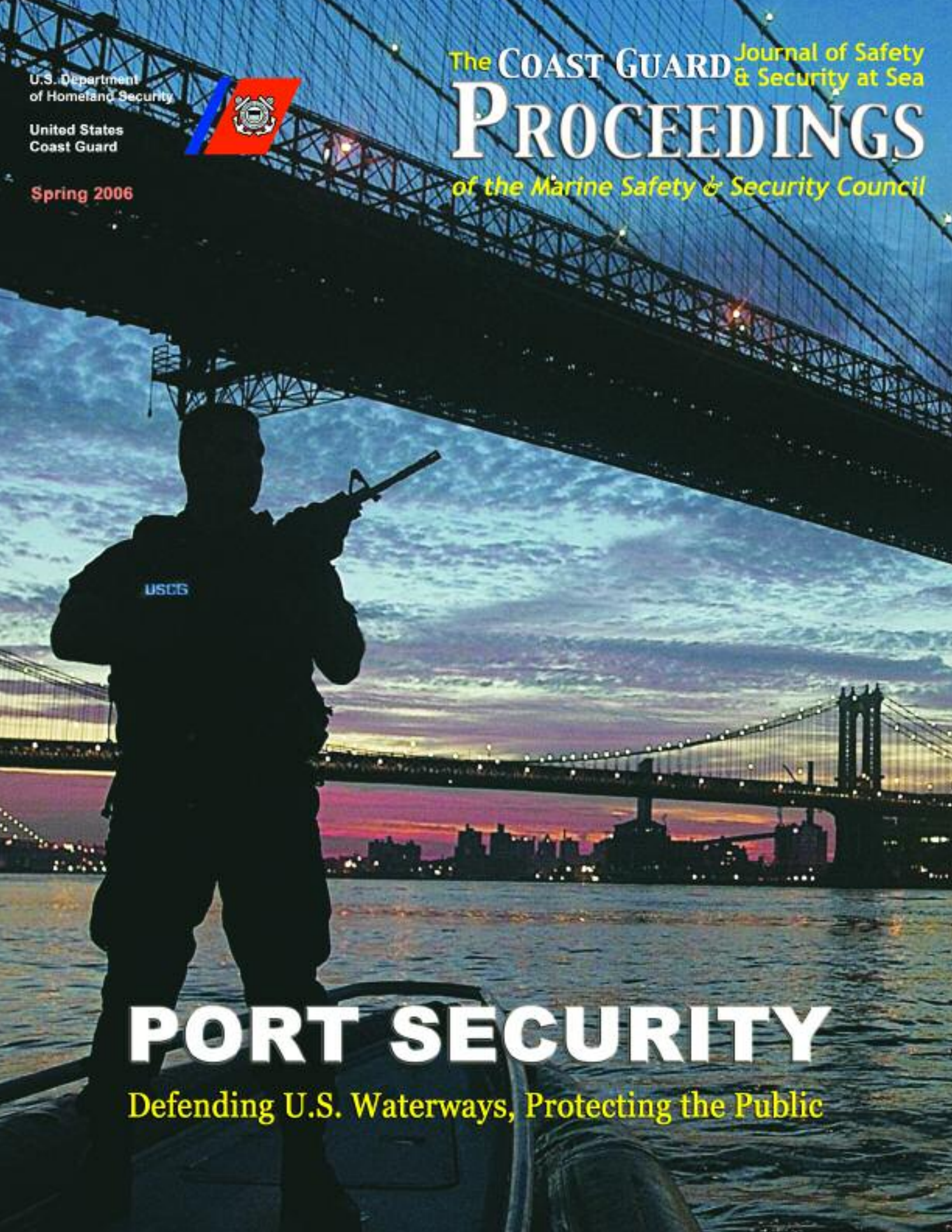
United States Coast Guard

Spring 2006

The Coast Guard Journal of Safety & Security at Sea

PROCEEDINGS

of the Marine Safety & Security Council



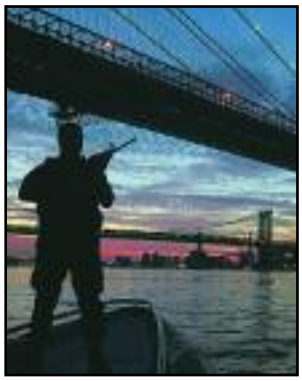
PORT SECURITY

Defending U.S. Waterways, Protecting the Public

PROCEEDINGS

Spring 2006

Vol. 63, Number 1



On the Cover

Petty Officer Jason Miele, a member of the Coast Guard Maritime Safety and Security Teams (MSST), stands guard in the East River near the Brooklyn Bridge. The MSSTs were created in direct response to the terrorist acts of Sept. 11, 2001.
U.S. Coast Guard photograph by PA1 Tom Sperduto.

Awareness

6 **Global Maritime Security**
CDR John Caplis

10 **Innovations for Port Security**
Dr. Marc B. Mandler

13 **The Deepwater Program**
RADM Patrick M. Stillman

19 **Safely Securing U.S. Ports**
LCDR Brady Downs

23 **HOMEPORT**
LCDR Mark Hammond, LCDR Karrie Trebbe

26 **America's Waterway Watch**
Chief Petty Officer Penny Collins, LT Kenneth Washington

29 **Three-Dimensional Awareness**
ENS Joseph Azzata

32 **On Watch**
Mr. William R. Cairns

36 **Maritime Domain Awareness**
Mr. Guy Thomas

Prevention

39 **Keeping U.S. Waters Safe and Secure**
LCDR Mark Willis, LCDR Malcolm McLellan

42 **Maritime Security Training**
LCDR Derek A. D'Orazio

45 **International Port Security Program**
Mr. Mike Brown

49 **Cargo Security**
Mr. Basil Maher, LCDR Mike Dolan

52 **Central California Area Maritime Security Committee**
LCDR Anthony C. Curry, Mr. Robert T. Spaulding

55 **Port Coordination in the Largest U.S. Petrochemical Complex**
LCDR D. Hauser

60 **Asymmetric Migration**
LCDR Mike Cunningham

63 **The Evolution of TWIC**
LCDR Jonathan Maiorine

66 **Port State Control Examination**
LT Ryan Allain, LT Craig Toomey

69 **Increased Port Security**
Mr. Chris Austen

73 **National Maritime Security Advisory Council**
Mr. John Bastek

Protection

76 **Airborne Use of Force**
LCDR Melissa Rivera, CDR Aaron C. Davenport

79 **Safeguarding the United States**
LCDR Brad Kieserman, LCDR Christopher F. Murray, LCDR Mike Cunningham

83 **Maritime Safety and Security Teams**
CDR Aaron C. Davenport

84 **Port Security**
Mr. Kenneth McDaniel

Response and Recovery

87 **National Response Options Matrix**
CAPT Wayne C. Dumas

89 **Counterterrorism Force**
LCDR Jose L. Rodriguez, LTC Michael Kichman, U.S. Army (ret)

On Deck

4 **Assistant Commandant's Perspective**
RADM R. Dennis Sirois and RADM T. H. Gilmour

5 **Champion's Point of View**
RDML Craig Bone

Nautical Queries
92 Engineering
94 Deck

Cover Photo Courtesy of PA1 Tom Sperduto.

Back Cover Photos: Courtesy of PA1 Daniel Tremper, PA3 Donnie Brzuska, PA3 Christopher Grisafe, and PA3 Kelly Newlin.

Icon Credits:
All are USCG illustrations.

Copyright © 2006 USCG and its licensors.

Assistant Commandant's Perspective

by RADM R. Dennis Sirois
Assistant Commandant for Response

by RADM T. H. Gilmour
Assistant Commandant for Prevention

Throughout our nation's history, the oceans, lakes, and rivers have been vital to our prosperity and to our security. Today, we continue to depend on these maritime highways for a Global Transportation System that delivers goods and materials to factories and stores across our country. The oceans and waterways are also favorite areas for recreation. For most of our history, warfare and perils such as piracy were first on our minds when we thought of threats to maritime security. Today, however, we also face a determined and resourceful terrorist enemy who would turn the vehicles of peaceful transportation—including ships, as well as planes, trains, and trucks—into deadly instruments of destruction.

A government has no higher duty than to protect its citizens. The president has called for a fully coordinated government effort to safeguard our interests in the Global Maritime Domain. Because a robust international effort is essential to achieving this objective, the president required that international outreach be an integral part of the strategy. We are committed to building and sustaining alliances within the community of nations to help achieve the goal of a more secure world. At a time when global terrorism, rogue states, international crime, and weapons of mass destruction threaten the world's oceans and waterways, no one nation can accomplish this goal alone. Success will come through the hard work of a powerful coalition of nations, focused on protecting the world's maritime interests.

To safeguard the maritime domain, the United States must forge cooperative partnerships and alliances with other nations, as well as with public and private stakeholders in the international community. We cannot and should not attempt to patrol every coastline, inspect every ship, screen every passenger, or peer into every container crossing the world's oceans. To foster stronger partnerships within the international community, the United States must have a coordinated and consistent approach to building international support and cooperation to reinforce global maritime security. We will propose ideas, and encourage others to do the same. We will speak frankly. We will also listen carefully. We will work together. Security must be a team effort.

The United States Coast Guard takes a layered and cooperative approach to maritime security, utilizing the expertise of federal, state, and local authorities as well as that of the private sector and of international partners to create a system of security measures to protect one end of a sea-based journey to the other. The goal is to harmonize security measures and economic growth. The layered, often interlocked or interrelated, security measures are designed to make it harder for terrorists or transnational criminal groups to attack the United States or harm our interests. These layered measures seek to protect the American public and the maritime commerce chain.

What follows in this issue of *Proceedings* is an overview of our current maritime security programs and initiatives.

ADM Thomas H. Collins
Commandant
U.S. Coast Guard

The Marine Safety & Security Council *of the* United States Coast Guard

RDML John E. Crowley Jr.
Judge Advocate General
Chairman
U.S. Coast Guard

RADM T. H. Gilmour
Assistant Commandant
for Prevention
Member
U.S. Coast Guard

RADM Dennis Sirois
Assistant Commandant
for Response
Member
U.S. Coast Guard

CDR David L. Nichols
Executive Secretary
U.S. Coast Guard

Steven Venckus
Legal Advisor
U.S. Coast Guard

View PROCEEDINGS Online at www.uscg.mil/proceedings

Editorial Team

Lisa H. Bastin
Executive Editor

Albert G. Kirchner Jr.
Acting Executive Editor

Barbara Chiarizia
Managing Editor

Ann Aiken
Art Director

Proceedings (ISSN 1547-9676) is published quarterly by the Coast Guard's Marine Safety, Security & Environmental Protection Directorate, in the interest of safety at sea under the auspices of the Marine Safety & Security Council. Special permission for republication, either in whole or in part, except for copyrighted material, is not required, provided credit is given to *Proceedings*. The views expressed are those of the authors and do not represent official Coast Guard policy.

Editorial Contact

email: ARL-DG-NMCProceedings @uscg.mil

Editor, *Proceedings* Magazine
U.S. Coast Guard
National Maritime Center
4200 Wilson Blvd., Suite 730
Arlington, VA 22203-1804

Subscription Requests/Changes

Please include mailing label information when changing address.

email: ARL-DG-NMCProceedingsDist @uscg.mil

Subscriptions, *Proceedings* Magazine
U.S. Coast Guard
National Maritime Center
4200 Wilson Blvd., Suite 730
Arlington, VA 22203-1804

Champion's Point of View

by RDML Craig E. Bone
U.S. Coast Guard Director of Inspection & Compliance Directorate

Nationally and internationally there has been a substantial increase in the security of the Global Maritime Transportation System since the terrorist attacks of September 11, 2001. The implementation of the International Port and Facility Security (ISPS) Code in July 2004 and the Maritime Transportation Security Act (MTSA) of 2002 has established a sound foundation of preparedness throughout all segments of the maritime transportation system.

While much has been done, there is no room for complacency. This *Proceedings* issue is meant to acknowledge efforts and challenges to work systematically to address innumerable potential threats. We need to also consider the lessons learned from natural disasters, such as Hurricane Katrina, and modify our planning to account for previously unforeseen obstacles in preventing, responding to, and recovering from devastating incidents.

Many of the articles covered in this issue represent the first public description of the Coast Guard's new capabilities and capacities in port security. There are more than 70 current initiatives that have either been completed, or are in the process of completion, which will strengthen the foundation of MTSA and ISPS. There are significant challenges to solidify security in the global maritime transportation system. Government agencies and industry will need to continually address and share best practices concerning threat and risk models, utilization of new technologies, development of needed standards for identification cards, vessel tracking systems, and training.

In this issue, we solicited a variety of topics and viewpoints from the project leaders in the Coast Guard and other partner stakeholders. I would like to sincerely thank the authors for their time and talent putting together contributions for this edition. We have no choice but to move forward and institutionalize port security practices worldwide, the threat is real and the risk and consequences severe. Terrorists will continue to look for ways to exploit the gaps and vulnerabilities within the Global Marine Transportation System and parts of our critical infrastructure. We must remain vigilant and tenacious in our efforts, if we are to thwart terrorism.

Global Maritime Security

An overview of the National Strategy for Maritime Security.

by CDR John Caplis
U.S. Coast Guard Office of Strategic Analysis

On December 21, 2004, President George W. Bush signed Maritime Security Policy National Security Presidential Directive 41/Homeland Security Presidential Directive 13 (NSPD-41/HSPD-13) with the goal of establishing U.S. policy, guidelines, and implementation actions to enhance homeland security by protecting U.S. maritime interests. It directs that all U.S. government maritime security programs and initiatives be coordinated to achieve a comprehensive and cohesive national effort involving appropriate federal, state, local, and private sector entities.

The Secretaries of Defense and Homeland Security were jointly charged with leading a collaborative interagency effort to craft a National Strategy for Maritime Security (NSMS) and eight supporting plans.

To successfully achieve their objectives, the National Strategy for Maritime Security and supporting plans must consider the following statements:

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

The National Strategy for Maritime Security strives for a holistic approach in dealing with the broad array of threats to security within the maritime domain, addressing activities that span from prevention to post-incident recovery. The NSMS strives to achieve its objectives through five cross-cutting strategic actions:

- **Enhancing international cooperation to ensure lawful and timely actions against maritime threats.** New initiatives are needed to ensure that all nations fulfill their responsibilities to prevent and respond to terrorist or criminal actions with timely and effective enforcement. The United States will continue to promote the development of cooperative mechanisms for coordinating regional measures against maritime threats that span national boundaries and jurisdictions. The United States will also work closely with other governments and international and regional organizations to enhance the maritime security capabilities of other key nations.

- **Maximizing Domain Awareness to support effective decision making.** A key national security requirement is gaining an effective understanding of all activities, events, and trends within the Maritime Domain that could threaten the safety, security, economy, or environment of the United States and its people. Domain awareness enables the early identification of potential threats and enhances appropriate responses, including interdiction at an optimal distance with capable prevention forces.

- **Embedding security into commercial practices to reduce vulnerabilities.** Private owners and operators of infrastructure, facilities, and resources are their own first line of defense and should embed into their business practices scalable security measures that reduce systemic or physical vulnerabilities. Embedding security practices rests upon the implementation and continual improvement of key legislation, such as the Maritime Transportation Security Act of 2002, and International Maritime Organization requirements, such as the International Ship and Port Facility Security Code.

- **Deploying layered security to unify public and private security measures.** Achieving maritime security is contingent upon executing a layered security system that integrates the capabilities of governments and commercial interests. The public and private sectors, acting in concert, can only prevent terrorist attacks and criminal acts by using diverse and complementary measures, rather than relying upon a single solution.

- **Assuring continuity of the marine transportation system to maintain vital commerce.** The United States must be prepared to maintain vital commerce in the aftermath of any terrorist attack or other similarly disruptive incidents that occur within the Maritime Domain. The response to such events should not default to an automatic shutdown of the marine transportation system; instead, the United States will be prepared to disengage selectively only designated portions and immediately implement contingency measures to ensure the public's safety and continuity of commerce.

The National Strategy for Maritime Security focuses on four main objectives:

- preventing successful terrorist attacks and criminal or hostile acts;
- protecting maritime-related population centers and critical infrastructure;
- minimizing damage and expediting recovery; and
- safeguarding the ocean and its resources.

The National Strategy for Maritime Security is further guided by the following principles:

- freedom of the seas must be preserved for legitimate military and commercial navigation;
- maritime security efforts should seek to facilitate global commerce and prosperity; and
- individual civil liberties and rights guaranteed by the U.S. Constitution, as well as the international rule of law, must be preserved.

The eight supporting plans of the National Strategy for Maritime Security cover the areas of:

- National Maritime Domain Awareness (MDA);
- Global Maritime Intelligence Integration;
- Domestic Outreach Engagement;
- Coordination of International Efforts and International Outreach;
- National Maritime Operational Threat Response;
- National Maritime Infrastructure Recovery;
- Maritime Transportation System Security; and
- Maritime Commerce Security.

Coast Guard's Role in Implementing National Strategy

NSPD-41/HSPD-13 created an interagency Maritime Security Policy Coordinating Committee (MSPCC) to serve as the primary forum for coordinating U.S. government maritime security policies. The MSPCC coordinated the development of the National Strategy for Maritime Security and its supporting plans and is now actively working on assigning responsibilities and tasks to agencies within the government for implementation. The Coast Guard, as a lead federal agency responsible for maritime homeland security, will take an active role in executing the National Strategy for Maritime Security and its eight supporting plans.

While an implementation strategy for the NSMS and its supporting plans is currently being developed, the Coast Guard should expect to play an active leadership role in several areas.

Integrating the Layers of Security

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

A significant challenge to constructing integrated layers of security is the fact that many of the layers are the responsibility of different agencies. Integrating these disparate maritime security layers will be nearly impossible to achieve through ad hoc cooperation. The solution to this dilemma involves unity of effort, shared responsibility, partnership, and mutual support, but requires an agency with significant maritime security responsibilities to step up and act as a coordinator for the purposes of integrating the government's efforts to provide layered security. This will be an important function, as coordinating the layers of security requires working with agencies, private sector interests, and international partners to integrate efforts and eliminate seams between different modes of transport, agency jurisdictions, and international boundaries, so as to deny their exploitation by criminal or hostile actors.

Coordinating Maritime Security Operations

Deploying a system of effective, layered security requires extensive operational coordination and unity of effort among the involved agencies and the private sector. Mission coordination is essential to integrate the maritime security operations of numerous agencies at the operational and tactical levels to achieve operational effectiveness. A need exists to identify an agency with organizational capacities to champion the development of coordination protocols for operating jointly to prevent and respond to threats, such as those contained within the national Maritime Operational Threat Response Plan. This agency would also facilitate command and control during specific incidents and provide a forum for interagency mission planning when a multi-agency response must be seamlessly coordinated.

The Coast Guard possesses the authorities, capabilities, competencies, and partnerships to fulfill this role and should expect to be called upon to act as a mission coordinator. The Coast Guard maintains a robust command, control, and communications (C3) network of local, regional, area, and national level, military-style command and control centers, supported by extensive communications systems. To meet the expanding requirements of the maritime security mission, the Coast Guard is transforming its C3 network into integrated, multifunction command centers and is also enhancing the capabilities of the supporting communications systems. The Coast Guard must prepare to leverage its C3 network capabilities to support integrated maritime security operations.

Preparing for Maritime Recovery Operations

The private sector has traditionally demonstrated an ability to adjust activities in response to disruptions in the maritime transportation system, so much so that it has often been said to be self-healing in nature. Widespread disruptions, however, caused by a security-related incident of national significance, could threaten to bring large portions of the maritime transportation system to a virtual standstill, and contingencies must be prepared.

Assuring continuity of commerce is likely to require extensive coordination between the public and private sectors to restart or keep the flow of commerce moving during such an event. The National Strategy for Maritime Security identifies the Coast Guard as

the executive agent for the Department of Homeland Security for coordinating mitigation measures to expedite the recovery of infrastructure and transportation systems in the Maritime Domain. As such, the U.S. Coast Guard should expect to play a leadership role in coordinating maritime recovery operations in consultation with federal, state, and local agency partners and the private sector.

On the national level, recovery policies and procedures that emphasize assuring continuity of commerce in the Maritime Domain, such as the Maritime Infrastructure Recovery Plan and the Plan to Reestablish Cargo Flow, as contained within the National Maritime Transportation Security Plan, must be developed and closely coordinated with the other federal agencies and the private sector. Within the ports, the Coast Guard Captain of the Ports, as Federal Maritime Security Coordinators, can anticipate that they will be required to coordinate with federal, state, local, and private sector stakeholders through the Area Maritime Security Committees to prepare contingency plans for conducting maritime recovery operations.

The Coast Guard, as a lead federal agency responsible for maritime homeland security, will take an active role in executing the National Strategy for Maritime Security.

Partnering for International Maritime Diplomacy

The Coast Guard, now more than ever, should expect to play a vital role as an instrument of national security in protecting, promoting, and defending the maritime interests of the United States and our international partners. It is a unique agency through which the United States can assist other nations in achieving maritime security throughout the domain. The Coast Guard is ideally suited to conduct international maritime diplomacy activities on behalf of the Department of State and the Combatant Commanders, as well as on its own behalf, to achieve the objectives of the NSMS.

In its international maritime diplomacy role, the Coast Guard can assist other nations in the:

- development of national maritime policies, strategies, standards, and legislation;
- professional and material development of national maritime security, maritime safety, and naval forces; and
- development of other maritime management and regulatory agencies.

The Coast Guard has traditionally been the chief advocate for the United States in international issues involving maritime safety. Similarly, the Coast Guard should expect to be called upon to be the driving force in moving maritime security issues to the forefront at international forums such as the International Maritime Organization.

Conclusion

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

About the author: *CDR John Caplis currently works in the Office of Strategic Analysis for the Coast Guard Chief of Staff. He was detailed to the HSPD-13 project team as the Deputy Action Officer for the Department of Homeland Security, where he was a member of the core writing team that drafted the National Strategy for Maritime Security and coordinated with the interagency working groups that developed the eight supporting plans.*

Innovations for Port Security

Technologists and users must partner for success.

by Dr. Marc B. Mandler
Technical Director, U.S. Coast Guard Research and Development Center

Many of us have pondered the riddle about the tree that falls in the forest with nobody in earshot. Does the tree make a sound? In the spirit of this classic riddle, here is another puzzle: If an inventor creates a solution to a problem, but no one ever adopts the solution, is it considered an innovation?

Some argue that creativity is the mother of innovation. Therefore, a solution that is not embraced by end users should still be considered an innovation if it is novel and creative. In the corporate world, where generating profits is paramount, chief executive officers will say that products that do not generate or have the potential to generate profits, no matter how creative, should not be called innovations.

Acquirers of port security technologies view the world a little differently when it comes to innovations. They are inundated with information on hundreds, perhaps thousands, of technologies that are promoted as improving port security. Are all of these innovations? The acquirers of port security technologies—federal, state, and local officials—view innovations as not simply those products that have the promise of improving the security of a port, but products that are proven to improve security and do it in an affordable and cost-effective manner.

How does one create a better environment for innovation in port security? Significant funding has been made available through a variety of sources to address security needs. Sometimes, the funding is provided to technology developers to create products that can improve security posture. Other funds are provided to federal, state, or local authorities to acquire the best technology for a specific application. Technology developers are poised to provide the quick, off-the-shelf solution. Their customers search for the off-the-shelf system that will address their perceived vulnerability. The U.S. taxpayer trusts that officials will be good stewards of their tax dollars and protect them from many of the security risks that they currently face.

Dr. Robert Frosch, a former administrator of the National Aeronautics and Space Administration and former vice president of General Motors, provides some caution to developers and acquirers alike in an article, "The Customer for R&D is Always Wrong."[1] He writes:

"After 40-odd years of working in application- and mission-oriented research, I have come to believe profoundly that the customer for technology is always wrong. Now, the technologists are usually wrong, too; they tend to be wrong in complementary ways. I have seldom, if ever, met a customer for an application who correctly stated the problem to be solved. The normal statement of the problem is either too shallow and short-term, or, even more likely, is a formula for the widget that the customer thinks is required to solve what the customer thinks is the problem. The technologist is usually peddling 'that wonderful thing we did in the laboratory yesterday,' and if it happens to be square and the hole is round, a little force-fitting may help."

To overcome the wrongness that Dr. Frosh says permeates discussions between technologists and customers, there needs to be a robust and active collaboration between technology developers and technology consumers. Technology developers will be more successful if they walk in the shoes of the customer to gain a

full appreciation of the environment in which the user operates. Those constraints can prevent a technology solution from becoming an innovation.

Similarly, technology users must be willing to invite developers to work alongside them and teach them about their world and then be willing to have their operations serve as the testing ground for evaluating new technology concepts. Innovation is intimately related to the degree to which the technologist and user work together to clearly define the problem, the desired outcome, and the characteristics of a successful solution.

Modeling and Simulation as Innovation Tools

Modeling and simulation are tools that can help promote the innovation process and facilitate dialog between technologist and acquirer. Models or simulations provide an environment to test out technology concepts, in a relatively low-cost way before development funds are expended, to evaluate the effectiveness of potential technology solutions.

The Coast Guard Research and Development Center (RDC), the Coast Guard's sole research facility, uses many tools to assist in technology evaluations to support port security decisions. Simulation models are used to examine, for example, the relationship between surveillance system coverage and resolution and the likelihood of detecting a target of interest. Models are also used to evaluate the effectiveness and costs of employing, for example, small unmanned aerial vehicles in support of Coast Guard port security missions. In recent work, RDC used models to examine the effectiveness of waterside barriers for protecting vessels and facilities and different screening strategies for reducing the risk to ferries and passengers of a vehicle-borne improvised explosive device.

Consider a facility operator who wants to protect a facility, cruise ship, or a liquefied natural gas (LNG) tanker from attack by a small boat carrying explosives. Physical barriers, devices placed in the water to stop or slow down a small boat, offer promise for protection.

Figure 1: The new Hawkeye port surveillance system at Sector Command Center Miami.

RDC completed a study in partnership with the Captain of the Port in Boston, the city of Boston, and others to select the best commercial, off-the-shelf barrier to protect LNG ships moored in downtown Boston and cruise ships that make ports of call in Boston. The city of Boston was looking for stopping capability but was also concerned about mobility in its ports, the ease with which a barrier can be put in place and removed, and how much deterrence to an attack a barrier would provide without incurring excessive maintenance and support costs. A layer of protection analysis, which is a risk-based model, was used to evaluate the range of factors important to the port and to aid in selecting the barrier that fit the needs of the port. The result of this collaborative analysis was consensus among a number of disparate groups on the best set of technologies and operations to protect LNG vessels and cruise ships. The process of using a model to educate the consumer helps improve the likelihood that the technology selected will actually improve security.

Similarly, RDC worked closely with the ferry industry and federal, state, and local authorities to examine the range of alternatives that could be used to protect ferries from attack by a vehicle-borne improvised explosive device. A range of commercial vehicle screening technologies was examined, and a simulation model was developed to illustrate the trade-offs among screening effectiveness, cost, and efficiency of ferry operations. This effort, done in conjunction with authorities and ferry operators, resulted in recommendations that are being implemented to reduce the risk to the ferry system.

Rapid Prototyping Promotes Dialog with Users

Another powerful tool to promote the innovation process and facilitate a robust partnership between technologist and user is rapid prototyping. Rapid prototyping is an iterative process whereby a technology concept is matured through a spiral cycle of technology improvements that evolve from user feedback during the technology development process. Rapid prototyping is especially useful as a tool to help refine operational requirements in situations where users must adapt to a new mission or a new way of doing business.

Shortly after September 11, 2001, the Coast Guard Research and Development Center began a program called CATS-I that used this rapid prototyping process to improve the capabilities at the port level to prevent and respond to terrorist incidents. At the port level, operators understood their need to maintain situation awareness of the activities in and around the port, but they did not have enough experience in port security to articulate their operational requirements. Sectors Miami and San Francisco served as test beds for rapid prototyping of a variety of technologies, such as port surveillance systems, port partner collaboration tools, trip wires, and blue force tracking tools (technologies that tell units where friendly forces are).

RDC developed a robust collaborative relationship with other Coast Guard and port partners in Miami and San Francisco and worked closely with these partners to improve and refine the understanding of operational requirements. A significant accomplishment from this rapid prototyping effort was the development of rudimentary surveillance technologies, blue force tracking tools, and port partner collaboration tools that were demonstrated to improve the productivity and effectiveness at the sector.

The success of the CATS-I rapid prototyping process spurred the Department of Homeland Security Office of Science and Technology to make significant investments in the development of a full-scale, operational port-level surveillance and command and control system in Miami. This system, called Hawkeye (Figure 1), being developed by the Coast Guard's Command and Control Engineering Center, continues to serve as a test bed for experimentation for sector-level technology improvements. Sector Miami staff play a key role in providing feedback to developers on the capabilities and the effectiveness of the system design. Further, Hawkeye is serving as a basis for the Coast Guard's Command 2010 program, to refine requirements and evaluate new technology concepts for the Coast Guard acquisition of sector command center capabilities.

A partnership between technologist and technology acquirer/user is essential for improving port security. While some funding is flowing to ports to improve their security posture, ports are large, the vulnerabilities are significant, and the funding is limited. Everyone involved in securing ports has a responsibility to participate in the process of innovation, so that the best and most economical technologies can be found to secure U.S. ports. True innovation is realized when technologists and users work together to achieve common goals.

About the author: *Dr. Marc Mandler is technical director of the Coast Guard Research and Development Center in Groton, Conn. He received a B.A. in psychology from Clark University and a Ph.D. in psychology from University of Rochester. He has been a civilian employee of the Coast Guard for more than 22 years.*

Endnote

[1] Research Technology Management, November-December 1996, pp 22-27.

The Deepwater Program

Reducing risk in the Maritime Domain.

by RADM Patrick M. Stillman
Program Executive Officer, U.S. Coast Guard Integrated Deepwater System

With his approval of the National Strategy for Maritime Security in 2004, President George W. Bush reaffirmed that the safety and economic security of the United States depends upon the secure use of the world's oceans. "The United States has a vital national interest in maritime security," the new strategy states. "We must be prepared to stop terrorists and rogue states before they can threaten or use weapons of mass destruction or engage in other attacks against the United States and our allies and friends."

The U.S. marine transportation system's ports and waterways are at once both a vulnerable and valuable dimension of the global war on terrorism. As a result, ADM Thomas H. Collins, the Commandant of the Coast Guard, has placed a high priority on bolstering

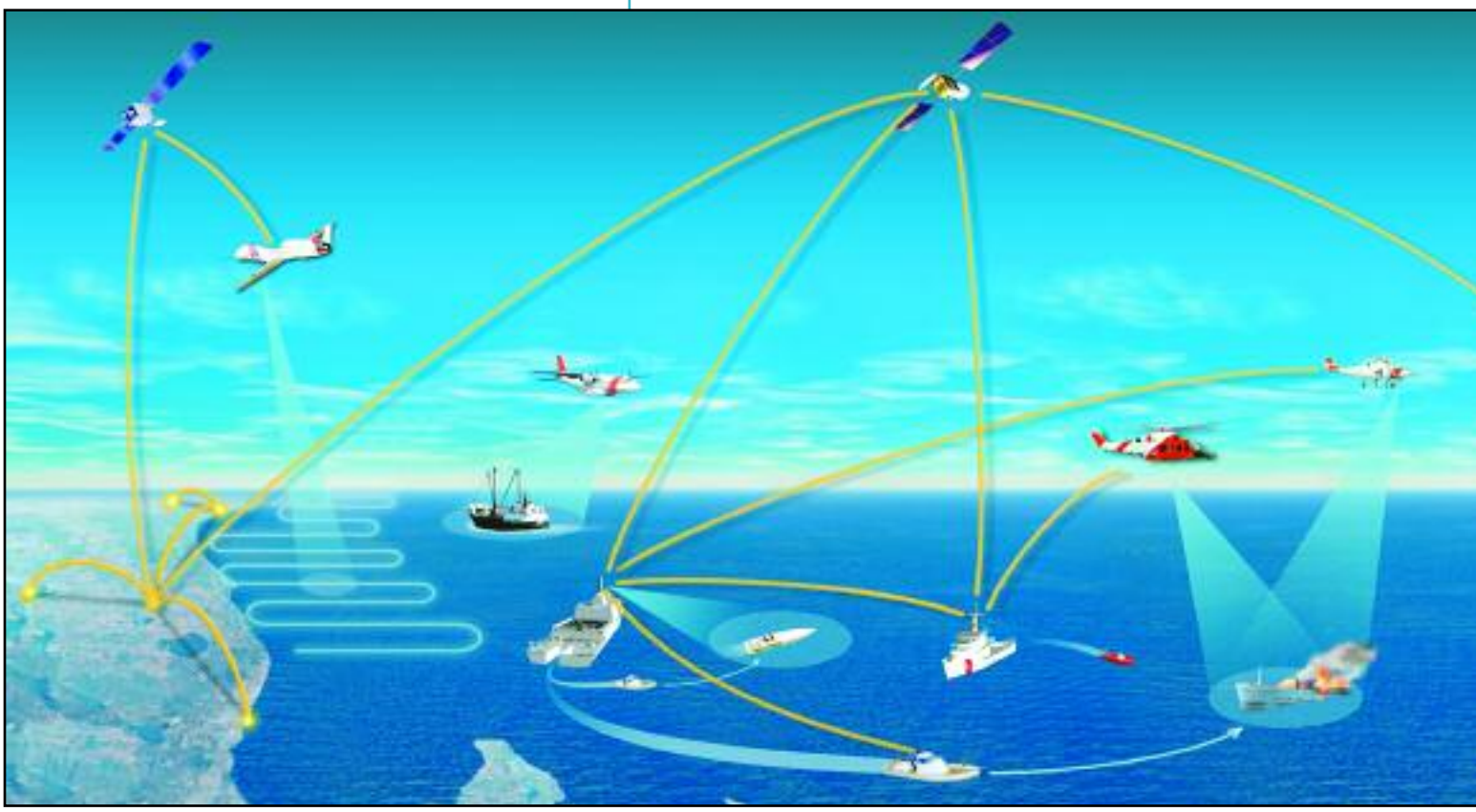


Figure 1: The Deepwater Program's network-centric system for command and control will link all of the Coast Guard's operational assets with a common operating picture and improve connectivity with the U.S. Navy, other federal agencies, and local first responders. Rich Doyle, USCG.

maritime security through vigorous implementation of the Maritime Transportation Security Act of 2002; the development of an enhanced maritime security regime; improved Maritime Domain Awareness; and the modernization and recapitalization of the Coast Guard's aging legacy assets and systems for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). It is for this reason that the Integrated Deepwater System plays such an important role in reducing risk in the Maritime Domain—beginning with the U.S. ports, waterways, and coastal areas that are so vital to the security and economic well-being of the United States and the safety of our citizens.

A Centerpiece for Transformation

"Recapitalizing the Coast Guard is the foundation of our ability to continue improving maritime security while facilitating the flow of commerce," ADM Collins testified to Congress in 2005. "The Integrated Deepwater System is the centerpiece for the Coast Guard's transformation and my top capital priority." Deepwater's three new classes of more capable cutters and associated small boats, manned and unmanned aircraft, integrated logistics, and improved C4ISR all will lead to a Coast Guard able to perform its multiple missions substantially more effectively well into the 21st century.

Last year, the Department of Homeland Security approved a revised post-September 11, 2001, implementation plan that aligns the Deepwater Program with the department's strategic goals of threat awareness, prevention, and protection against terrorist attacks; and response and recovery, should they occur. The revised plan, based on a comprehensive performance-gap analysis, updated the original pre-9/11 Deepwater Program by requiring improved capabilities on all assets; retaining, upgrading, and converting aviation legacy assets as part of the final asset mix; and adjusting the program's overall asset delivery schedule to improve operational effectiveness at an affordable cost.

The revised plan ensures Deepwater cutters and aircraft will be equipped with the right systems and capabilities to operate successfully in our more challenging post-9/11 threat environment. The Deepwater Program, projected to be a progressive $24 billion, 25-year modernization, conversion, and recapitalization effort, now incorporates requirements for such improved functional capabilities as:

- A network-centric system for C4ISR improvements to harness the power of an interoperable network that will improve Maritime Domain Awareness and provide a common operating picture. This is key to the Coast Guard's ability to lead the interagency effort to know and respond to maritime conditions, anomalies, vulnerabilities, and threats. Improvements to C4ISR enable earlier awareness of events through the more effective gathering and fusing of terrorism-related information, analysis, coordination, and response—all critical to detecting, deterring, and defeating terrorist attacks. Upgrades to Deepwater surface assets, for example, contribute directly to improved intelligence collection and fusion through sophisticated Shipboard Sensitive Compartmentalized Information Facility sensors and increased data-exchange bandwidth.
- Improved maritime-security capabilities, such as increased speed and integrated weapons systems on selected Deepwater cutters, essential to higher levels of maritime homeland security during a terrorist attack, opposed boardings, and other high-risk operations.
- Helicopter airborne use of force and vertical insertion and delivery capabilities to allow helicopters to provide warning and/or disabling fire and to deploy, deliver, and recover boarding teams safely and more effectively.
- Upgraded fixed-wing aircraft for long-range surveillance to increase Maritime Domain Awareness and reduce maritime patrol aircraft shortfalls in operating hours; organic Coast Guard air transport will be able to deploy Maritime Safety and Security Teams and National Strike Force teams faster for response with their equipment.
- Improved capabilities for anti-terrorist/force protection on select Deepwater assets with all-weather self-defense and the ability to protect high-value assets; assets will have the capability to engage terrorists with higher assurance of survivability and continued mission capability.
- Improved capabilities for detection and defense for chemical-biological-radiological (CBR) threats—essential to survival and continued operations during a CBR attack involving a weapon of mass destruction.

It is not difficult to envision how these more-capable Deepwater platforms will enable the Coast Guard to maintain a more vigilant and responsive maritime presence along the U.S. maritime border, starting at

U.S. ports, waterways, and coastlines and extending seaward to wherever the Coast Guard needs to be present or to take appropriate maritime action. This is the layered maritime defense mandated by the National Strategy for Maritime Security.

As the new strategy states, "Ports in particular have inherent security vulnerabilities: They are sprawling, easily accessible by water and land, close to crowded metropolitan areas, and interwoven with complex transportation networks. Port facilities, along with the ships and barges that transit port waterways, are especially vulnerable to tampering, theft, and unauthorized persons gaining entry to collect information and commit unlawful or hostile acts."

The Deepwater Program will posture the Coast Guard to operate far more effectively in this complex environment. When Deepwater is complete, cutters and aircraft will no longer operate as relatively independent platforms with only limited awareness of what surrounds them in the Maritime Domain. Instead, they will have the benefit of receiving information from a wide array of mission-capable platforms and sensors, enabling them to share a common operating picture as part of a network-centric force operating in tandem with other cutters, boats, and both manned aircraft and unmanned aerial vehicles (Figure 1).

Although originally conceived with deepwater missions in mind—those extending more than 50 nautical miles from U.S. coastlines—the Deepwater Program's mobile multimission platforms are ideally suited for the wide range of homeland security operations encountered in U.S. ports, waterways, and coastal areas. Improved ship designs for Deepwater's three classes of new cutters, for example, will provide better sea keeping and higher sustained transit speeds; greater endurance and range; and the ability for launch and recovery, in higher sea states, of improved small boats, helicopters, and unmanned aerial vehicles. These key attributes will enable the Coast Guard to implement more stringent maritime homeland security responsibilities, including jurisdiction over foreign-flagged ships. Deepwater's more capable cutters will be important players in the screening and targeting of vessels before they arrive in U.S. waters, onboard verification through boardings, and, if necessary, enforcement-control actions—more quickly, safely, and reliably.

The Deepwater Program's manned and unmanned aircraft will deliver substantially more flight hours than today's legacy systems and provide improved airborne use of force and vertical-insertion capabilities. These improvements will be of inestimable value to operational commanders in addressing today's tremendous burden of balancing the mismatch between inadequate resources to growing mission requirements.

Figure 2: The cutter USCGC *Vigilant*, homeported at Cape Canaveral, Fla., received the Deepwater Program's final installation of its first increment of C4ISR system upgrades in November 2005. All 210-, 270-, and 378-class cutters are now outfitted with a classified local area network and have access to the Department of Defense's Secret Internet Protocol Network—a key enabler for more effective maritime security patrols. USCG photo.

The Coast Guard's existing inventory of HH-60J and HH-65 helicopters will be converted to multimission platforms outfitted with more-capable systems. Deepwater's new CASA CN235-300M maritime patrol aircraft, upgraded HC-130 long-range search aircraft, and the Eagle Eye HV-911 vertical takeoff-and-landing unmanned aerial vehicle also will significantly increase search and surveillance areas from today's levels.

Making a Difference Now

Turning from the future, the Deepwater Program is also about sustaining and modernizing today's Coast

Guard. Recent upgrades to legacy platforms are making a difference now in improving operational performance until the transition to converted or new-construction platforms occurs.

In autumn 2005, for example, the final installation of Deepwater's initial increment of C4ISR upgrades was completed on the medium endurance cutter USCGC *Vigilant* (Figure 2). All 210-, 270-, and 378-class cutters are now outfitted with a classified local area network and have access to the Department of Defense's Secret Internet Protocol Network (SIPRNET), both underway and in port. This Deepwater modernization effort began with the first installation on the USCGC *Northland* in 2003 and corresponding installations ashore at the Communications Area Master Stations Atlantic and Pacific.

Figure 3: The medium endurance cutter USCGC *Tampa* sits high and dry at the Coast Guard Yard, Baltimore, Md., during a major systems refurbishment as part of the Mission Effectiveness Project for 210-ft. and 270-ft medium endurance cutters. Gordon I. Peterson, USCG.

Deepwater C4ISR upgrades have already led to more successful mission performance at sea by increasing Maritime Domain Awareness and enabling more effective joint operations. Commanding officers on legacy cutters say Deepwater C4ISR upgrades have revolutionized their work—helping the Coast Guard to interdict and seize record levels of illegal drugs at sea during the past two years. Cutters outfitted with more capable Deepwater command-and-control upgrades also served with distinction during the Coast Guard's response to Hurricanes Katrina and Rita in 2005. They demonstrated their effectiveness enabling on-scene coordination of operations with local first responders and other federal agencies in ports like New Orleans, La., and Gulfport, Miss.

Deepwater also is funding other sustainment projects for older surface assets. Last May, the medium endurance cutter USCGC *Tampa* (Figure 3) was the first 270-ft. cutter to enter a nine-month major systems refurbishment at the Coast Guard Yard in Baltimore, Md., as part of the Mission Effectiveness Project (MEP).

MEP is a key part of the Deepwater strategy to allow the Coast Guard to bridge the gap until new cutters are delivered. This multi-year project for 210-foot and 270-foot cutters will replace obsolete and increasingly unsupportable systems, to improve reliability and reduce maintenance costs. Up to 27 of the 270-foot Bear Class cutters and 210-foot Reliance Class cutters will be phased into the yard's workload over the next several years to extend their service lives for an additional 10 to 15 years.

The Coast Guard's top aviation priority, Deepwater's accelerated re-engining of the workhorse HH-65 helicopters, also is progressing well. Three modernized HH-65C helicopters deployed during the Coast Guard's response to Hurricane Katrina; their aircrews saved 305 lives during 85 sorties. Compared to older and less reliable Bravo models, the more powerful and efficient HH-65C has twice the endurance on station (two hours and 30 minutes) and can hoist twice as many people (six).

With a recent contract award, the first of the six HC-130J long-range search aircraft will soon begin its "missionization" modifications, following final system design and engineering. Modifications will result in 90-percent C4ISR commonality with the CASA MPA. The J model of the venerable Hercules boasts

improved power and performance over its predecessor and will easily convert for cargo and personnel transport missions, including the handling of oversized equipment.

Sustaining Momentum

Deepwater is postured to move forward with an appropriate sense of urgency. A fiscal year (FY) 2006 appropriation of $933.1 million (later reduced by a 1 percent recision to $923.8 million) allows the Coast Guard to sustain and modernize legacy cutters and aircraft to increase their useful service life while the acquisition of new assets advances (Figure 4).

Current Deepwater funding is expected to sustain our momentum in providing the Coast Guard with the more capable assets it needs to improve maritime homeland security, to implement the National Strategy for Maritime Security, and to perform all enduring core missions.

Deepwater's FY-2006 budget provides for:

- continuation of the production line for the National Security Cutter;
- continuation of design work for the first Offshore Patrol Cutter;
- completing the design and acquiring long-lead materials for the first Fast Response Cutter, now scheduled for delivery in 2008, 10 years ahead of its original schedule;
- the next phase of the Eagle Eye VUAV for testing;
- completion of re-engining of operational HH-65 helicopters (Figure 5) using two production lines;
- service-life extension and conversion of HH-60 helicopters and HC-130H LRS aircraft into Deepwater end-state aircraft and continued missionization of the Coast Guard's six HC-130J aircraft;
- service-life extension and electronics upgrades for legacy medium endurance cutters; and
- continued development of Deepwater's interoperable C4ISR system to improve Maritime Domain Awareness and provide a common operating picture.

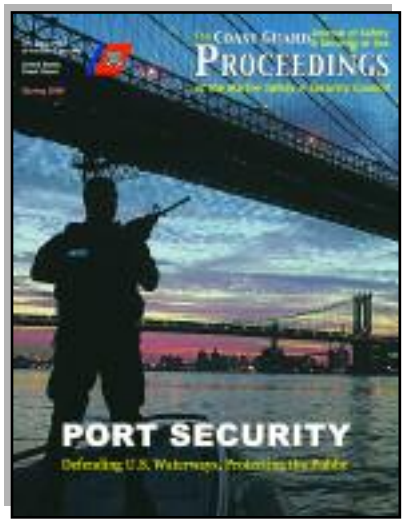
The President's FY-2007 budget request for the Coast Guard includes $934.4 million for the Deepwater Program—a major investment to enable the Coast Guard to be ready, aware, and responsive in the future, wherever and whenever it is needed. The Deepwater Program will not transform the Coast Guard overnight for its post-9/11 missions; progressive modernization and recapitalization are a marathon, not a sprint. Month by month and year by year, however, more capable Deepwater assets, linked by a network-centric system for C4ISR, will strengthen smart borders and protect the nation's ports, waterways, and coastal areas.

Figure 4: President George W. Bush is joined by legislators, cabinet members, and law enforcement officials in the East Room of the White House as he signs the Homeland Security Appropriations Act for fiscal year 2006. The appropriation will sustain the Deepwater Program's momentum in modernizing and recapitalizing the Coast Guard's aging legacy assets. Courtesy Paul Morse, White House.

The Deepwater Program will progressively enable the Coast Guard's implementation of a layered, defense-in-depth maritime security strategy for what has been recognized as the nation's most valuable and vulnerable sector, the Maritime Domain. In this sense, the Deepwater Program is a critical investment in achieving a more secure American homeland and building a 21st-century Coast Guard.

About the author: *RADM Patrick M. Stillman, the Integrated Deepwater System's first Program Executive Officer, leads the largest modernization and recapitalization program in Coast Guard history.*

Figure 5: The Deepwater Program's re-engining of HH-65 helicopters has been accelerated as the Coast Guard's top aviation priority. Three re-engined HH-65C helicopters performed superbly during Hurricane Katrina rescue operations, saving 305 lives during 85 missions. As depicted here, older model helicopters undergo a comprehensive modernization during the re-engining process. PAC Jeff Murphy, USCG.



We'd Like Your Input

PROCEEDINGS Magazine, Spring 2006

READER'S SURVEY

As an effort to assist authors and the *Proceedings* magazine staff, this short questionnaire was developed. Please take a few moments to complete it.

Please return this questionnaire to ARL-DG-NMCFeedback@uscg.mil. Simply type the question number and your response in your email with a subject line of "Spring Proceedings." You may also return the survey by fax at 202-493-1065 by circling the number of your choice below.

1. Was the content in this issue of *Proceedings* useful to your pursuits in the maritime industry?

   Strongly Agree 5……4……3……2……1 Strongly Disagree

2. Was the design and layout of this issue of *Proceedings* pleasing to the eye and conducive to readability?

   Strongly Agree 5……4……3……2……1 Strongly Disagree

3. Do you have any suggestions for improvements to *Proceedings*?

   YES / NO.
   If you answered "yes," what would you like to see included?

_____

_____

_____

_____

_____

Reader's Survey

Safely Securing U.S. Ports

The port security assessment program.

by LCDR Brady Downs
Deputy, Domestic Assessment Division, U. S. Coast Guard Inspections and Compliance Directorate

Shortly after September 11, 2001, the U.S. Coast Guard created the Port Security Directorate to enhance security in U.S. seaports. A crucial part of this organization is the Port Security Assessment Team at Coast Guard Headquarters, which has the responsibility of assessing port vulnerabilities and potential consequences of maritime-related terrorist acts and implementing tools to help ports reduce the risk of terrorism. The directorate immediately made an impact by conducting port security assessments in the nation's militarily and economically strategic ports, completing studies of the consequences of terrorist acts on specific types of vessels and infrastructure, developing a risk-based tool to help ports identify maritime critical infrastructure and reduce their risk of terrorism, and assisting the Department of Homeland Security (DHS) in administering grants to improve port security.

Security Assessment

The Port Security Assessment Team took a very close look at the vulnerabilities of critical infrastructure and key assets in ports supporting the marine transportation system. The current assessment approach was unique, in that it looked at port infrastructure from the perspective of the terrorist and used Coast Guard-led teams with former U.S. Navy Seals to identify potential targets within the port. The teams identified potential targets, including high-consequence waterfront facilities, passenger vessels and terminals, bridges, and crucial waterways. These teams focused on the vulnerabilities of these targets and developed scenarios for attacking them, then followed on with recommendations to improve security, including how to detect, deter, and disrupt potential attacks.

To raise security awareness within the port, the assessment identifies methods and locations where terrorists might conduct surveillance of targets, gain access to the target, stage equipment near the target, and outlines activities that may indicate that security is being probed prior to an attack. Using the unique terrorist operations perspective enhances the vulnerability assessments required by the Maritime Transportation Safety Act and prevents duplicating the security assessments being widely conducted by industry and government agencies. Assessments have been conducted over the past three years in 72 of the nation's most strategic port systems.

Risk Assessment and Analysis

Besides the vulnerability assessments, another key issue within each port is the assessment of risk. Risk incorporates the elements of threat, vulnerability, and consequence. As Department of Homeland Security Secretary Chertoff said, "What should drive our intelligence, policies, operations, and preparedness plans and the way we are organized is the strategic matrix of threat, vulnerability, and consequence. And so, we'll be looking at everything through that prism and adjusting structure, operations, and policies to execute this strategy."

Considering the uncertain nature of security threats, and given that resources to counter them are limited, it is very important to apply risk analysis to tackle the greatest vulnerabilities with the worst consequences. The Coast Guard has used a tool called the port security risk assessment tool (PSRAT) for the past four years to assess risk in the various ports across the nation.

Currently, the Domestic Assessment Division within the Directorate of Inspections and Compliance has created an enhanced risk calculation tool, which is called the maritime security risk assessment model (MSRAM). MSRAM substantially improves the detail of the risk model and gives a more accurate prioritization of risk at the port and national levels to provide stakeholders with the information they need to make risk-based decisions and best apply their limited resources.

The maritime security risk assessment model:

- improves the threat component, by applying threat data from the Coast Guard's Intelligence Coordination Center as to the intent and capability of the adversary;
- involves Coast Guard District and Area Commands in review of data to provide consistency across ports nationally;
- requires assessing the capability of owners/operators of critical infrastructure, local law enforcement, and Coast Guard security assets to protect targets and deter and interdict attacks;
- requires estimating the secondary economic impacts with the loss of the target, considering recoverability and redundancy of the target;
- addresses response capability as a primary consequence mitigation factor for owner/operators, local first responders, and the Coast Guard;
- incorporates revised attack scenarios to ensure alignment of the Coast Guard's port, waterways, and coastal security missions with Department of Homeland Security efforts;
- features improved consistency of consequence and vulnerability scores between ports by having subject matter experts assign acceptable ranges, based on experience and field data;
- integrates an asset screening step that will allow users to determine if the consequence ratings rank high enough to require a more detailed review of the most critical assets in the port;
- includes a "change-case" capability, where mitigation strategies can be applied to the scenario/asset combination, to evaluate the resulting risk reduction/risk buy-down;
- brings training to field units, with the deployment of the tool to ensure a consistent approach nationally;
- supports strategic and operational decisions by rolling up of field-level risk assessments to portray risk density of targets;
- produces standard reports and the ability to query data by various means; and
- provides data to support local and national risk-based decision making.

Special Technical Assessments

In addition to the vulnerability assessments and the risk analysis tool developed via the PSRAT/MSRAM, the Port Security Assessment Team conducts special technical assessments to gather accurate information on vulnerabilities and determine the possible consequences of terrorist attacks on various vessel types and other critical port infrastructure. These assessments assist all levels of the Coast Guard, especially the Captains of the Port in their role as the federal maritime security coordinators, and asset owners and operators in making risk-based policy decisions based on factual data.

Special assessments typically include a technical review of the vessel or port infrastructure, mission, location, known vulnerabilities, cargo, areas of transit, terrorist modes of attack, and historical review of related incidents. Technical experts then use computer models to determine blast effects of various explosions for a range of attack scenarios, providing a consequence assessment. The information gained by these assessments provides a better understanding of what may actually happen during a terrorist attack, so that the most appropriate measures may be implemented to protect U.S. ports and waterways.

Special technical assessment projects are nominated by Coast Guard Headquarters, areas, districts, sectors, and field units. Examples of special technical assessments conducted include blast and consequence analysis of:

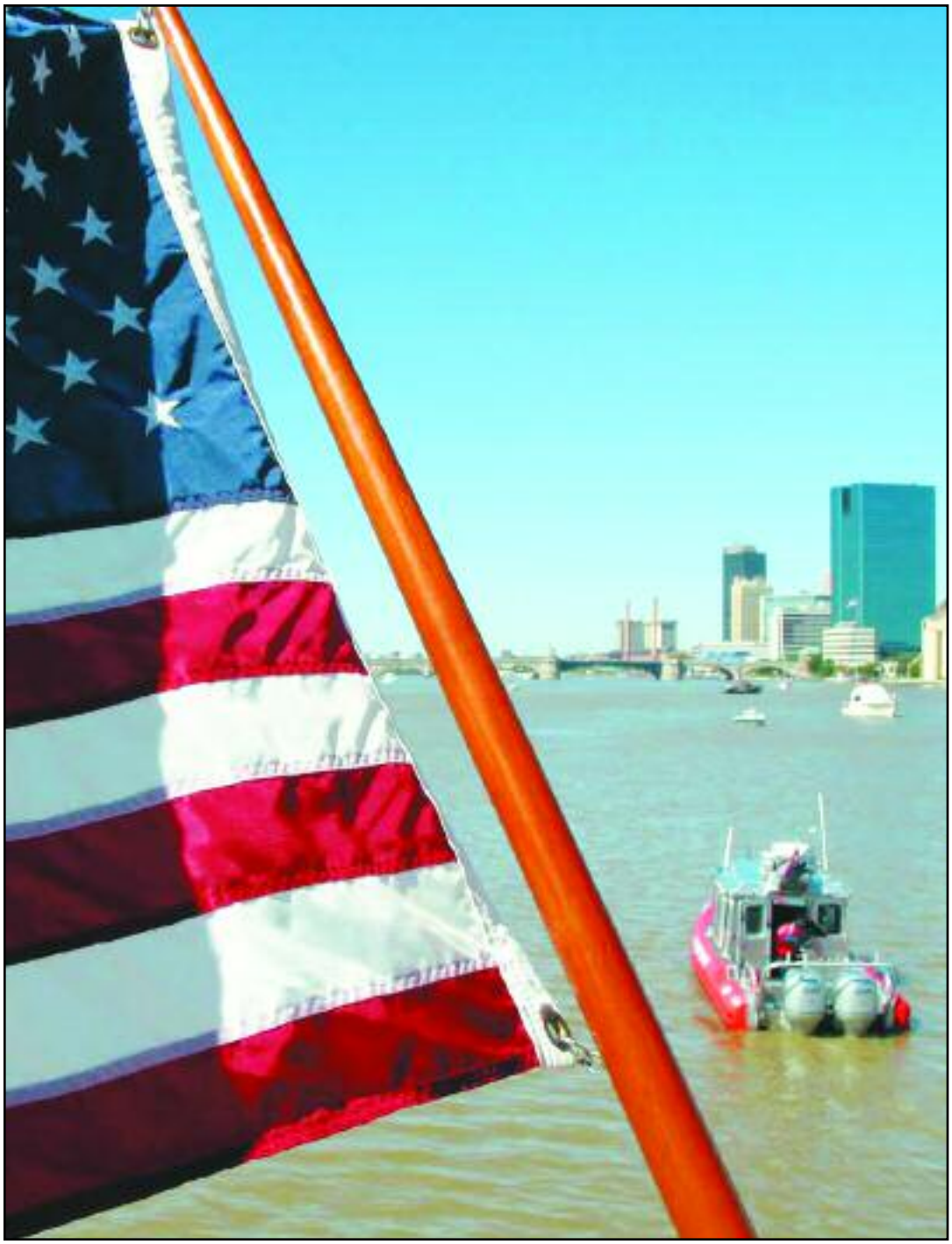
- liquefied petroleum gas ships;
- passenger ferries;
- barges carrying certain dangerous cargoes;
- tunnels;
- liquefied petroleum gas barges;
- cruise ships;
- single skin tank vessels; and
- ammonium nitrate commodities flow study.

Due to the sensitive information contained in these reports, they are classified but can be accessed by authorized personnel via the Port Security Directorate's secure Website. Also, key stakeholders

with appropriate clearances have been briefed on the results of these reports

Funding

When vulnerabilities are identified, consequences are known, and risks are prioritized, it is important to then take steps to reduce risk in the port. This takes resources. One of the mechanisms in place to address the needs, vulnerabilities, and documented gaps is the port security grant program. The federal government administers this program, which funds projects that reduce security risks in ports. In 2004, the Office of Grants and Training was designated as the lead agency to centralize state and local terrorism preparedness and grant administration with other emergency preparedness grant programs. The Coast Guard plays a significant role by assisting DHS in the grant process, which has awarded over $560 million since 9/11.



Port security assessments, the maritime security risk assessment model, special technical assessments, and port security grants combine to provide some of the tools and capability critical to a layered security regime.

Port security assessments, the maritime security risk assessment model, special technical assessments, and port security grants combine to provide some of the tools and capability critical to a layered security regime. This regime will mitigate risks in U.S. ports and within the marine transportation system.

About the author: *LCDR Brady Downs was commissioned in the U.S. Marine Corps in 1986, where he served in the 7th Marine Amphibious/Expeditionary Brigade. In 1990, he transferred into the U.S. Coast Guard. His tours include Officer Candidate Instructor in Yorktown, Va.; Officer in Charge of the Presidential Honor Guard in Washington, D.C.; and Assistant Operations Officer aboard the Coast Guard Cutter* Dallas. *He has served as Search and Rescue coordinator for Coast Guard Group N.Y., Pollution Investigator for Captain of the Port N.Y., and Senior Marine Inspector and Marine Casualty Investigator for Activities New York. He currently serves in the Directorate of Inspections and Compliance.*

U.S. Deparment of Homeland Security

United States Coast Guard

The Coast Guard Journal of Safety at Sea

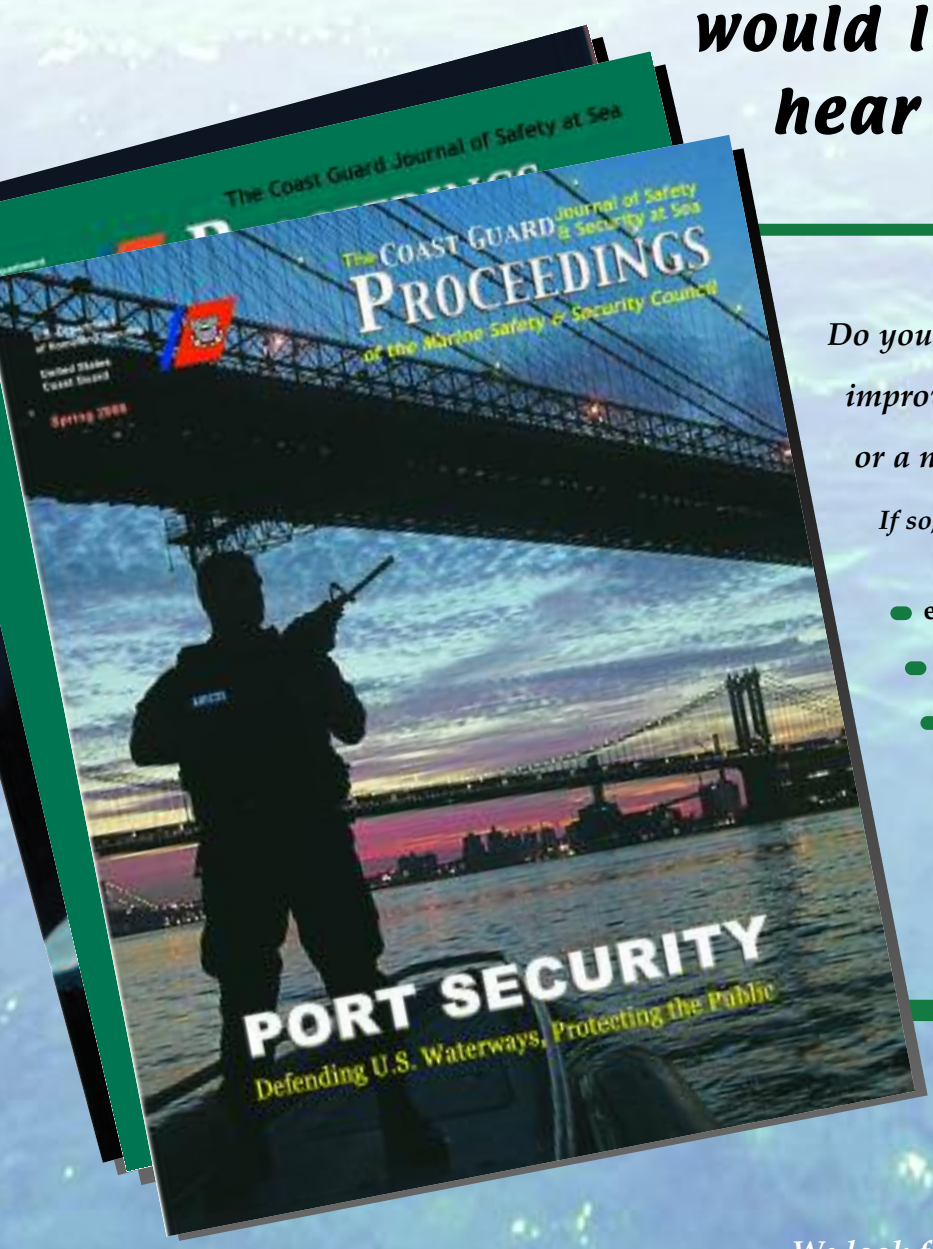
PROCEEDINGS

of the Marine Safety & Security-Council

The editors of PROCEEDINGS

of the Marine Safety & Security Council

would like to hear from you!



Do you have a suggestion about improving the magazine, an article idea, or a neat photo to share?

If so, please contact us at:

- **e-mail: ARL-DG-NMCProceedings@uscg.mil**
- **Phone: (202) 493-1072**
- **Mailing Address:**

  U.S. Coast Guard, Proceedings Magazine,
  4200 Wilson Blvd., Suite 730,
  Arlington, VA 22203-1804

We look forward to hearing from you soon, and we hope you have enjoyed this issue of ***PROCEEDINGS****!*

HOMEPORT

This secure Internet portal provides critical information and service to the public, maritime security partners, and Team Coast Guard.

by LCDR Mark Hammond
U.S. Coast Guard Office of Port and Facility Activities

by LCDR Karrie Trebbe
Homeport Project Officer, U.S. Coast Guard Office of Resources and Information for Prevention

Consider these scenarios: An urgent message arrives at the local Captain of the Port office. It requires the immediate dissemination of a Department of Homeland Security threat bulletin containing sensitive security information to all Maritime Transportation Security Act-regulated bulk-liquid facilities in that port. How is this currently accomplished? Multiple phone calls, faxes, hand delivery?

Prior to the next meeting of your Area Maritime Security (AMS) committee, you wish to communicate with committee members, exchange ideas, and solicit comments/feedback regarding a sensitive portion of the AMS plan. However, there is currently no easily accessible, secure method of doing this without meeting face to face.

What about changes in the Maritime Security (MARSEC) level for your port? What is the process by which you ensure appropriate entities are notified in a timely manner, and how do you track MARSEC level attainment for each entity?

Got Homeport? Then no problem!

Homeport (http://homeport.uscg.mil) is a publicly accessible, secure Internet portal that supports unique U.S. Coast Guard business requirements by providing personalized information delivery and critical services to the public, maritime industry, and Team Coast Guard. Version 1.0, which primarily supports port security functionality, was deployed October 3, 2005. It serves as the Coast Guard's primary communication tool to support the sharing, collection, and dissemination of sensitive but unclassified (SBU) information, including sensitive security information (SSI). Homeport delivers an unprecedented level of collaboration and information sharing capability and has the potential to revolutionize the way the Coast Guard communicates with the public and maritime security partners.

Background/History

The Maritime Transportation Security Act of 2002 (MTSA) mandated increased information sharing and the development of a suite of maritime security plans. In light of these requirements, in the spring of 2004, the U.S. Coast Guard Office of Port, Vessel, and Facility Security (G-PCP) sought to develop an electronic plans (e-plans) management system to establish an SSI-level database and Web-based portal access to

the vessel, facility, and area maritime security plans required by the MTSA. The proposed concept was to design a system that would afford instant access, within a secure environment, for information sharing and collaboration among critical decision makers within federal, state, local, and industry for routine maritime security and crisis situation management.

The U.S. Coast Guard Office of Information Resources for Prevention collaborated with the Office of Port, Vessel, and Facility Security to develop the proposed system. The Office of Information Resources, in close coordination with the Coast Guard's Infrastructure Management Division and the technical staff at the Coast Guard's Operational Systems Command (OSC), developed a robust, Coast Guard-wide Internet portal. This system also has the potential to replace every Captain of the Port /Federal Maritime Security Coordinator Internet Website and other Coast Guard Websites with one consistent Internet presence.

The capabilities of Homeport also enable the Coast Guard to align with Department of Homeland Security (DHS) goals and support two key points of Secretary Chertoff's six-point agenda:

- increasing overall preparedness, particularly for catastrophic events by enabling wide dissemination of threat/MARSEC information to our maritime stakeholders, and
- enhancing information sharing with our partners.

Further, Homeport serves to support the National Strategy for Homeland Security, released September 2005. This strategy specifies that the federal government will build a national environment that enables the sharing of essential homeland security information horizontally across each agency of the federal government and vertically among federal, state, and local governments; private industry; and citizens. This strategy calls on DHS to lead the effort to define sharing requirements; establish processes for providing and receiving information; and develop technical systems to share sensitive information with public-private stakeholders.

System Development

During the summer of 2004, Homeport was developed and successfully completed DHS vulnerability testing. In November 2004 a prototype of Homeport was initially deployed to eight Coast Guard units for operational testing and evaluation. Development continued and enhancements were made based on user feedback. Operational testing and evaluation was completed in March 2005. Between March 2005 and the official deployment on October 3, 2005, policy and guidance regarding the use of Homeport were developed.

The full capabilities and potential of Homeport were realized during Hurricane Katrina response and recovery operations. Coast Guard operation centers were inundated with phone calls and requests for assistance. In coordination with OSC; the Office of Information Resources; Coast Guard's Infrastructure Management Division; Coast Guard Headquarters Command Center; and the Eighth District Command Center, Homeport developers delivered the capability of allowing the public to complete a missing/stranded person request form online. Coast Guard Headquarters and District Eight operation centers were able to log into Homeport to view the requests. Within 24 hours of making the online request form available, over 6,000 requests were submitted. In the end, Homeport received over 16,000 requests for help.

System Deployment

Multiple training sessions were conducted in July and August 2005 at OSC Martinsburg, W.Va., to establish a pool of qualified Homeport registration approvers. Approvers are responsible for the review, proper vetting, and approval of Homeport user accounts. The training included basic system operations, specific functionality, and key features enabling members to return to their units to begin generating port-wide usage and populating local content areas.

Post-deployment training is planned during fiscal year 2006, consisting of several train-the-trainer sessions. Additionally, on-demand training will be made available to each sector desiring specific, focused training. G-PCP is also in the process of developing a series of training videos that will be available to the field in the near future. These videos will highlight the many useful tools and functionality within the system that are designed to enhance coordination among various port security partners.

G-PCP hosted a series of workshops comprised of Coast Guard personnel, representing a cross section of various field units and program offices. This group was brought together to represent the diversity of potential Homeport users and to address concerns regarding the implementation of Homeport. The end-product of these workshops was G-MPS (now G-PCP) Policy Letter 01-05, which provides detailed guidance on the proper use of the port security functions within Homeport, including review/approval of user registrations, use of SBU communities, publishing threat

products, and setting MARSEC levels. A core aspect of the policy that is central to the registration process is the proper vetting of registrants by account approvers, since registered users have access to a variety of sensitive security information.

Access to Homeport user accounts is currently limited to the following user groups:

- owners and operators, vessel security officers, and company security officers of vessels that are required to submit a vessel security plan under MTSA;
- owners, operators, and facility security officers of waterfront facilities required to submit a facility security plan under MTSA;
- members of an Area Maritime Security Committee;
- members of national-level committees, such as the Safety Advisory Committee, Harbor Safety Advisory Committee, National Industry Security Partner, Port Readiness Committee, and National Maritime Security Advisory Committee; and
- Coast Guard members who deal with Area Maritime Security Committees.

User access is approved based on a registrant's eligibility and need to know. The general public has the ability to view a wide range of information, much of which is currently found on the existing Coast Guard Website.

System Capabilities and Features

Homeport Version 1.0 offers many useful capabilities and features for information sharing and collaboration. Anyone can access general information without an account. However, depending on their profile, registered users have access to the following capabilities in Homeport:

- publish and update unit Internet information (such as statistics, safety and security zones, and inspection schedules);
- notify any maritime industry Homeport user (via e-mail);
- change MARSEC levels for the entire COTP zone or an individual port component;
- see MARSEC attainment levels of individual vessels and facilities in their COTP zone;
- view the security plan for any vessel or facility;
- manage Homeport registration for maritime industry users and industry partners;
- manage the security plan review and approval process;
- publish and disseminate local security alerts; review national security alerts and threat products; and collaborate with their Area Maritime Security Committee, Harbor Safety Committees, and Safety Advisory Committees;
- easily publish and maintain enterprise marine safety, security, and environmental protection Internet information;
- publish and disseminate national security alerts;
- publish and disseminate threat products, with the ability to target distribution to specific port users;
- view security plans for any vessel or facility;
- see MARSEC levels of any vessel or facility;
- collaborate with any Area Maritime Security Committee, Harbor Safety Committees, and Safety Advisory Committees or other established communities.

The collaboration feature is one of the most valuable tools of Homeport. Homeport collaboration spaces, known as communities, are where a designated group of users can work together on projects, set meetings, generate tasking, and exchange information about topics of interest within a secure or non-secure environment.

Short-term enhancement plans for Homeport include the incorporation of an enterprise solution for an Alert Notification System (ANS) whereby Captains of the Port and Federal Maritime Security Coordinators can broadcast alerts through multiple means of communication. Further, the office of Information Resources continues to work with DHS on building appropriate connections between Homeport and DHS' Homeland Security Information Network, which provides the main communication, analysis, and collaboration tool for connectivity to state and local agencies.

For more information regarding Homeport, visit http://Homeport.uscg.mil.

About the authors: *LCDR Mark Hammond is stationed at the U.S. Coast Guard Office of Port and Facility Activities.*

LCDR Karrie Trebbe is the Homeport Project Officer, U.S. Coast Guard Office of Resources and Information for Prevention.

America's Waterway Watch

This homeland security outreach program is preventing terrorism through awareness.

by Chief Petty Officer Penny Collins
Program Coordinator, America's Waterway Watch, U.S. Coast Guard Office of Port and Facility Activities

by LT Kenneth Washington
Program Manager, America's Waterway Watch, U.S. Coast Guard Office of Port and Facility Activities

America's Waterway Watch (AWW), www.americaswaterwaywatch.org, is a maritime homeland security outreach program created to encourage members of the recreational boating public, as well as the maritime industry, to recognize and report suspicious activity. AWW educates the public by describing:

- what to look for;
- where to look; and
- how to respond when you see something suspicious.

What, Where, and How

For what should the public look? Suspicious activities can include:

- people appearing to be engaged in surveillance of any kind;
- people attempting to buy or rent fishing or recreational vessels with cash for short-term, undefined use; and
- unusual night operations.

Where should you look? Sensitive locations include:

- under and around bridges, tunnels, or overpasses;
- near industrial facilities such as power plants and oil, chemical, or water intake facilities; and
- near military bases and vessels or other government facilities or security zones.

Finally, how should you respond? Recommendations include:

- Secure and lock your boat when not aboard.
- Disable the engine on stored or trailered boats.
- Do not approach or challenge anyone acting in a suspicious manner.
- Call the National Response Center at 800-824-8802 or 877-24WATCH when you see something suspicious.
- Call 911 if you see an immediate danger to life or property.

The homeland security mission has become more of a priority since September 11, 2001. For large commercial waterfront facilities and vessels, new security regulations have been promulgated under the Maritime Transportation Security Act of 2002 (MTSA) and have been in force for a few years. While these regulatory requirements are a major step in the right direction, no single effort can address all security concerns for the entire maritime transportation system, or for the maritime environment as a whole. It has been estimated that there are over 95,000 miles of shoreline, 6,000 bridges, thousands of marinas, and approximately 70 million recreational boats in the United States. Given this extensive area of responsibility, it is not possible to maintain a high level of security over all these areas that may be vulnerable to potential terrorist or illegal activity, without help from a vigilant public.

Given these recent events, the Commandant of the Coast Guard encouraged the maritime industry to report suspicious activity to help prevent future

events of terrorism in the maritime area. Many local Coast Guard Captains of the Port developed outreach programs, staffing them with dedicated Coast Guard Active Duty, Reserve, and Auxiliary personnel to address this call in their local areas.

Local Programs

Local outreach programs began to organize in their areas of responsibility to meet this request for greater vigilance and reporting of suspicious activity. Local programs such as "On Guard" in Miami, Fla., and "Community Coastal Watch" in Mobile, Ala., prepared pamphlets and other materials to inform the recreational boating public and maritime stakeholders that their assistance was needed to help protect U.S. waterways. The message was well received by the maritime industry and recreational boaters in each Captain of the Port zone across the country.

Because all of these local programs were homegrown, some problems came to light because of inconsistencies. For example, each program had its own criteria for spotting suspicious activity and even its own contact numbers for making reports. Essentially, these local programs needed to be connected nationally, and there was no central place to obtain information about all of them. While the local programs were very successful, they did not share a common link with other programs and materials. In early 2005, the America's Waterway Watch program was created. A key objective of AWW is to bring together all local programs under one initiative that is nationally connected, but locally focused.

The AWW program provides national recognition for all programs and unites them under one umbrella, without losing local focus. AWW has created brochures, stickers, posters, and other educational materials to be used by all local programs to support their missions. The aforementioned toll-free numbers have been created for use by all AWW program participants to report suspicious activity.

U.S. Coast Guard Auxiliary

The program could not have succeeded without the help and close partnership of other organizations. The Coast Guard Auxiliary had taken a leading role in security-related outreach programs with its Waterway Watch program, which is focused on the recreational boating community. This volunteer group has once again proven its merit by developing brochures and other educational materials, creating a Website, and conducting numerous outreach activities with the recreational boating public across the country (Figure 1). The auxiliary program, Waterway Watch, has now been incorporated into AWW, so that there will be no conflict in names. The auxiliary has been charged to take the lead in the promulgation of AWW within the recreational boating community.

As U.S. Coast Guard Auxiliary Commodore Gene M. Seibert said in a recent press release, "The active duty Coast Guard can't be everywhere, all the time. There are 70 million recreational boaters. Through America's Waterway Watch, the Coast Guard Auxiliary is adding eyes and ears to the nation's efforts to prevent terrorism."

Figure 1: Two Coast Guard Reservists and two Auxiliarists from the America's Waterway Watch team conduct public outreach at the Ft. Lauderdale boat show. From left: PS1 Glenn Moffett (Reservist); Mr. Kenneth Deonarine (Auxiliarist); Mr. Irving Goldman (Auxiliarist); LT Pedro Mesa (Reservist).

Figure 2: Coast Guard Commandant ADM Thomas H. Collins is flanked by reservists from the America's Waterway Watch program team and active duty personnel from the Coast Guard Recruiting Command (CGRC). All are participating in an outreach effort at Lowe's Motor Speedway, Charlotte, N.C. From left: FN Michael Cajagas (CGRC), AMT1 Rickey Allen (Recruiting Office, Charlotte, NC); SK1 Chris Morere (Recruiting Office, Raleigh, N.C.); PAC Renee Gordon (Officer-in-Charge, Recruiting Office, Charlotte, N.C.); ADM Thomas H. Collins; AMT1 Charles Kramer (CGRC, Raleigh, N.C.); CAPT Bruce Viekman (Commanding Officer, Coast Guard Recruiting Command); and PS1 Terry Waterfield (LANTAREA - CGD5, Portmouth, Va.)

Both the Auxiliary and regular Coast Guard have added additional partnerships to the America's Waterway Watch effort. Organizations now participating include the U.S. Power Squadrons, National Association of State Boating Law Administratiors, Boat U.S., the U.S. Army Corps of Engineers, the National Sheriff's Association, the states of Michigan and Connecticut, Association of Marina Industries, Navy Sea Cadets, Association of Shire Yacht Clubs, and International Association of Chiefs of Police.

How the Public Can Help

Aside from partnerships, AWW is being marketed in other ways. For instance, National Association for Stock Car Auto Racing (NASCAR) fans are the target audience for an AWW public service announcement featuring the Labonte racing family. Marketing to this segment of the population makes sense, because a majority of NASCAR fans are also recreational boaters (Figure 2).

AWW directly supports two elements of the U.S. Coast Guard Commandant's Maritime Strategy for Homeland Security:

- increasing Maritime Domain Awareness; and
- leveraging partnerships to mitigate security risks.

The Coast Guard defines Maritime Domain Awareness (MDA) as "the effective understanding of anything associated with the global maritime environment that could impact the security, safety, economy, or environment of the United States." America's Waterway Watch is a vital part of the Coast Guard's overall Maritime Domain Awareness picture, since a more vigilant and aware public will greatly increase deterrence to future terrorist activities.

The public's participation in the program provides valuable information about suspicious activity. AWW's partnership with the National Response Center ensures that the suspicious activity reports received are shared with the Department of Homeland Security, Federal Bureau of Investigation, Central Intelligence Agency, and many other government agencies that require this information to plan and prepare for any potential terrorist attack in the maritime sector.

Continued support of the America's Waterway Watch program will ensure that the agencies needing the information will receive it on a timely basis. AWW is unique, in that it offers the average citizen an opportunity to actively contribute to the protection of our way of life.

The future of America's Waterway Watch is bright. As new partnerships are established and fostered, the message will continue to reach the people who will be the eyes and ears in helping to protect the United States from those who would do harm. The maritime area is huge and, subsequently, vulnerable. The Coast Guard alone cannot protect all U.S. maritime interests. It will require educational materials, the continued support of the public through these outreach programs, and continued funding from leaders in government to move this effort forward.

About the authors: *Chief Petty Officer Penny Collins has 32 years of service with the U.S. Coast Guard as a reservist. On active duty since October 15, 2001, CPO Collins serves as the Program Coordinator for America's Waterway Watch. Her responsibilities include developing training procedures, coordinating partnerships, and interacting with the Coast Guard commands for reserve participation as well as the Coast Guard Auxiliary for augmentation.*

LT Kenneth Washington, former Program Manager for America's Waterway Watch, had 14 years of active duty service with the U.S. Coast Guard; seven of those years were spent as a boarding Officer. As program manager, his responsibilities included acquiring funding for the program and managing program activities. He served as the Assistant Branch Chief for the U.S. Coast Guard Coordination and Awareness Branch.

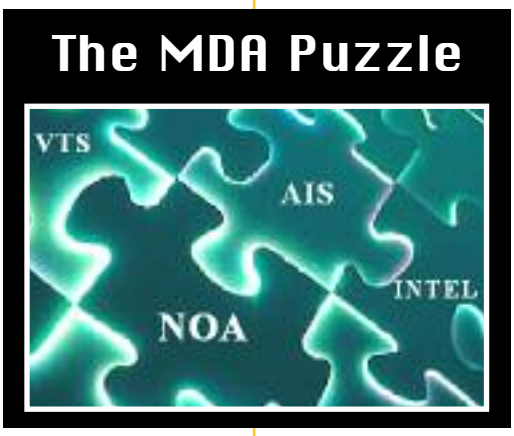
Three-Dimensional Awareness

The notice of arrival and its role in Maritime Domain Awareness.

by ENS Joseph Azzata
Assistant Project Officer, Notice of Arrival, U.S. Coast Guard

Imagine this scenario: On the dawn of the 11th day at sea, the crewmembers of the fictional product tanker *Neptune* rise in preparation for their first port call in the United States. The *Neptune* is struggling to make its notice of arrival (NOA) time, after taking some heavy seas during its transatlantic trip. The bar pilots are keeping an eye on the vessel's progress, so they can position their pilot boat accordingly. However, the pilots and the local U.S. Coast Guard units are not the only groups tracking the tanker's progress and preparing for its arrival.

Secretly, a four-man crew is approaching the pilot boarding area from the south, in a 100-foot, power-driven supply ship. Their mission is to ram the tanker and deliver a deadly cargo of ammonium nitrate fuel oil. As the supply ship comes up to speed, the captain on the bridge of the tanker notices the smaller ship on what looks to be a collision course. The tanker is practically helpless, with steering capabilities reduced at slow speed, so the captain can only hope this unknown vessel is going to alter course as he gives a few perfunctory pulls on his ship's whistle. Onboard the smaller supply vessel, the crew has no intention of stopping as they jam the throttle to full ahead…



Maritime Domain Awareness

Such a doomsday scenario may seem a bit extreme. It is hard for the general public to imagine such a threat and, therefore, may assume a threat like this does not exist. But naivety is not a defense against attacks on U.S. ports and infrastructures. As the lead federal agency for maritime security, the U.S. Coast Guard is actively working to minimize the possibility of success of such a scenario by enhancing and expanding Maritime Domain Awareness (MDA).

One dimension of MDA is the notice of arrival regulation (33CFR160.2), which, generally speaking, requires vessels to report their arrival data, date, time, location, crew, cargo, and passengers to the Coast Guard for vetting. It is a static tool, in that information is only available when submitted by the user. However, it is vital, because so much information is received that is not currently captured in other MDA initiatives. The information captured in the NOA allows the Captain of the Port (COTP) to preposition the proper resources, such as armed boarding teams (Figure 1) and boat crews, to maximize effectiveness. Or, in the case of a product tanker arriving, the COTP may implement a moving security zone, based on available intelligence, for the date of arrival.

However, the NOA is only one dimension of Maritime Domain Awareness. Three-dimensional coverage requires real-time information feeds, such as vessel tracking systems (VTS) and automatic identification system data, coupled with credible intelligence. This provides more insight into what the vessel is actually doing and what information may have been purposely omitted from the NOA.

Figure 1: A boarding team positions itself to board a Bahamian flagged cargo ship. PA3 Donnie Brzuska, USCG.

Take the tanker scenario above, and assume that one of the unlicensed crewmembers is a known terrorist. The captain enters the person's alias and sends the completed NOA off to the Coast Guard as required. The staff at the Intelligence Coordination Center (ICC) Coast Watch processes the NOA and finds this crewmember's alias matches one on a terrorist database. The ICC then informs the Captain of the Port and local law enforcement of this crewmember's presence, as well as the vessel's noncompliance. The vessel tracking system and automatic identification system data cannot provide a crewmember's name, so it is vital to integrate the current systems to provide this layered defense.

Integration of Intelligence

The integration of the various data feeds and information sources will make it far easier to track vessels in U.S. ports and waterways. Currently, the Coast Guard uses what is known as the COP, or common operating picture. It provides exactly that—a computer-generated picture of all surface operations in the Maritime Domain. Using the NOA, AIS, and other tracking feeds, this system is able to categorize and track a vessel based on NOA data, intelligence data, and other external sources. The scope is far greater than that of the current vessel tracking system and automatic identification system coverage. This overarching view allows a vessel to be tracked point to point, with no limited shadow areas. The COP centralizes the effort of many systems, which not only saves time in the screening process, but reduces the number of personnel needed behind a desk when they can be better used on the dock or underway on patrol.

Although a significant hurdle has been created for would-be terrorists, there is still much to be done. The Coast Guard is continually looking for ways to improve its current NOA regulation. Currently, the NOA regulation only requires reporting data on U.S. and foreign-flagged commercial vessels greater than 300 gross tons. The regulation also requires information from foreign-flagged recreational vessels greater than 300 gross tons and for any vessel, either U.S. or foreign, carrying any certain dangerous cargo. This equates to roughly 600 NOAs processed daily, which is a sizable population of the total arrivals. However, nearly any ship is capable of creating a threat to homeland security, including smaller commercial and recreational vessels.

Closing the Gap

To enhance domain awareness, it is necessary to increase the scope of the current NOA applicability to include all foreign commercial vessels, regardless of tonnage, and any U.S. commercial vessel arriving from a foreign port. All inbound vessels need to be screened, particularly those arriving from foreign ports or places, to vet their crew and cargo. The security screening process can only begin when the notice of arrival is submitted.

Let's go back to the tanker from the scenario, which is about to encounter a deadly threat in the form of a 100-foot supply vessel. Response is limited to the time from the first acknowledgement of the threat until impact. This could be hours or, in some cases, just a few minutes. Probability favors the attacker. However, the missing piece from our tanker scenario is intelligence. The story is now changed to include credible intelligence that informs the Coast Guard of a plan to destroy the tanker. This intelligence may be nautical charts and an operation outline found in a hotel room or data from an informant. With this information, the tanker is determined to be the target. The COTP can then order the tanker to divert from the port, while the Coast Guard leads a law enforcement team to the smaller threat vessel and intercepts the four would-be terrorists before they come within visual contact of the

tanker. That's having Maritime Domain Awareness.

So, with the notice of arrival, the Coast Guard knows when and where the tanker is arriving. We know the crew, we know the cargo, and we know all of the hard data. AIS and VTS tell where the vessel is, its speed, and what course it is on. At this point, the Coast Guard has two-dimensional coverage. Intelligence can bring all this information together and give it some purpose. Not every ship is a product tanker and receives as much scrutiny. But add some credible threat, and now this actionable information can be used to allocate the proper response (Figure 2). This intelligence may come in the form of high-level knowledge passed between agencies, or it may come from the average boater concerned about suspicious activity.

The Coast Guard has developed a program to help the general public assist in protecting U.S. waterways. America's Waterway Watch (www.americaswaterwaywatch.org) provides the proper channels for the public to contact the Coast Guard in the event they witness unusual activity in and around U.S. maritime infrastructure. Many eyes on the water are needed, and who better to be aware of the intricacies of a harbor or coastal area then the boaters and workers who spend their days on and around it?

So what is the answer? Simply put, if the United States wants to have more comprehensive Maritime Domain Awareness, the scope of applicability for the notice of arrival and other tracking initiatives such as AIS needs to be expanded. The Coast Guard cannot track what it does not require, so the first step is including more vessels. Will this be a waste of time because the majority of those vessels are compliant and cause little concern to the COTP? Yes, the vast majority will be vetted and cleared without incident, but, for that small population of vessels that cause concern, the Coast Guard can direct its response in a coordinated manner.

For example, more time can be spent researching why the AIS feed indicates a port call at Berth A, while the NOA indicates a port call at Berth B. Maybe this anomaly is operator error; however, it might be something else more devious. This layered approach to MDA can only be successful if the Coast Guard continues to utilize the proper tools as well as enhance them. The notice of arrival is but one piece of the Maritime Domain Awareness puzzle, but, without it, the puzzle is incomplete.

About the author: *ENS Joseph Azzata works as the Assistant Project Officer for the Notice of Arrival Regulation. Prior to this assignment, he was sailing as Third Mate in the U.S. Merchant Marine. He received his license from the United States Merchant Marine Academy, Kings Point, N.Y.*

Figure 2: The U.S. Coast Guard Cutter *Adak* holds position alongside a cargo dhow. PA1 John Gaffney, USCG.

On Watch

Vessel tracking technologies for maritime security.

by Mr. William R. Cairns
Principal Engineer for Long-Range Identification and Tracking
U.S. Coast Guard Office of Navigation Systems

The United States' 96-hour notice of arrival data indicate that, on an average day, 1,040 vessels over 300 gross tons approach the United States from foreign ports, while another 350 ships are present in U.S. ports. An additional unknown number of vessels approach the United States and transit the exclusive economic zone on coastwise routes, bound for non-U.S. ports. These vessels are not required to send a notice of arrival, since they are not bound for U.S. ports and are not generally tracked. An estimated 5,000 of these large vessels are within 2,000 nautical miles of the United States at any time.

The Case for Vessel Tracking

The U.S. Coast Guard is faced with the responsibility of maintaining surveillance of maritime approaches to the United States for safety, security, and environmental protection. The economic impact resulting from just an 11-day loss of the use of a West Coast port has been estimated to be $140 million to $2 billion. Ongoing migrant and drug law enforcement efforts demonstrate the limited ability of U.S. civil government and military entities to see what is happening near the maritime borders.

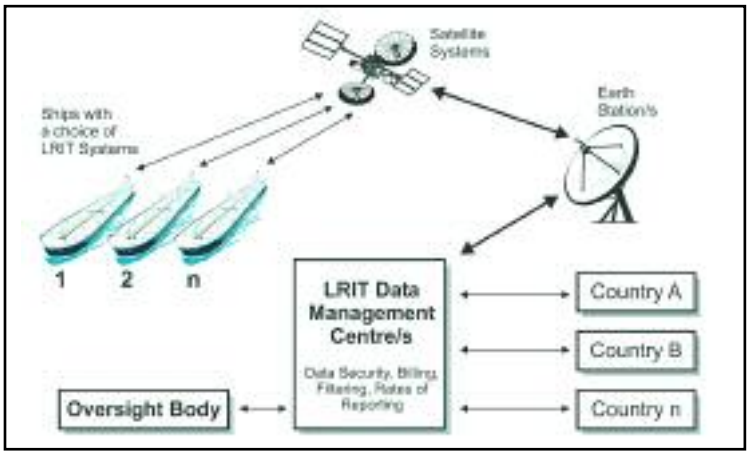


Figure 1: Long-range identification and tracking concept. Courtesy Inmarsat.

The Coast Guard is pursuing vessel tracking technologies to assist in the detection, classification, identification, and targeting of vessels. Among these technologies, automatic position reporting is being considered for tracking ships along the U.S. coastline, out to 2,000 nautical miles.

Long-Range Identification and Tracking

Long-range identification and tracking (LRIT) is a cooperative surveillance capability. In the LRIT concept (Figure 1), a ship carries radio communications equipment that reports identification, position, and time to authorities tracking that ship.

To improve maritime security in the near term, the Coast Guard may pursue voluntary LRIT. Ships subject to the Safety of Life at Sea Convention (SOLAS) and fitted with Global Maritime Distress and Safety Inmarsat-C equipment should have the capability to report position information. Many already use this capability or other satellite communications, such as fleet management systems, to report position and other information to shoreside agents and owners. Ship owners may be asked to voluntarily make their position information available to the Coast Guard electronically and permit polling.

LRIT and International Regulations Legislation
The Maritime Transportation Security Act (MTSA) of 2002 authorized long-range tracking to assist in maritime security: "The Secretary may develop and implement a long-range automated vessel tracking system for all vessels in United States waters that are equipped with the Global Maritime Distress and Safety System or equivalent satellite technology...."[1]

The Coast Guard and Maritime Transportation Act of 2004 amended this section of MTSA 2002 by requiring the implementation of long-range tracking, consistent with international treaties, conventions, and agreements to which the United States is a party.[2] More recently, pending legislation may call upon the Coast Guard to conduct a pilot project for long-range tracking using satellite systems to aid maritime security. [3]

With legislation as the underlying authority to implement LRIT, the Coast Guard is pursuing several regulatory initiatives at both the international and domestic levels.

Proposed Mandatory Participation for SOLAS Ships
The United States is leading the effort at the International Maritime Organization (IMO) for adoption of an LRIT SOLAS amendment that includes flag, port, and coastal state access to long-range identification and tracking information. The United States seeks to have SOLAS ships carry LRIT equipment capable of automatically transmitting ship identity, position, and time of position.

A U.S.-proposed draft amendment[4] to SOLAS Chapter XI-2 (Special Measures to Enhance Maritime Security) states that contracting governments, subject to certain restrictions, can receive LRIT information transmitted by ships as follows:

- Flag states: All flag ships worldwide.
- Port states: All ships indicating an intention to enter, at a distance or time set by the port state.
- Coastal states: All ships, regardless of flag, within a distance of 2,000 nautical miles of the coast.

The U.S. proposal was submitted to the IMO Maritime Safety Committee 78th session (MSC 78) in May 2004 but was not adopted. In December 2004, MSC 79 broadened the scope of LRIT beyond security, to include safety and environmental protection.[5] The IMO Radiocommunications and Search & Rescue Subcommittee (COMSAR) is developing LRIT performance standards and functional requirements and resolving other technical issues.

LRIT Study
During April and May 2005, the Coast Guard; the Republic of the Marshall Islands (RMI); and Pole Star Space Applications Ltd., an LRIT application service provider; conducted an LRIT feasibility study. RMI submitted its results to the IMO Maritime Safety

Figure 2: PurpleFinder Web-based display from the Marshall Islands LRIT Feasibility Study. Courtesy Pole Star Space Applications Ltd.

Committee 80th session (MSC 80). [6]

The United States acted as both port state and coastal state in this study. When the Coast Guard received a notice of arrival for a Marshall Islands ship, a request to track was sent to Pole Star. RMI ships that participated in this study were voluntarily tracked, even when not

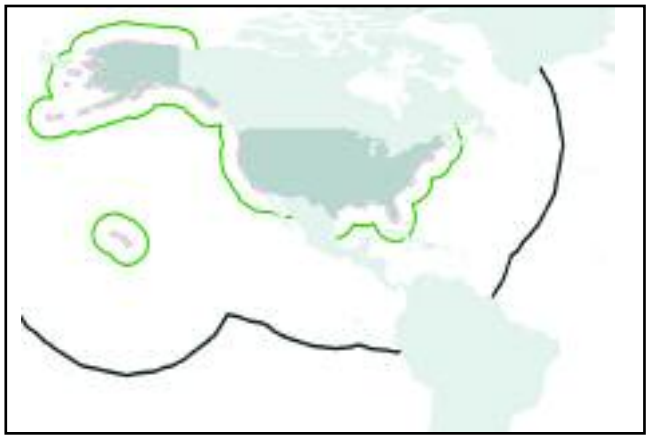


Figure 3: The 2,000 nautical mile and 300 nautical mile thresholds from the U.S. coasts.

bound for a U.S. port. Pole Star provided RMI ship raw data feeds, including IMO number, position, course, and speed reported, over Inmarsat-C. The Coast Guard Operations Systems Center processed this data and sent it to Coast Guard Command and Control Engineering Center to be integrated into the common operational picture. The position reports allowed the United States to track RMI vessels on the common operational picture and also via Pole Star's

Figure 4: Potential AIS coverage from NOAA data buoys.

PurpleFinder Web-based tracking tool (Figure 2). The feasibility study demonstrated to MSC 80 that long-range identification and tracking is achievable in the near term, from both technical and policy perspectives.

LRIT Regulations

At the conclusion of the IMO Maritime Safety Committee 80th session, officials agreed on the LRIT system architecture and minimum information requirements. It was agreed that the transmission of LRIT information should not require any intervention by shipboard personnel, will be at no cost to the ship, and will be available free of charge to contracting governments for search and rescue purposes. Only contracting governments that request and obtain LRIT information would be required to pay for the service.

MSC 80 officials also agreed that an independent long-range identification and tracking coordinator should perform oversight of the LRIT data center, application service providers, and elements of the communications systems. The LRIT coordinator should verify that all LRIT participants adhere to long-range identification and tracking information security requirements. The IMO Maritime Safety Committee requested the International Mobile Satellite Organization to advise the committee whether it was willing and able to undertake this oversight role. [7]

MSC 80 identified a number of LRIT key points:

- nothing in the regulation shall prejudice the rights or obligations of states under international law;
- the purpose of the regulation is for security, search, and rescue, and any other purpose as determined by IMO;
- the regulation applies to ships 500 gross tons and above;
- flag states can receive LRIT information from all their ships globally;
- flag states can name contracting governments that shall not receive LRIT information on their ships;
- port states can set either a time or distance for the mandatory receipt of LRIT information for ships bound for their ports;
- the distance at which a coastal state can receive LRIT information remains under discussion. [8]

An MSC intersessional working group meeting was held in October 2005 to develop draft SOLAS amendments on LRIT. Because an agreement could not be reached on coastal state access to LRIT information, the draft amendment only includes flag and port state access. The proposed amendment, submitted by the United Kingdom as Circular Letter No. 2681, dated November 8, 2005, is being circulated in advance of MSC 81 so that it might be adopted there. [9] At press time, COMSAR 10 is expected to complete work on long-range identification and tracking performance standards and functional requirements and forward these to MSC 81 for approval.

The deliberations at COMSAR 10 and MSC 81 on long-range identification and tracking performance standards and the draft amendment will have a significant positive impact on international maritime security. Figure 3 indicates the vast tracking area to which the United States will have access at the 2,000 nautical mile threshold (black line). This distance roughly equates to the 96-hour notice of arrival (at a ship speed of 20 knots.) The green line indicates the 300 nautical mile threshold.

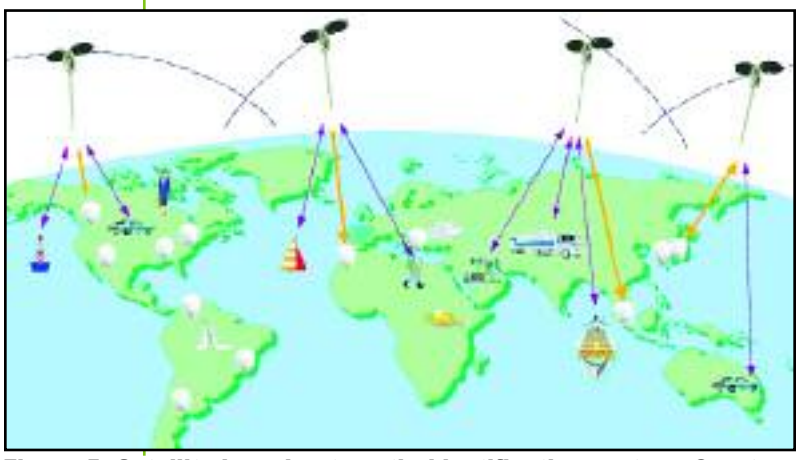


Figure 5: Satellite-based automatic identification system. Courtesy ORBCOMM.

Automatic Identification Systems

In addition to long-range identification and tracking for maritime security, automatic identification systems are also taking a role in the near-shore environment. An automatic identification system (AIS) is equipment required to be installed on SOLAS-class vessels effective July 2004.[10] AIS messages include a host of information such as ship identification, position, time, cargo, speed, and rate of turn. Although this system was designed for collision avoidance, by communicating information directly between ships within VHF range, AIS is now being used as a tool for maritime security.

Nationwide AIS

The Coast Guard is pursuing a major acquisition to deploy AIS receivers nationwide. In the short term, smaller scale efforts are being made in the Gulf of Mexico; in waters near Hawaii, California, and Alaska; and on offshore National Oceanographic and Atmospheric Administration (NOAA) data buoys. Figure 4 indicates the additional coverage that may be attained from these buoys.

Range of AIS Systems

AIS is a line-of-sight system, operating in the VHF band. A good rule of thumb for line-of-sight coverage is:

$$d=\sqrt{2h_{antenna}}+\sqrt{2h_{ship}}$$

where d is the line-of-sight distance (in miles) and h represents respective heights of shore and ship antennas (in feet). An AIS antenna on a tower at 300 feet should receive signals from a ship automatic identification system 30 feet above the waterline out to 32 miles. However, research has shown that AIS may reach much greater distances.

More comprehensive propagation models indicate a broader coverage area than the rule of thumb. Using the Engineer's Refractive Effects Prediction System-PROPR model, two ships with class A AIS antennas at 100 feet, 12.5 watt transmit power, 2.5 dB antenna gain, and receiver sensitivity of –107 dBm ought to receive each other at 40 nautical miles. From a similarly equipped ship to a shore station with 100-foot, 9.5 dB antenna gain and –119 dBm sensitivity, the shore station ought to "see" the Class A at 97 nautical miles. [11]

The Coast Guard Research and Development Center has established a network to study methods to improve AIS reception. Personnel conducted measurements on AIS shore site reception to determine apparent coverage area. At one typical site, 50 percent of the time, the maximum reception range was 140 nautical miles; 10 percent of the time the maximum reception range was 220 nautical miles. These distances are only achieved intermittently, but that may be good enough for security applications.

Although tower-mounted AIS may reach these distances, it is still limited in range. By placing AIS receivers at heights not achievable with towers, the capability expands to a significantly larger footprint.

Satellite-Based AIS

Coast Guard contracted with Johns Hopkins University Applied Physics Lab to determine if automatic identification system signals could be captured over a wide area, from a low-earth-orbit satellite. Because AIS transmissions are self-organizing, time division multiple access, vessels within the same horizon can broadcast their information in specific time slots, without stepping on each other's signals. This study examined the feasibility of receiving and deciphering a large number of simultaneous signals, with due regard to satellite receiver saturation. It showed that receiving automatic identification system signals at a satellite is feasible and a significant number of signals could be received simultaneously, without loss of message content. A contract was issued with ORBCOMM, a satellite data communications company, to put an AIS receiver on one of their satellites for testing. Figure 5 shows the satellite-based AIS concept. At this writing, the test satellite was due to be launched in 2006.

After validating the concept with a successful test, the Coast Guard plans to deploy a follow-on constellation. If testing of a satellite with an AIS receiver is successful, deployment could begin for a five-year phase in period to launch up to 26 satellites.

Through the use of technologies such as long-range identification and tracking and automatic identification systems, coupled with international regulations, the Coast Guard is striving to improve its maritime security stance.

About the author: *Mr. William R. Cairns is Principal Engineer for Long-Range Identification and Tracking in the Waterways Management Directorate at U.S. Coast Guard Headquarters. He has served on U.S. delegations to the IMO Maritime Safety Committee and NAV and COMSAR Sub-Committees and is coordinator of the COMSAR Correspondence Group on LRIT. He is a Fellow, Royal Institute of Navigation, and member of the White House Military Aides Association.*

Endnotes

[1] 46 USC 70115.
[2] Coast Guard and Maritime Transportation Act of 2004, P.L.108-293, 118 Stat.1080.
[3] Coast Guard and Maritime Transportation Act of 2005, H.R. 889 section 404.
[4] IMO MSC 80/3/3.
[5] IMO MSC 79/23 para 5.72.
[6] IMO MSC 80/5/9.
[7] IMO MSC 80/24 para 5.98.3.
[8] IMO MSC 80/24 para 5.108.
[9] IMO Circular letter No.2681 dated November 8, 2005.
[10] SOLAS V/Regulation 19.
[11] Current Status of AIS Class B Development and Findings on AIS Signal Reception Range, David Pietraszewski and Joseph Spalding, 29 September 2004.

Maritime Domain Awareness

Technology is the easy part.

by Mr. Guy Thomas
Science & Technology Advisor, U.S. Coast Guard

Maritime Domain Awareness (MDA) has always been a focus for the U.S. Navy and U.S. Coast Guard, but, since September 11, 2001, the term has taken on new meaning as the sea services have worked to close security gaps in U.S. maritime frontiers. In the multi-front war against global terrorism, those who would exploit the maritime environment and transportation systems for unlawful or hostile means must be denied. U.S. national interests lie well beyond territorial waters and cannot be constrained by geographic boundaries. The United States is the world's leading maritime nation, whether measured by the sheer number of vessels plying its waters, the volume of goods transported by ship, or the economic value of its maritime commerce. With such reliance on an efficient and effective global maritime transportation system, the United States must be firmly committed to its security.

From the U.S. perspective, the sooner illegitimate activity in the global maritime environment can be identified and halted, the more secure the homeland will be. This means becoming aware of illegal or potentially threatening activities as distant from U.S. shores as possible to determine the optimal response. Taking that a step further, then, critical areas such as cargo loading facilities, embarkation/debarkation points, shipping lanes, choke points, as well as our own maritime approaches and facilities, must be monitored to establish a layered security regime. Additionally, layers of awareness must also be established that are centered upon traditional areas of interest, such as an environmental pollution and recovery, resource poaching, humanitarian efforts, or search and rescue operations.

Senior government officials, tasked with creating a national plan to improve Maritime Domain Awareness (see sidebar), recognized the need for the development of a common operational picture, with a user definable interface to a collaborative information environment (CIE). The challenge is to provide this common operational picture to all necessary entities in as complete and accurate manner as near to real time as possible. To do this, the envisioned collaborative virtual database must be equipped with the latest automated data manipulation tools, capable of data mining, pattern recognition, anomaly detection and other planner, analyst, and operator automated assistance tools.

The strategy and plans workgroup, one of seven formed after the multi-agency May 7, 2004, MDA summit, developed seven essential tasks that, when accomplished, are expected to achieve comprehensive Maritime Domain Awareness. These tasks include monitoring of vessels, people, cargo, and designated areas of interest in the global maritime environment; accessing all relevant databases; collecting, analyzing, disseminating relevant information; and developing appropriate metrics to measure performance toward accomplishment of the MDA related missions.

The other workgroups included ones for technology, legal, intelligence, common operational picture, outreach and budget. The intelligence workgroup defined the potential threats and the technology work group initiated a survey of what assets were available within the government to assist in the detection of those threats. Once it was understood what the agreed tasks were versus those threats, and a rough idea of what concept of operations was feasible and likely to be enacted, the technology workgroup performed a gap analysis on the entire MDA system and proposed a range of initiatives to improve the capability to detect, track, classify, and identify vessels, the cargo in them and the people on them, including their intentions, in the Technology Roadmap.

Technological Solutions

Since a core requirement of the MDA collaborative information environment is accurate vessel detection

and location data, the technology workgroup examination focused on ways to enhance the ability to detect vessels and craft both on the high seas and in the littorals. They looked at both sensors and likely platforms.

Radar

The first area of examination was, not surprisingly, long range radar systems upgrades. The utility of three types of long range (beyond line of sight) high frequency radars is being studied:

- The buoy-mounted HF surface wave radar, currently used for ocean current and wave height observation, appears to have promise. This is especially true if several are used together in a multi-static mode.
- The very large array relocatable over the horizon radar (ROTHR) appears the most promising in many ways, with demonstrated detection ranges of 1500+ miles.
- The large array shore or barge-based HF surface way radar, which may have some limited utility in unpopulated areas.

Other sensors

To screen shipments before they depart foreign countries destined for the United States, Customs and Border Protection (CBP) uses non-intrusive technology to quickly inspect cargo containers. Enhanced capability to detect a wider variety of potentially threatening substances is under development. Additionally, smart boxes, which are shipping containers with built-in sensors that can detect temperature changes or unauthorized entry and some prohibited items, now in use to protect valuable or perishable contents, are currently being evaluated.

New sensors— both active, such as upgraded radars, and passive, such as the exploitation of the reflection of radio, TV, cell tower and satellite downlink signals, and acoustics—are being examined.

Formation of the National Strategy for Maritime Security

Today, a major paradigm shift is occurring with regard to Maritime Domain Awareness, as the Coast Guard, in active partnership with a broad range of governmental agencies, seeks to protect U.S. ports and waterways from those who would do them harm.

Indeed, since September 11, 2001, numerous war games, seminars, and forums have been held to discuss needed improvements in the maritime security of the United States. Those discussions ranged from the search for technological silver bullets to legal and policy issues, to resources required gathering and analyzing all forms of intelligence and information. In August 2003, the U.S. Coast Guard, the lead federal agency for security in the Maritime Domain, recognized its lead responsibility and created the Maritime Domain Program Integration Office (MDA PIO).

It was immediately recognized that there needed to be a summit of all federal agencies involved in the Maritime Domain, and, beginning in January 2004, planning was initiated. The MDA summit concept plan was quickly approved by the Secretaries of Defense and of Homeland Security. Over the next four months, numerous planning meetings were held with almost 30 federal government organizations. The culmination was the MDA Summit, held at Johns Hopkins University Applied Physics Laboratory on May 7, 2004, co-hosted by the Honorable James Loy, Deputy Secretary for Homeland Security, and the Honorable Paul McHale, Assistant Secretary of Defense for Homeland Defense. In attendance were senior members of every federal agency with a stake in the U.S. Maritime Domain.

Due to meticulous pre-planning, the senior members of those 25+ agencies were able to agree on just what MDA is, establish its guiding principles, achieve a baseline understanding of the issues involved, and set a course for the way ahead. One of the main findings was that the efforts to provide the maritime security of the United States was heretofore disjointed and lacked clear authority and chain of command. To address this challenge, a senior steering group, made up of deputy cabinet level members, was created, and a team, co-led by the Navy and the Coast Guard, was formed to develop an implementation plan and draft a presidential directive.

An accepted definition of MDA was agreed upon: "The effective understanding of anything associated with the global Maritime Domain that could impact the security, safety, economy, or environment of the United States." This is an extremely broad and ambitious definition, which by its breadth requires unprecedented levels of cooperation among U.S. government agencies, civil authorities, foreign government agencies, and private industry. That cooperative effort is reflected in the broad composition and subject matter of the seven workgroups that were established to address various aspects of MDA. Those workgroups included strategy and plans, legal, outreach, budget and resources, intelligence, common operational picture, and technology.

On December 21, 2004, President George W. Bush signed the National Security Presidential Directive-41/Homeland Security Presidential Directive-13. This dual-titled directive established U.S. maritime security policy and directed the development of a wide-ranging National Strategy for Maritime Security (NSMS) that includes eight policy actions. The NSMS was subsequently signed on September 20, 2005. The eight supporting plans followed suit over the next several months.

The purpose of the directives is to enhance U.S. national security by focusing the disparate maritime security-related efforts occurring across a wide range of government agencies into a cohesive and comprehensive national effort. The first, and most fundamental, of the policy actions is Maritime Domain Awareness. Each policy action has a deliverable due to the president, and, in the case of MDA, this deliverable is a national plan to achieve Maritime Domain Awareness.

To that end the MDA Implementation Team has been created and is now at work.

Platforms

Commercial satellites, and high and medium altitude, long endurance craft, both lighter-than-air and more conventional unmanned aircraft such as the Global Hawk, have the potential to localize and identify vessels on the high seas. Unconventional platforms, such as lighter-than-air vehicles (free-floating and tethered), oceanic surveillance buoys, and new buoys built for ship surveillance, are being considered for surveillance of our approaches. Employing existing oil rigs or even building new, free-floating platforms for surveillance purposes are also under consideration. Nothing is off the table.

Transponders/Beacons

Large commercial vessels now carry a collision avoidance and harbor traffic control device called the automatic identification system (AIS). It contains information similar to the transponders carried on airliners, and work is underway to convert this system to a system similar to air traffic control, to better identify all vessels near U.S. shores. Eventually, AIS may have space-based relays on commercial satellites. These same ships are also required to carry the satellite communication-based Global Maritime Distress and Safety System (GMDSS) which can be polled to determine the ship's location. Additionally, several companies now sell commercial satellite-based asset tracking systems which could also be used as a vessel tracking system at a nominal cost. Both the U.S. Air Force and the U.S. Army are using commercial satellite-based systems for asset and "blue force tracking" to good effect. Expansion of either, or both, for use as an MDA tool is under consideration.

Operational Concept

Coupling long range sensors with cooperative reporting devices, such as AIS, and satellite-based tracking devices, with the mandated advanced notice of arrival—which requires all large commercial vessels to report their intention of entering a U.S. port 96 hours in advance—appears to best establish a baseline as to what is approaching the U.S. coast. Sensors, as described above, coupled with the transponder/beacon systems, could determine which contacts are not reporting, thereby allowing watchstanders and analysts could focus special attention of those few tracks. One of the first things they would do is query data bases to understand known potential problems. A description of some of the tools under consideration is below.

Data Fusion

Another rich area for the development of understanding of MDA's environment is data fusion including, data-mining, pattern recognition and anomaly detection of information in existing databases, owned by a wide range of organizations, including many governmental organizations, international organizations, and cooperative private companies such as insurance, trading, shipping, and ship building and operating companies who fully understand it is in everyone's best interest to participate in the CIE. Analytical software that can either run alone, or in conjunction with data-mining and anomaly detection software, is being developed.

A Look to the Future

Global information system display and decision tools for analysis and decision makers at all levels are also being investigated, as are the means to tie all of these functions together and build a true, real-time, common operational picture. One of the major initiatives in this area is composable FORCENet, which allows the user to define his/her relevant community of interest on the fly. Composable FORCENet, a Navy initiative to build its own service-oriented architecture (SOA), is developing the tools to allow a user to quickly define his own rules for his own information domain, using smart push and pull tools to make optimum use of all information available and relevant to the particular system/console operator. It will build the user defined operational picture.

Great strides can be made toward improving Maritime Domain Awareness through efforts to enable and enhance information sharing among governmental agencies and by incentivizing private industry participation. However, there are significant policy as well as technological challenges to be overcome. Notable synergies will be realized, as various operational pictures are integrated and databases from participating agencies are made available.

Beyond establishing communication pathways, policy, as well as technical, solutions are also being sought to solve issues concerning restricted data accessibility and protection of civil liberties and proprietary information. If anything, the policy issue is actually larger than the technology issues. Much has been done, but more remains to be done. The Navy /Coast Guard team, working together, is fully engaged in developing new ways to safeguard the United States from a wide range of possible maritime threats.

About the author: *Mr. George Guy Thomas is Science & Technology Advisor, Maritime Domain Awareness, U.S. Coast Guard. A retired Navy commander, he has published several articles on technical intelligence, reconnaissance and surveillance systems, and electronic warfare. Mr. Thomas is a distinguished graduate of the Naval War College, he holds a Master's Degree in Computer Information Systems from Bryant College. He is a member of Delta Mu Delta, national graduate school honor society.*

Keeping U.S. Waters Safe and Secure

Industry leadership in port security.

by LCDR Mark Willis
Waterfront Facility Security Branch Chief, U.S. Coast Guard
Office of Port and Facility Activities

by LCDR Malcolm McLellan
Vessel Security Branch Chief, U.S. Coast Guard
Office of Port and Facility Activities

The maritime industry has always played an integral part in the development and implementation of regulations. Without this support and leadership, the regulatory process would be contentious and potentially damage the staunch relationship that the U.S. Coast Guard has developed with maritime industry partners. Their assistance in developing the provisions of the Maritime Transportation Security Act (MTSA) of 2002 was invaluable. During this process, the alternative security program (ASP) was developed to provide industry partners greater flexibility in meeting MTSA requirements.

The Coast Guard was commended by the maritime industry for establishing the ASP provisions that prompted security programs compatible with a large segment of the regulated U.S. merchant maritime fleet. Several organizations, including the American Waterways Operators, Passenger Vessel Association, Lake Carriers Association, and the Offshore Marine Service Association, rose to the challenge and developed ASPs for their specific industry segments. To date, there are nine approved alternative security programs, which include thousands of vessels and facilities throughout the nation.

American Waterways Operators

The American Waterways Operators (AWO) is a national association representing the owners and operators of towing vessels and barges serving inland and coastal waters of the United States. The towing industry accounts for 79 percent of all domestic waterborne freight (Figure 1). Of the 31,449 towing vessels and barges in the towing industry, AWO

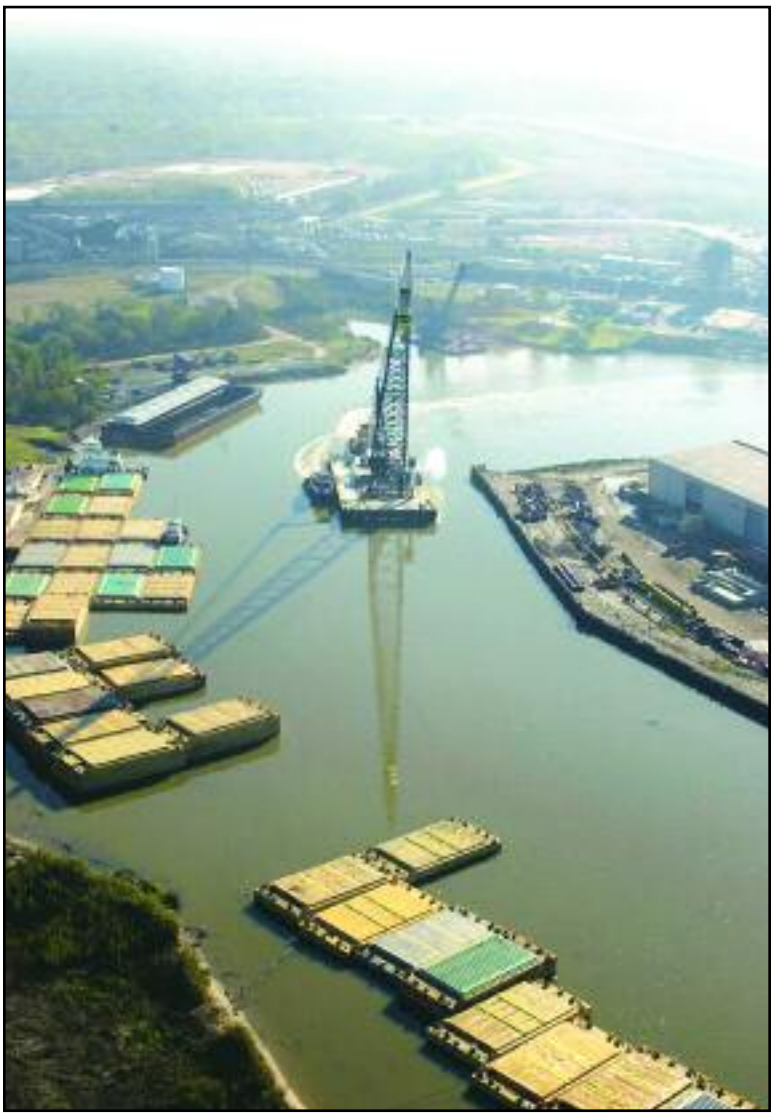


Figure 1: A crane barge manuevers near other barges on the Houston ship channel. PA2 James Dillard, USCG.

member companies account for 80 percent of them. Since September 11, 2001, AWO took a very proactive approach toward development of an ASP for the towing industry.

According to Ms. Amy K. Hewett, AWO's manager, government affairs, "AWO brought together a diverse cross section of members to develop their alternative security program." Their efforts resulted in a practical alternative security program that significantly enhanced the security of the towboat industry.

"The AWO ASP has enabled AWO members to focus on implementing security measures to reduce the vulnerability of their vessels and operations, rather than spending time developing individual vessel plans and obtaining Coast Guard approval," Hewett said.

When asked about changes the AWO would like to see in the ASP portion of the rule, Hewett commended the Coast Guard for allowing trade associations and other industry groups to develop ASPs that address the particular needs of specific segments of the maritime industry. However, she recommended the use of the same compliance checklist by member companies when verifying a vessel's implementation of the AWO ASP.

The Lake Carriers Association

The Lake Carriers Association (LCA) represents U.S.-flagged vessel operators on the Great Lakes. The association has 12 member companies, which operate 55 vessels, including self-propelled vessels and integrated tug/barge units that range in length from 383 to 1,013.5 feet. In fact, 13 of LCA's vessels are more than 1,000 feet long. Cargo carried by these vessels includes coal, iron ore, stone, cement, salt, grain, and liquid bulk products (Figure 2).

Figure 2: The *Columbia Star* navigates a lock.

An LCA-developed alternative security program for Great Lakes carriers was approved by the Coast Guard in December 2004. For its efforts, the LCA was commended by RADM Ron Silva, Commander of the 9th Coast Guard District: "Your foresight will not only assist the Great Lakes community in complying with MTSA requirements but, more importantly, will greatly enhance the security of your vessels and the people of the Great Lakes."

According to Mr. Glen Nekvasil, LCA's vice president, corporate communications, "the primary success of the ASP is that it is tailored to the Great Lakes environment. Also, everyone has a clear understanding of what is required and how best to achieve its goals. What will be most important in the future will be to ensure that any changes in the security regime are based on risk and recognize the difference in operating conditions throughout the U.S. Merchant Marine."

The Offshore Marine Service Association

The Offshore Marine Service Association (OMSA) is a national trade organization of offshore marine operators that addresses and pursues issues relevant to vessels engaged in various offshore activities, including crew boats for oil rigs, offshore supply and utility service vessels, lift boats, cargo and derrick barges, offshore construction and other specialized offshore support vessels. After 9/11, OMSA provided the leadership needed to prevent exploitation of offshore marine industry assets by terrorists.

"OMSA immediately recognized that one of the cornerstones of security for America's vital offshore oil and gas infrastructure was the people and vessels that support that infrastructure," commented Mr. Ken Parris, OMSA vice president. "With offshore sources of oil and gas supplying more than 25 percent of America's energy needs, it was vital to prepare a unified program that would quickly ramp up the offshore industry's security posture."

OMSA took responsibility to develop a unified security plan that could be used across the entire industry and formed a working group of company security officers to develop responses to security scenarios for various threat levels. These recommendations were developed into an industry-relevant ASP and submitted to Coast Guard for approval.

When asked about OMSA's experience in developing and implementing its ASP, Parris said, "Our experience was one of consultation and cooperation. By involving the Coast Guard staff early, and through regular contact, we were able to produce a product that required minimal editing prior to final approval. Deployment and implementation of the plan was facilitated by the use of an industry-wide ASP."

Figure 3: Passengers are screened prior to ferry launch.

The Passenger Vessel Association

The Passenger Vessel Association (PVA) is a trade organization that focuses on the issues and concerns relevant to owners and operators of small passenger vessels. PVA members own or operate passenger ferries, small dinner cruise ships, charter vessels, gaming vessels, excursion vessels, and other small passenger vessels that carry an estimated 200 million passengers each year. The limited resources available and competitiveness of the small passenger vessel industry has made compliance with the MTSA security regulations more challenging. To ensure the security of the passengers, crews, and cargo, it was imperative that this challenge be met and overcome. By partnering with the Coast Guard, PVA was able to develop industry standards for security of passenger vessels that led to the development of an approved PVA alternative security program (Figure 3).

Ms. Beth Gedney, director of safety, security, and risk management for PVA, said, "Developing the ASP was a very positive experience. We believe that the end result is always much better when Coast Guard and PVA develop the document together, to address concerns on both sides; the result is a better product that requires less adjusting afterwards."

PVA president Mr. Gary Frommelt commented, "This is a significant achievement for the passenger vessel industry and a major benefit for PVA members. It means that PVA members will have direct access to a security program that has already been thought through for them. They will have a viable and effective tool that will allow them to efficiently enhance their organization's security, while helping to meet the security needs of our nation."

The Maritime Transportation Security Act has been very successful in enhancing the security posture of the maritime industry and community. A key element of this success has been the leadership provided by the maritime industry's professional organizations. The strong partnership, leadership, and collective professional experience of the marine industry ensured the development of new countermeasures to traditional areas of vulnerability along the waterfront and in the coastal domain. This permitted the Maritime Transportation Security Act to be developed and implemented rapidly following the tragic events of 9/11. Programs such as the ASP continue to ensure that security requirements are catered to the customer, thereby providing the flexibility needed to maintain effective security systems.

About the authors:

LCDR Malcolm McLellan has been in the marine safety field for 12 years, with assignments to Coast Guard Marine Safety Office Mobile, Activities Europe, and MSD Greenville. He is currently assigned to the Office of Port and Facility Activities at Coast Guard Headquarters, where he handles all issues relating to vessel security.

LCDR Mark Willis has been in the Marine Safety and Security Field for 15 years. He has had assignments in Marine Safety Office Puget Sound in Seattle, the Persian Gulf, Container Inspection Training and Assist Team and Marine Safety Office Honolulu. He is currently the Waterfront Facility Security Branch Chief in the Office of Port and Facility Activities at Coast Guard Headquarters.

Maritime Security Training

The specifics of federal and international requirements.

by LCDR Derek A. D'Orazio
Chief, U.S. Coast Guard Marine Personnel Qualifications Division

The Code of Federal Regulations (33 CFR Subchapter H) implements the Maritime Transportation Security Act of 2002 (MTSA)[1]. It also aligns, where appropriate, domestic maritime security requirements with the international maritime security standards contained in the International Convention for the Safety of Life at Sea, 1974 (SOLAS Chapter XI-2), and the International Ship & Port Facility Security (ISPS) Code.

The Coast Guard has partnered with the Maritime Administration (MARAD) and the United States Merchant Marine Academy (USMMA) to develop model maritime security training courses and tables of competence, and a voluntary maritime security training course approval program, in accordance with section 109 of the MTSA.

Internationally, there have been a number of recent developments with respect to maritime security training. The International Maritime Organization (IMO) has developed mandatory training requirements for ship security officers (SSO) for future inclusion in the Standards of Training, Certification & Watchkeeping Convention, 1978, as amended (STCW). IMO has also published a circular with guidance on company security officer training requirements, and similar guidance for port facility security officer training is anticipated in the near future.

The Coast Guard will implement the new international requirements and guidance when 33 CFR Subchapter H is revised. There will be transitional provisions for grandfathering existing certified personnel at the time the regulations are revised.

Current Requirements

Subchapter H requires all personnel on applicable vessels to have some degree of maritime security knowledge, depending on the level of responsibility of the individual; however, the regulations do not currently require formal training. Rather, this knowledge can be obtained through training or equivalent job experience.

Vessel applicability is stated in 33 CFR 104.105. The regulations apply to most U.S. commercial vessels and to foreign commercial vessels operating in U.S. waters. Foreign vessels with a valid International Ship Security Certificate certifying compliance with the ISPS Code are deemed to be in compliance with most 33 CFR Subchapter H requirements, including the maritime security knowledge provisions for vessel and company personnel.

Each vessel to which 33 CFR Subchapter H applies must have a designated Vessel Security Officer (VSO) in accordance with 33 CFR 104.215. All other vessel personnel must meet the requirements of 33 CFR 104.220 or 104.225, depending on whether they have security duties. Each applicable vessel owner/operator is also required to designate a company security officer (CSO)[2], and all company personnel with security duties must have appropriate security knowledge through training or equivalent job experience.[3]

Owners/operators of applicable waterfront facilities must likewise designate a facility security officer (FSO)[4], and all facility personnel must have some degree of appropriate security knowledge through training or equivalent job experience.[5] Facility appli-

cability is stated in 33 CFR 105.105.

Since the regulations do not currently require approved training, the Coast Guard does not at this time approve or certify any maritime security training courses. However, as a matter of enforcement, the Coast Guard evaluates the qualifications of vessel, company, and facility personnel during inspections by assessing their knowledge and ability to carry out their security duties and responsibilities.

MTSA Section 109

Section 109 of the MTSA, "Maritime Security Professional Training," required the Secretary of Transportation, as delegated to MARAD, to develop standards and curricula to allow for the education, training, and certification of maritime security personnel. MARAD and the Coast Guard have been working together to fulfill this mandate through a joint committee that also includes the United States Merchant Marine Academy and the Transportation Security Administration. This group is informally referred to as the MTSA 109 committee.

USMMA, in coordination with the Coast Guard, collaborated with counterparts in India to develop IMO model courses for ship security officer (IMO Model Course 3.19); company security officer (IMO Model Course 3.20); and port facility security officer (IMO Model Course 3.21).[6] These courses respectively align with applicable ISPS Code requirements and with the VSO, CSO and FSO requirements in 33 CFR Subchapter H.

USMMA, in coordination with the MTSA 109 committee, developed competence tables and model training courses for the other classes of personnel specified in the 33 CFR Subchapter H regulations (in addition to VSO, CSO, and FSO):

- vessel personnel with specific security duties,
- facility personnel with specific security duties, and
- maritime security awareness for all other classes of personnel specified in the regulations, including vessel and facility personnel without security duties.[7]

These non-proprietary competence tables and model courses, which align with 33 CFR Subchapter H and the ISPS Code, are freely available to the public on the MARAD Website at: www.marad.dot.gov/MTSA/MARAD%20Web%20Site%20for%20MTSA%20Course.html

In response to industry demand, the MTSA 109 committee also developed a voluntary program for approval and certification of maritime security training courses under section 109 of MTSA. This program is funded by MARAD, and it is currently offered at no cost to training providers. The goal of this program is to promote high quality, uniform training of maritime security professionals. Maritime security training providers seeking course approval and certification are encouraged to submit applications under this program. Full details are available on the MARAD Website referenced above.

International Developments

IMO has developed mandatory training requirements for ship security officers for inclusion in STCW.[8] These requirements will not become internationally mandatory until 2009; however, countries may choose to domestically implement the new SSO requirements sooner than that.

A Coast Guard crew in a 25-foot patrol boat guards the southern tip of New York City as the Staten Island Ferry, *Andrew J. Barberi*, approaches the slip at the South Ferry Terminal. PA2 Mike Hvozda, USCG.

STCW will be revised to add a new regulation, VI/5, "Requirements for the issue of certificates of proficiency for ship security officers." Under these new provisions, candidates for certificates of proficiency

as SSO must have approved seagoing service of not less than 12 months—or appropriate seagoing service and knowledge of ship operations—and they must meet the standard of competence set out in a new section A-VI/5 of the STCW code.

Section A-VI/5 contains a table that specifies the minimum standards of proficiency for SSO. The table lists five separate competences encompassing 29 different knowledge, understanding, and proficiencies, all of which are to be demonstrated through approved training or examination. Physical searches and non-intrusive inspections also require practical demonstration by the SSO candidate.

IMO has also published Maritime Safety Committee (MSC) Circular 1154, dated May 25, 2005, "Guidelines on Training and Certification for Company Security Officers" (cited as MSC/Circ. 1154).[9] This circular contains a competence table for company security officer that is very similar to the new STCW Code section A-VI/5 competence table for SSO discussed above. It includes a practical demonstration requirement for physical searches and non-intrusive inspections for company security officer candidates. Although not mandatory, countries may choose to implement these requirements in domestic regulations.

More recently, the 37th session of the IMO Standards of Training & Watchkeeping Subcommittee (STW 37) developed guidelines on the training and certification of port facility security officers.[10] It is consequently anticipated that the IMO will be publishing an MSC circular for port facility security officer, similar to the one for company security officer, in the near future and that this circular will contain a competence table for use in certifying port facility security officer candidates.

Finally, STW 37 reviewed STCW to identify other areas that might need to include additional mandatory security-related training requirements, in addition to SSO, in support of the ISPS Code. The United States submitted a paper to STW 37 identifying the need to incorporate mandatory security-related training provisions into STCW for ship personnel with security responsibilities and for ship personnel without security responsibilities. The paper also identified the options available for incorporation of these provisions into STCW. This would ensure that all ship personnel have security training and that the level of this training is commensurate with their onboard duties; however, STW 37 was unable to reach agreement on the specifics of this issue. This issue will be further discussed at the next MSC meeting, and at STW 38.

Future Requirements

The Coast Guard will implement the new international requirements and guidance when 33 CFR Subchapter H is revised. Any formal training that is required would be accomplished in the same fashion as other STCW training, necessitating future Coast Guard approval of maritime security training courses.

It is envisioned that there will be transitional provisions for grandfathering existing certified personnel at the time the regulations are revised. However, it is premature to predict exactly what will be required for current personnel to be certified under the revised regulations.

As of this writing, no timetable has been set as to when the Coast Guard will revise 33 CFR Subchapter H. Full information will be published in the Federal Register when the regulations are revised.

About the author: *LCDR Derek A. D'Orazio is the Chief of the Maritime Personnel Qualifications Division at U.S. Coast Guard Headquarters in Washington, D.C. He is a licensed attorney. He was most recently stationed at Marine Safety Office Houston-Galveston for five years, where he served as the Senior Investigating Officer in the nation's largest petrochemical port.*

Endnotes:

[1] The Maritime Transportation Security Act of 2002 is codified at 46 U.S.C. Chapter 701: http://www.law.cornell.edu/uscode/html/uscode46/usc_sup_01_46_06_VI_10_701.html

[2] 33 CFR 104.210.

[3] 33 CFR 104.220.

[4] 33 CFR 105.205.

[5] 33 CFR 105.210 & 105.215.

[6] For more details, access the IMO Website at: www.imo.org/home.asp

[7] A "Maritime Security for Military, First Responder and Law Enforcement Personnel" model training course was also developed in conjunction with the Federal Law Enforcement Training Center. This class of personnel is not referenced in 33 CFR Subchapter H, but the course is designed for military, first responder, and law enforcement personnel without prior maritime background. Emphasis is placed on prevention of acts of terrorism in marine and intermodal transportation systems.

[8] The term ship security officer, as used by the IMO, is synonymous with the term vessel security officer used in 33 CFR Subchapter H.

[9] MSC/Circ.1154: http://www.imo.org/includes/blastDataOnly.asp/data_id%3D12634/1154.pdf

[10] The term port facility security officer, as used by the IMO, is synonymous with the term facility security officer used in 33 CFR Subchapter H.

International Port Security Program

Implementation of international regulations.

by Mr. Mike Brown
U.S. Coast Guard International Port Security Program

The maritime industry is highly vulnerable to terrorist exploitation. A series of terrorist attacks directed at the United States and other nations in recent years have forced many governments to adopt a new perspective towards terrorism and to take a new approach to better deter terrorist acts (Figure 1).

To reach out and partner with other maritime nations, the Coast Guard developed the International Port Security (IPS) program. The IPS program currently consists of more than 30 Coast Guard officers and civilian professionals, stationed at Coast Guard Headquarters and at selected field offices around the world. It seeks to promote international port security by engaging in bilateral and multilateral discussions with trading nations to share and align maritime security practices.

International port security liaison officers (IPSLOs) work with each of our trading partners. Liaison officers are now assigned to work with European nations, Africa, the Middle East, and Asia-Pacific governments, as well as with nations in Central and South America and the Caribbean islands.

Legal Framework

The United States has been working very hard to build a consensus and reach out to its international trading partners to improve the level of maritime security throughout the world to collectively deter, rather than respond to, acts of terrorism. With the support of the United States and other governments, the International Maritime Organization (IMO) wrote and adopted the International Ship and Port Facility Security (ISPS) Code. The ISPS Code took effect on July 1, 2004, and is binding on all IMO member nations.

At the same time IMO was working to develop the ISPS Code, the U.S. Congress was drafting the Maritime Transportation Security Act (MTSA), which required that the U.S. Department of Homeland Security (DHS) learn about the antiterrorism measures in place in ports throughout the world. The Secretary of DHS delegated this responsibility to the Coast Guard.

The Coast Guard's IPS program uses an accepted international standard, the ISPS Code, as a point of reference to engage in discussion regarding antiterrorism measures in place in foreign ports. The IPS program also utilizes the International Labour Organization (ILO) Code of Practice on Security in Ports. The ISPS Code focuses on the ship/port interface, which is a critical element of port security. However, the more overarching framework, as outlined in the ILO Code, helps to fill gaps in the overall review of security measures in place in a country. Looking at security holistically, with the roles of various levels of government and other stakeholders integrated into a comprehensive security regime to augment the individual vessel and facility's efforts, provides the best protection.

Country Visits

The mandate of the IPS program is to visit all U.S. maritime trading partners in the next three years. The Coast Guard has worked with international security experts to develop a system for determining the order in which visits to countries will be requested. Some of the factors that will be considered include:

- cargo volume;
- cargo value;

Figure 1: Terrorist acts have prompted significant changes in the international port security environment. The ISPS Code and the Coast Guard's International Port Security program are two complementary responses to this new threat environment.

- the number of vessels arriving in the United States from a particular country;
- the amount of cargo originating from a country; and
- the amount of transshipped cargo.

Visits are predicated on receiving invitations from trading partners to visit their ports, and to engage their government in discussions on improving port security and aligning security practices.

The Coast Guard learned that many nations believed foreign port facilities would be examined in a similar manner as the Transportation Security Agency (TSA) looks at an airport. This is not the case. The Coast Guard does not intend to check every lock or access control station, but only to get an overall idea of the process used and the scope of how successful the ISPS implementation has been. A review of the ISPS Code implementation at a port facility will be more of a global overview of the security in place.

The ISPS Code is a performance-based standard, and there are multiple ways to implement and achieve compliance. The IPS program looks at the port state's implementation philosophy and not the U.S. interpretation of the ISPS Code. The United States believes it can learn from another country's approach as it hopes other countries can learn from the United States. The Coast Guard in no way wants to infer that a port facility is expected to do more than its government requires.

The Coast Guard begins to engage with a country, normally through the IPSLO, well in advance of a visit. Countries are formally notified by sending them a letter and package, which explains the program and what will hopefully be accomplished during the visit and requests an invitation to visit their country. Background information is shared regarding ISPS implementation, and areas of interest are outlined that the Coast Guard believes would be useful for discussion.

Upon arrival, the Coast Guard visit team normally first meets with the designated authority or government agency responsible for port facility security—this might be the ministry of transport or a maritime agency—and conducts an information exchange. This exchange is a good starting point to fully understand the nation's ISPS implementation process and how the government undertakes its responsibilities in Part A, Section 4-"Responsibilities of Contracting Governments" of the ISPS code.

The Coast Guard reviews the ISPS Code implementation guidance that the country has developed for its own port facilities and ships. This enables the team to better understand the decision-making process used to implement the code. The ISPS Code uses a performance-based philosophy; however, the Coast Guard understands that another country may decide to take a prescriptive approach on certain requirements, such as dictating fence heights, closed circuit TV coverage, or a designated access control system. The Coast Guard is also interested in learning about the assessment and plan review process used by a nation. For example, are recognized security organizations used? If so, how were they chosen, and what authority were they given?

Next, the team visits representative ports that engage in trade with the United States. During these port visits, the team reviews and discusses ISPS Code implementation issues and effectiveness of related antiterrorism measures (Figure 2). During the visit, the team seeks to learn more about:

- access control;
- restricted areas;
- handling of cargo;
- delivery of stores/supplies;
- security monitoring;
- security policies and procedures; and
- security training and exercises.

It is valuable to see first-hand examples of how these issues are addressed, as well as how any security incidents are addressed or resolved. Neither the ISPS Code nor MTSA requires that specific types of physical security measures be imposed to ensure the security of the facility, ship, and cargo. Nations, ports, and facilities are free to decide the best combination of security measures to meet their needs, while ensuring that the purposes of the ISPS Code are achieved. The U.S. government and Coast Guard fully respect that various nations and ports will implement innovative and locally useful practices to meet these security goals.

Discussions with many trading partners reveal that many countries draw upon a similar set of tools when examining their options for implementing effective physical security. These security tools often include walls, fences, and barricades, lighting and signs, access control and searches, alarms, cameras and locks, identification cards, guards, and patrol vehicles and water craft. During the visits, the Coast Guard team looks at these and other physical security measures to understand how the total security posture developed (Figure 3).

The Coast Guard team and the country's port security personnel maintain a continuous and active dialogue regarding each country's practices, challenges encountered, and how they met them. Any questions, issues, problems, or best practices will be discussed with the host government to achieve clarification. The overarching goal is to have a frank and open sharing of ideas so that both the United States and the country being visited can learn from one another to improve security in both countries. All nations that invite the Coast Guard to visit their ports to discuss port security measures are invited to visit the United States and some of our ports to observe how we have implemented the ISPS Code.

Observations

Since commencing these visits in spring, more than 40 countries have been visited, representing every continent. Overall implementation of the ISPS Code worldwide has been good. Most countries have reported their compliance status to the IMO, and the United States has

Figure 2: The Coast Guard visits foreign ports to gain a better understanding of ISPS implementation and to share security practices.

had excellent participation with many of our trading partners. Most countries visited thus far have substantially implemented the ISPS Code.

There is good awareness of the requirements of the ISPS Code, and physical security in most ports is generally good. Sustainability may be a challenge for some countries, and the management infrastructure to maintain effective oversight of continued implementation of the ISPS Code must continue to evolve in some nations as well.

When the ISPS Code was first implemented, many nations, corporations, ports, and facilities expressed concern about the added costs of improved facility security. These concerns were and are understandable; there can be significant costs involved in upgrading security. Once stakeholders examined the issue of improving security against terrorist threats, however, many have found that the collateral benefits of improving facility security justified the investment in security infrastructure for many reasons other than antiterrorism and meeting the requirements of the ISPS Code.

Improved fences, walls, lighting, and access control can result in significantly reduced incidents of theft. Stowaways discovered onboard can be very costly to shippers. The same security measures that protect facilities and ships against terrorism protect ships

Figure 3: Physical security is generally good in most facilities visited.

against stowaways gaining access to ships. Tightly controlled access and movement of trucks can significantly reduce motor vehicle accidents, reducing down-time and the other costs of investigating accidents and damage to vehicles and cargo. Restricting facility access to authorized employees and guests reduces threats to employee safety, and searches of persons entering and exiting facilities could prevent inebriated persons or persons carrying weapons from entering the facility.

Tidy, well-lighted facilities, free from the congestion of unnecessary persons and vehicles, where employees and visitors feel safe while being constantly aware their actions are being monitored, operate with increased efficiency. This results in significantly improved cost savings. Better cargo monitoring and accountability have also led to increased customs revenues.

As a result of the visits, several highly effective, low-cost security measures have been identified. These best practices can be implemented without large capital investments. For example, one country constructed low-cost ramps to facilitate the underside inspection of vehicles. In another case, inexpensive laminated pocket cards with emergency contact information were provided to workers to facilitate emergency communications. These best practices are posted on the Coast Guard's IPSP Website at www.uscg.mil/hq/g-m/mp/xfaqs.html.

Protecting United States' Ports

Vessels coming from insecure foreign ports can pose a significant threat to the ports in the United States and any other country that they call in. It is, therefore, very important to secure the entire supply chain, including the foreign ports.

Nations that have not certified to IMO that they are in compliance with the ISPS Code are listed in U.S. Port Security Advisories, and the Coast Guard imposes conditions of entry on vessels arriving to the United States from ports in those countries. This subjects those vessels to increased scrutiny, delay, and additional costs.

In the event that problems are noted during a country visit, the Coast Guard works very closely with the country to try to resolve the issues. If necessary, a plan of action to improve shortcomings will be discussed. Finding 100-percent compliance all the time is not expected. Things break, and systems can become inoperable. The expectation of the visits is not to see 100-percent compliance but, more importantly, to see how cases of noncompliance are handled. The integrity of each nation's maritime security system and its overall effectiveness are really what interests the team.

It is the Coast Guard's intent to follow up with the host nation regarding any major security deficiencies or concerns with ISPS implementation that are noted during visits. The Coast Guard sincerely hopes that any significant concerns identified during the visit can be resolved and/or addressed within a 90-day period following the visit. The Coast Guard liaison officer(s) responsible for the designated country will work closely with the host nation to accomplish this goal.

Final Thoughts

The Coast Guard is partnering with international organizations such as the Asia Pacific Economic Cooperation Forum and the Organization of American States to assist in capacity building. The Coast Guard is actively engaged with IMO to improve implementation of the ISPS Code. The United States has been partnering with other countries through International Organization for Standardization to develop a standardized method for conducting port facility security assessments and subsequent development of port facility security plans. The hope is that this effort will lead to a standardized approach, which will make it easier for those involved in maritime security to achieve and maintain ISPS compliance.

It is the Coast Guard's intent to continue to work closely with trading partners and other international stakeholders. By working together, the overall security of the global maritime transportation system can be raised to a level that will deter the actions of those whose intent is to cause it harm.

About the author: *Mr. Mike Brown is one of the senior members of the International Port Security Team at Coast Guard Headquarters and has been involved with the program since its inception. Mr. Brown is a retired Coast Guard Captain with 30 years of service and holds master's degrees in political science and national resource strategy.*

Cargo Security

Progress through industry and government cooperation.

by Mr. Basil Maher
President and Chief Operating Officer, Maher Terminals, Inc.

by LCDR Mike Dolan
Chief, U.S. Coast Guard Cargo Security Branch

In the improvement of homeland security, few issues are as challenging as cargo security. Despite the urgency to improve cargo security, it must be done fairly, with reasonable costs, and without slowing the movement of goods that drives the economic engines of the United States. Sound risk management principles must be evenly applied, and technology used where appropriate and beneficial. Given these constraints, there is only one way to make meaningful progress: Industry and government must work together on each and every step of the way.

The Challenges

There are numerous and complex international supply chains that move containers, bulk materials, vehicles, packaged and break-bulk articles, and hazardous materials of all kinds in and out of the United States. A typical international supply chain may have many distinct segments, or nodes, that speed a cargo's journey from the factory overseas to final distribution to the retailer or consumer.

The overarching question remains: How is security for the foreign portions of the supply chains that are in the control of our trading partners secured? The U.S. government does not have jurisdiction in other countries, and individual companies may only have influence on one or two links in the chain. Progress is being made by combining the government's authority and jurisdiction with companies' willingness to insist that suppliers and shippers improve security throughout the supply chain.

The Roles

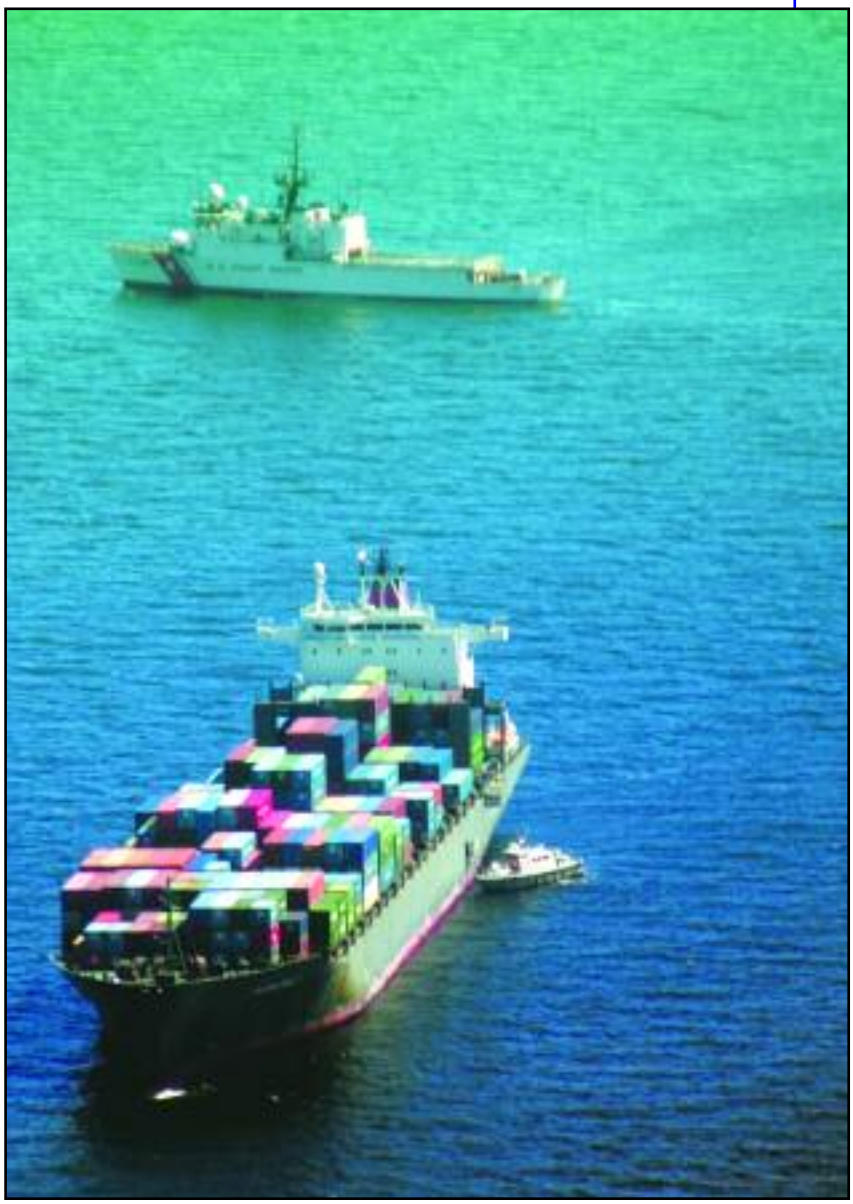
As with national security, cargo security is a government responsibility. Law enforcement agencies and the military perform their respective roles, and the regulatory agencies carry out a plethora of different kinds of inspections and screening of cargo within their authorities and jurisdictions. An example is a Customs and Border Protection (CBP) officer working at a marine terminal, physically inspecting an imported shipment of boxes of finished apparel. The officer is looking for contraband as well as trade violations with regard to the product itself.

There is another role of the government: setting standards. Through regulations and other methods, the government sets the level of security required or expected. The government then checks to see that companies are meeting the standards. This process is called verification, or auditing. To illustrate this role, envision that, while the CBP officer is examining the imported apparel in the warehouse, a Coast Guard Petty Officer is at the facility's front gate, verifying that the guard force is controlling

Petty Officer 1st Class Michael Boyle and bomb sniffing dog Dusty inspect a container and truck for explosives as part of the annual Multi-Agency Strike Force Operation in Long Beach Harbor. More than 300 containers and trucks were inspected by the Coast Guard, local police departments, and the California Air Resource Board, to ensure compliance with various federal, state and local regulations. Dave Hardesty, USCG.

access in accordance with the facility's approved security plan. The Coast Guard did not specify exactly how access was to be controlled; it allowed the facility to decide the best method. The petty officer is making sure they are following their plan.

For their part, private companies have always had good corporate security as a standard business practice, for such age-old reasons as theft prevention, quality assurance, infrastructure protection, and insurance considerations. The actual act of installing and operating security systems is left to each company. Under the theory of a free market, industry seeks the best-value solutions for their security needs, and vendors compete to provide quality products to fill the need. It has long been recognized that good security ultimately improves business competitiveness. Thus, the private sector holds a vast wealth of knowledge and expertise in supply chain security. Whereas these practices used to be driven by efficiency and cost-effectiveness, now companies are also motivated to do their part for homeland security, as well as to avoid having their company being surreptitiously used by terrorists. Companies are thinking broader than their immediate interests.



The Coast Guard Cutter *Escanaba*, a 270-foot medium endurance cutter homeported in Boston, enforces a safety zone around the M/V *Palermo Senator* as a small boat carrying a multi-agency inspection team approaches the cargo ship. PA2 Eric Hedaa, USCG.

So how has government and industry worked together on cargo security since September 11, 2001? Where are we, and what remains to be done?

What Has Been Achieved

The Maritime Transportation Security Act of 2002 (MTSA), a domestic law, was followed quickly by the International Ship and Port Facility Security (ISPS) Code, an international regime that is mandatory for countries that are signatories to the International Convention for the Safety of Life at Sea. These two legal instruments did something very important: They set up compatible security regulations for U. S. ports, commercial vessels, and foreign ports. This covers the maritime portion of the international supply chain, from foreign port to domestic delivery.

In 2002, the Coast Guard was tasked to write the regulations that implemented MTSA. It was a huge task that had to be done quickly—so quickly, in fact, that the normal administrative requirements for public comments on regulations were waived. It was at that point that Coast Guard leadership made two conscious decisions: open a dialogue with industry and make the regulations performance-based.

Given all of the programs and initiatives that are being used to strengthen maritime security, perhaps the most important single activity is the dialogue between industry and government. It is formal, like the new National Maritime Security Advisory Committee, established in March 2005. It is also informal, like the networking that occurs during meetings of the Hampton Roads Area Maritime Security Committee. It is a dialogue that goes beyond the traditional regulatory agency to regulated community interchange, although the MTSA regulations have certainly

generated a lot of those discussions.

As already mentioned, the MTSA regulations are performance based. Vessel operating companies and port facilities have been allowed to develop their own security plans. This gives them some flexibility and allows them to use solutions that work best for their business type and particular operating location. For example, the regulations state that containers must be checked upon entry onto a marine terminal, but how that is accomplished and the frequency of subsequent checks is not specified, until there is a change in the security level.

Implementing the regulations has been a bumpy road, but the interaction and dialogue it has generated at all levels has greatly helped educate everyone on the salient issues. Solutions have emerged that would not have been possible under the typical prescriptive regulatory model. For example, when it came time to implement facility security plans, the port terminals and the Coast Guard worked cooperatively to meet certain deadlines, while recognizing the needs of the port businesses to keep operating efficiently. Issues were openly discussed, so the important major security actions were implemented and not impeded by misunderstandings over less important portions of the plans.

Future Challenges

The role of technology in cargo security is a huge and continuingly evolving issue. We have seen new product development, grant programs, government research, international technical standards development, and vigorous debate on exactly what role technology should play and when. Initially inadequate for the rigors of maritime transport, the physical equipment continues to rapidly mature. Devices and applications for individual container security are of particular interest, being the most affected by unit costs. The challenge is to judge when, how, and what technology is to be employed across a portion of the supply chain to achieve valuable security improvements.

Since an attack on the marine transportation system is generally accepted as being probable, the flow of commerce during and after an event must be continued—not just as a matter of keeping the economy strong, but in recognition that the waterborne transportation system itself is an asset to be used for evacuations and to provide relief supplies to victims. The government may need to apply controls on the physical systems. However, industry experts hold the knowledge that is needed to truly discern and understand additional threats to the system, as well as the direct and indirect effects of various actions that might be used to mitigate additional damage. How are the right people rapidly identified and consulted to enable good decisions to be made quickly? Government and industry leaders are collaborating and working on solutions to this critically important problem.

A great challenge of cargo security is addressing the portions of supply chains that are overseas, not directly controlled by the U.S. government or domestic companies. Programs such as the Customs-Trade Partnership Against Terrorism have opened new approaches to incentive-based programs and the training of foreign supply chain security specialists. Future work will see the expansion of voluntary international standards for industry use, as well as development and implementation of supply chain security programs in the World Customs Organization and possibly in the International Maritime Organization. Each organization and standard will strengthen security in additional areas of the international spectrum, thus incrementally denying the use of supply chains to enemies.

Conclusion

The United States recognizes the threat of terrorists using the mechanisms of global trade to attack citizens in its homeland. Americans are fiercely competitive in the business world, and a healthy separation is maintained between government regulations and the free market. But, in this urgent effort to protect the homeland, private business enterprises and government agencies are working closely together. If the government sets high but fair standards, and industry partners harness their immense collective power to solve tough problems, the United States can ensure its transportation system will not be used against it.

Progress is being made by combining the government's authority and jurisdiction with companies' willingness to insist that suppliers and shippers improve security throughout the supply chain.

About the authors: *Mr. Basil Maher is the President and Chief Operating Officer of Maher Terminals, Inc. He is also a member of the National Maritime Security Advisory Committee and President of the National Association of Waterfront Employers.*

LCDR Mike Dolan is Chief of the Cargo Security Branch at U. S. Coast Guard Headquarters. LCDR Dolan enlisted in the Coast Guard in 1991 and has served in port operations positions in Port Canaveral, San Juan, and Norfolk.

Central California Area Maritime Security Committee

Port security put to the test.

by LCDR Anthony C. Curry,
Chief, Contingency Planning & Force Readiness,
U.S. Coast Guard Sector Los Angeles-Long Beach, Calif.

by Mr. Robert T. Spaulding,
Port Security Specialist,
U.S. Coast Guard Sector Los Angeles-Long Beach, Calif.

The fishing vessel *Mary Lou* has set out for a day of fishing. Suddenly, there is an explosion, and the boat quickly sinks in flames. Emergency crews race to the scene and find the area saturated by mines. The first true test of the newly formed Central California Area Maritime Security Committee (AMSC) was underway. This event signaled the start of the Lead Shield/Rogue exercise—a full-scale antiterrorism exercise, developed to test the committee's ability to form a unified command and respond effectively to a large-scale terrorist attack.

Figure 1: An aerial view of the port of Los Angeles–Long Beach.

Central California Area Maritime Security Committee

The Central California AMSC was established in February 2004, as mandated by the Maritime Transportation Security Act of 2002. The committee's mission is to advise the federal maritime security coordinator on the identification of critical port infrastructure and operations, risks, and mitigation strategies and methods. The committee also advises on the development of a continuous overall port security evaluation process that includes contingency plan development and dissemination of maritime security-related information to port stakeholders. The executive steering committee is composed of 15 voting members and six nonvoting members and encompasses a wide spectrum of government agencies, port operators, labor unions, political representatives, and other maritime community members.

With such a diverse membership, a process-oriented structure is a critical component for success. The National Incident Management System/Incident Command System, as developed by the California Department of Forestry, was chosen by the executive steering committee to give this organization the framework to function as both a prevention and a response entity. This concept has proved successful for decades as a means of

effectively unifying the efforts of numerous agencies. It enables the AMSC to put into place a system of continuous improvement that utilizes lessons learned from exercises and actual responses.

The committee is a collaborative effort, with membership from all aspects of the port community; it truly is an area committee. The Coast Guard chairs this dynamic committee and has guided the group from the critical inception stage and continues to work closely with myriad port stakeholders to maintain an atmosphere of ownership and partnership. The Federal Bureau of Investigation (FBI) serves as the vice-chair of this committee. This is a huge benefit, as it gives the committee ready access to a wide range of federal criminal investigative and intelligence services. The combined leadership and expertise the Coast Guard and FBI bring to the committee provide a strong regulatory foundation and response expertise to handle any number of security-related challenges that face the Port of Los Angeles–Long Beach (Figure 1).

The committee is composed of four sections in accordance with the ICS structure: operations, finance/administration, logistics, and planning/intelligence. Each of these sections is chaired by a voting member agency. The operations section is chaired by the Los Angeles Police Department; the finance/administration section is chaired by the California Office of Emergency Services; the logistics section is chaired by the Los Angeles Sheriff's Department; and the planning/intelligence section is chaired by Immigration & Customs Enforcement. Enthusiastic acceptance of this organizational structure inspired the Transportation Security Administration to copy the model and form a similar committee that addresses security challenges at Los Angeles International Airport.

The Central California AMSC meets on a quarterly basis to discuss ongoing security initiatives, the progress of grants within the port complex, and future multi-agency exercises. Motions for actions and activities must be passed by a majority of the present voting executive steering committee. In addition, the committee has hosted numerous distinguished guest speakers, such as then-Department of Homeland Security Secretary Tom Ridge, Senator Diane Feinstein, Congresswoman Lucille Roybal-Allard, and acclaimed homeland security expert and author Steve Flynn.

Figure 2: Dolphins were used in exercise Lead Shield/Rogue to detect mines.

Testing the System

Although the committee is less than two years old, it has already been tested under two major exercises: Determined Promise '04 and Lead Shield/Rogue (Figures 2, 3, and 4). During the latter full-scale exercise, for the first time, the Central California AMSC functioned as the core of a unified command. This gave numerous port stakeholders the opportunity to be a part of the readiness process from the initial planning stage to the "hot wash." The experience enlightened port stakeholders to the fact that response is the applied portion of prevention. This new perspective on this process infused the numerous Central California AMSC members with enthusiasm for making their port complex the best prepared in the country.

Figure 3: Mobile command post for exercise Lead Shield/Rogue.

Another key benefit of the AMSC is that all plans and documents that are produced by the organization are truly team efforts. The first plan was the Area Maritime Security Plan, which had the goal of

improving the safety and the security of the Los Angeles–Long Beach Port complex. This plan is an evolving document that lists all critical infrastructures and AMSC assets and provides important contact guidance within the AMSC hierarchy. In light of the highly criticized governmental responses to recent natural disasters, it was evident that there was a need to have a coordinated port evacuation plan.

In October 2005 the Central California AMSC held the first in a series of workshops that will help shape the focus and contents of a new AMSC port evacuation plan. The purpose of the first workshop was to identify the challenges faced by the port, regarding port evacuation, recovery, and reconstitution. The sector contingency planning staff consolidated the findings of this workshop and drafted a white paper that captured and organized a wide variety of critical port concerns. The evacuation subcommittee will use this white paper to collaboratively develop a draft port evacuation plan that focuses on the safe and efficient evacuation of the ports of Los Angeles and Long Beach.

Figure 4: Training for exercise Lead Shield/Rogue.

Once the port evacuation plan draft is complete, AMSC plans to test the plan during the upcoming PortStep tabletop exercise this summer. Refinements to the plan will be made based on the lessons learned during this exercise. This process exemplifies the Central California AMSC's desire to engage only in exercises that test a plan and have thorough metrics to measure performance, based on established criteria. Thus, lessons learned during the exercise are captured in a meaningful way, and area plans are continuously improved.

Real-Life Application

By working together during meetings, exercises, and plan preparation, the AMSC member organizations have formed strong relationships with each other that will be invaluable during any major crisis requiring a coordinated response. The first few hours of any response effort are absolutely critical for first-responder coordination. Recently, the Central California AMSC engaged its joint coordination center (JCC) in response to the 2005 London terrorist attacks on mass transit. The JCC, similar to a crisis action center, is comprised of personnel from numerous first-responder agencies. It was designed to coordinate joint agency preventative security operations within the port complex during increased maritime security levels, or based on specific credible intelligence. Within hours of the London attack, the JCC quickly and efficiently coordinated increased waterside and landside patrols by a wide range of law enforcement agencies. The intelligence gathered by the patrols was rapidly presented to the AMSC through the FMSC. Without a doubt, the JCC has proven itself as a worthwhile security instrument that requires only a minor investment of resources.

Due to enormous media interest in the port complex, the AMSC proposed the formation of a public relations and joint information center subcommittee during the August 2005 quarterly meeting. Once established, this group will be composed of a cross section of member agency's public information officers. These personnel will work closely together to consistently provide press releases, interview coordination, and other vital public information services to the unified command and the media.

The terrorist attacks on September 11, 2001, and recent natural disasters have taught us the importance of having senior local government leadership and first responders familiar with working together. The Area Maritime Security Committee concept has proven itself a very successful strategy. However, the strategy by itself is not enough. The reason this committee is so successful is due to its Incident Command System structure, excellent interagency communication, and teamwork.

About the authors: *LCDR Anthony C. Curry is currently Chief of Contingency Planning & Force Readiness for U.S. Coast Guard Sector Los Angeles-Long Beach, Calif. He has served in the Coast Guard for 16 years. Previous assignments include MSO Honolulu; MSO/GRP Los Angeles-Long Beach; MSO Portland, Maine; and the National Maritime Center. He holds a B.S. in management from Northern Illinois University and a M.S. in quality systems management from the National Graduate School.*

Mr. Robert T. Spaulding is a Port Security Specialist for U.S. Coast Guard Sector Los Angeles-Long Beach, Calif. He has spent 20 years on active duty: 10 years U.S. Navy and 10 years USCG. He retired as a U.S. Coast Guard LCDR. Previous assignments include MSO Honolulu and MSO Galveston. He holds a B.A. in education from National University.

Port Coordination in the Largest U.S. Petrochemical Complex

A public/private partnership.

by LCDR D. Hauser
Assistant Chief of Response, U.S. Coast Guard Marine Safety Office Houston-Galveston

In November 2001, 30 maritime stakeholders from southeast Texas assembled in the Port of Houston Authority's boardroom and unanimously agreed to charter the area's first port security committee. Four years later, the Houston-Galveston Area Maritime Security Committee (AMSC) has grown into a stronghold of over 70 appointed members, with a following of 800 government and industry stakeholders, all serving to protect the second largest petrochemical complex in the world.[1]

The ports of Houston, Texas City, Galveston, and Freeport are home to more than 140 Maritime Transportation Security Act (MTSA)-regulated facilities, from barge cleaning operations to the world's biggest petrochemical producers. The area is home to Dow Chemical's largest chemical plant in the world,[2] Exxon-Mobil's largest refinery in the world,[3] and Shell's largest refinery in the United States.[4] All operate under one Coast Guard Captain of the Port (COTP). One-fourth of the nation's petroleum products are refined just inside the Gulf Coast, along the Houston Ship Channel[5]; a 53-mile long, 45-foot deep man-made channel, dredged more than 90 years ago to accommodate deep-draft vessels. It was believed that the inland channel was a safe location and was less costly than operating along the Gulf Coast.

Today, the ports of Houston, Texas City, Galveston, and Freeport are densely landscaped with refineries, chemical plants, cruise ship terminals, and the nation's second largest recreational boating community in Galveston Bay.[6] Just south of the four ports, offshore platforms dot the Gulf of Mexico. It is a 60-mile drive from Houston to the most southern port city of Freeport, Texas, and, in this stretch of roadway, the petrochemical infrastructure is neighboring the state's largest city within a 10-county metropolitan area of 5.1 million people.[7]

How does one COTP ensure that every MTSA-regulated commercial interest—as well as nonregulated entities using the waterway, along with a broad group of government employees—work together effectively to protect private assets and public infrastructure? The Area Maritime Security Committee has been a tremendous vehicle used to drive the security agenda home, and, although it is difficult to measure success by what may have been prevented, the Houston-Galveston AMSC has clearly been a port model worthy of notice.

Organizing Maritime Transportation System Stakeholders

The Houston-Galveston AMSC is comprised of a maritime industry subcommittee and law enforcement subcommittee. Additionally, there is an executive steering group made up of federal agency heads, the State of Texas, and chairpersons from the two subcommittees. The executive steering group sets the annual goals for the committee, ensuring alignment with Homeland Security directives. AMSC's accomplishments include a local communications system with 800 registrants and the development of an area maritime security plan that has been receiving accolades from reviewers. AMSC also has several work groups, comprised of volunteers who assist with developing joint industry and government training programs, exercises and drills, communications products, and port coordination procedures.

Just as other Area Maritime Security Committees in the nation are addressing unique issues in their ports,

the Houston-Galveston AMSC identified ways to consolidate various port safety and security initiatives and unite the efforts of different committees. For instance, the training and public affairs workgroups from the Central Texas Coastal Area Committee and Houston-Galveston AMSC have consolidated, which provided joint training opportunities and improved individual work-time efficiency, by reducing the number of meetings participants attended.

Port Coordination: Meeting the Challenges

During an elevated threat level in the nation's number-one port for foreign waterborne commerce,[8] and with more than 11,000 U.S. and foreign flag deep-draft vessels reporting into vessel traffic service annually, receiving security attainment status reports from regulated facilities and vessels would likely strain local Coast Guard resources. Assistance was needed to coordinate the receipt of attainment reports from industry during Maritime Security Level 3 (MARSEC 3). Assistance came, and it was received from the very same people whose companies the Coast Guard regulated. Industry volunteers tackled one of the toughest port management issues in the Houston-Galveston area when they developed the port coordination team (PCT) concept. They successfully bridged security attainment information for the four port areas, plus the offshore sector, linking it to the local federal maritime security coordinator (FMSC) during an elevated MARSEC condition.

The industry-led PCT galvanized maritime stakeholders from across a large, regional port area and ensured that the FMSC had a process in place to restart vessel movements and facility transfers after a temporary shutdown. Although facility and vessel owners and operators focused their security efforts on protecting company assets, they were equally concerned about protecting the integrity of shared infrastructure like the man-made Houston Ship Channel. It was in their best interest to engage through the AMSC with other stakeholders to ensure that traffic management schemes and procedures supported the restoration of maritime business.

It was expected that, during MARSEC 3, maritime commerce would temporarily pause. The AMSC determined that a general instruction guide or pause checklist was needed to ensure alignment with PCT procedures. The Area Maritime Security Committee established the pause workgroup in advance of the completion of MTSA vessel and facility security plans. Industry, together with the local Coast Guard, developed a pause checklist[9] for vessels and facility operators that supplemented the port coordination team procedures. The checklist succinctly outlines the immediate actions that vessel and facility operators must take during MARSEC 3 to support the PCT process. The checklist, used in conjunction with facility and vessel security plans, has been incorporated into the area maritime security plan.

The combined ports of Houston-Galveston see a variety of traffic and service a variety of customers, including tankers, bulk carriers, rigs, cruise ships, barges, and container vessels. Pictured is a segment of the Galveston ship channel during a busy day. PA2 James Dillard, USCG.

The port coordination team is comprised of members from the ports of Houston, Texas City, Galveston, and Freeport, and offshore sector. As described in the PCT's operating procedures: "These members represent core constituents responsible for consolidating information from their respective groups in order to provide information to the COTP on port infrastructure needs. The procedures further explain that as a conduit through which information flows, the PCT permits the COTP to establish shipping priorities, implement port reopening protocols and better manage the flow of vessel movement without compromising the safety and security of the impacted ports."[10]

Testing the Port Coordination Concept

Since September 11, 2001, the Port of Houston has experienced five jumps in maritime security conditions, either by an upgrade to MARSEC Condition 2 or through modified MARSEC surges that required additional Coast Guard resources and security measures to protect critical infrastructure. Additionally, the AMSC sponsored two security exercises to test communications and PCT procedures. These secure liberty exercises activated the port coordination team and required members to mobilize to the four port areas, communicate with MTSA-regulated facilities, and issue attainment reports through the operations section to the federal maritime security coordinator.

During Secure Liberty II, the four ports and the offshore sector stood up separate port command centers that were located at each of the port offices. The port command centers were organized geographically and were staffed by a port representative, industry members, and a Coast Guard liaison. The port coordination team, which is the core group responsible for collecting information from the different command centers and reporting it to the incident commander, mobilized to the Houston-Galveston Marine Safety Office and augmented the operations section. Vessel traffic service (VTS), co-located with the MSO, received attainment reports from underway vessels, and, since the vessel traffic service also has vessels docked at facilities, it was a natural fit to locate the port coordination team next to VTS to strengthen maritime domain awareness by having a common operating picture.

The port coordination team mobilized to MSO Houston-Galveston included:

- PCT liaison (chair of maritime industry subcommittee);
- Port of Houston liaison to the port command center (industry rep);
- Port of Texas City liaison to the port command center (industry rep);
- Port of Galveston liaison to the port command center (industry rep);
- Port of Freeport liaison to the port command center (industry rep);
- offshore liaison to the port command center (industry rep);
- non-VTS user representative (auxiliary waterways recreational vessel rep); and
- law enforcement representative (chair of the law enforcement subcommittee).

Specific capabilities that exist at the primary port coordination team gathering site in Houston include:

- closed circuit TV feeds from vessel traffic service;
- real-time automatic identification targets;
- limited access to the Coast Guard common operating picture (C2PC);
- Internet access;
- telephone access; and
- general administrative support.

With such a large contingency of facilities and vessel operators, it was important to announce the exercise well in advance, so that operators knew what to expect during a simulated, temporary port shutdown triggered by a MARSEC 3. During the exercise, facility operators were given the choice to implement or simulate implementing their security plans and measures for MARSEC 3. Once each facility security officer was satisfied that all security measures had been attained, each contacted their respective port command center to report the status of their facility. A pause checklist, port command center contact information, and operating procedures were provided prior to the exercise on the AMSC's Website, so all the participants knew what to do and who to contact.

During the Secure Liberty II exercise, more than 700 port stakeholders were notified at 6:05 a.m. of the simulated increase to MARSEC 3 through a notification call-out system. Forty-five minutes later, the first port

coordination team member arrived at the MSO. At 8:30 a.m., the port coordination team was fully functional. By 10:20 a.m., more than 80 percent of the MTSA facilities, including offshore, reported MARSEC 3 attainment of security measures for the entire Houston-Galveston COTP area.

Aggressive outreach about the exercise greatly enhanced the speed with which attainment reports were submitted and dually served to prepare industry for a real incident. The port coordination team had access to the Internet at MSO Houston-Galveston and used a shared spreadsheet to enter data received by the port command centers. Information was quickly documented and communicated to the federal maritime security coordinator.

To guarantee a successful transfer of port status information from the command centers in the field, the PCT must have a direct line of communication to the incident command staff, which is best accomplished through a PCT liaison. The PCT liaison, Mr. Raymond Butler, also serves as the AMSC maritime industry subcommittee chairperson.

Other Possibilities Beyond Security

The PCT concept is not limited to threat-level elevations. Applying the procedures, either partially or wholly in small or large ports, can also easily be accomplished for waterways management issues, such as vessel casualties or natural disasters. The PCT is designed so that elements can organize either geographically or functionally, which aligns with the national incident management system (NIMS) model. The PCT construct provides an expandable and flexible organizational structure, regardless of the event. For instance, the PCT has been activated in Houston during heavy-weather incidents and during extended, limited visibility closures, when the COTP deemed it necessary. In these instances, the PCT members did not physically relocate to the different port areas. Various port stakeholders, representing constituents from different locations spanning the maritime transportation system, conducted operational planning and port status meetings telephonically. During these safety-related, waterways-management evolutions, core constituents include:

- Port of Houston Authority;
- Port of Texas City;
- Port of Galveston;
- Port of Freeport;
- offshore port (lightering interests);
- American Waterways Operators (such as tow companies);
- West Gulf Maritime Association (such as agents and labor);
- Houston Pilots Association;
- Galveston-Texas City Pilots Association;
- oil refiners;
- oil terminals;
- chemical carriers;
- non-VTS users (such as recreational and fishing vessels); and
- harbor tugs.

Once the PCT is activated for waterways-management issues, the PCT is naturally suited for recommending port reconstitution protocols to the COTP for restoring commerce in the impacted port area. Recommended guidelines may include:

- imposing traffic measures to minimize overtaking situations;
- staggering the entry of vessels into the Houston Ship Channel;
- identifying particular vessels/cargos for priority entry into the port(s); and
- identifying critical berths that require vessel departures.

Regardless if the incident or port waterways management issue has a safety or security focus, or requires an organization based on function or geographic location, the PCT has been an extraordinary force, comprised of the best minds in the petrochemical industry. Establishing the port coordination team network has successfully fused private and public entities, providing the local FMSC with real-time information on the status of maritime interests in the ports.

It is with optimistic caution that some federal regulators look toward industry to self-regulate and advance stewardship ideals that transcend beyond the bottom line. The Coast Guard, through the COTP staff, views volunteers from the private sector with grateful appreciation. Industry stakeholders from Houston, Texas City, Galveston, and Freeport have been willing to give an inordinate amount of time to ensure a safe and secure port area for the collective good of all maritime commerce. Their stewardship clearly illustrates the meaning behind the four pillars posted on the industry-driven AMSC Website, which are the fleet of four ships: relationship, partnership, stewardship, and leadership. These are routinely referenced by the local COTP as watchwords to industry and the Coast Guard crews throughout the region.

In the Future

As Coast Guard personnel who currently work with

Marine Safety Unit Houston is located on the Houston ship channel. PA2 James Dillard, USCG.

the port coordination team transfer out of the area and Sector Houston is born, the future of the port coordination process will depend heavily on the maritime community's continued involvement with the AMSC. To ensure their participation, it is necessary that Coast Guard leadership continually facilitate dynamics that foster industry's investment in the security of their ports by communicating the criticality of shared infrastructure and shared partnerships.

The PCT concept has functioned effectively in Houston and Galveston and demonstrated that viable partnerships with industry are rewarding and serve to leverage resources when government assets are in high demand. Established, professional relationships lead to solid partnerships and, in the case of the PCT, result in practical port coordination procedures that encompass vital communication and notification protocols.

Rich with Capabilities

Appointed AMSC members and numerous other stakeholders attend bimonthly meetings, which typically fill the Port of Houston Authority's boardroom to standing-room only. Those who come to meetings and join the workgroups possess an abundance of technical skills and professional expertise in managing complex projects and building consensus. Although the local Coast Guard steers the port security agenda, the port community brings additional skills and a high level of enthusiasm to the process that helped shape a successful security planning program.

For more information on the Houston-Galveston AMSC or PCT procedures, please access www.amsc-hougal.com.

About the author: *LCDR D. Hauser is Assistant Chief of Response at U. S. Coast Guard Marine Safety Office Houston-Galveston.*

Endnotes

1. Port of Houston Authority, "General Information: The Ports Present," (Houston: POHA, accessed October 30, 2005); available from http://www.portofhouston.com/geninfo/overview2.html; Internet.
2. Dow Chemical Company, "The Dow Texas Operations Public Report," (Midland: Dow, accessed October 30, 2005); available from http://www.dow.com/publicreport/2002/local/texas_ops/overview/overview.htm; Internet.
3. Office of Energy Efficiency and Renewable Energy, ExxonMobile Chemical Company (Houston: DOE, accessed October 22, 2005); available from http://texasiof.ces.utexas.edu/texasshowcase/pdfs/casestudies/cs_exxonmobile.pdf; Internet.
4. Randi Kaye, American Morning, Cable News Network – CNN (Aired September 23, 2003, transcript accessed October 27, 2005); available from http://transcripts.cnn.com/TRANSCRIPTS/0509/23/ltm.04.html; Internet.
5. Energy Capital Houston, "A World Class Industry," (Houston: Houston Publications, accessed October 30, 2005); available from http://www.energycapitalhouston.com/articles/article04.html; Internet.
6. Bay Area Houston Economic Partnership, "Recreation," (Houston: Bay Area Houston, accessed November 8, 2005) available from http://www.bayareahouston.com/Home/LivingEnvironment/Recreation; Internet
7. Wikipedia, "Greater Houston," (Encyclopedia Online: accessed November 1, 2005) available from http://en.wikipedia.org/wiki/Greater_Houston; Internet.
8. American Association of Port Authorities, "Port Updates," (Alexandria: AAPA, accessed November 2, 2005) available from http://www.aapa-ports.org/pressroom/hurricane_updates.htm; Internet.
9. Area Maritime Security Committee – Houston Galveston, "Pause Checklist," (Houston: AMSC, accessed October 10, 2005) available from http://www.amsc-hougal.com/event.htm; Internet.
10. Area Maritime Security Committee – Houston Galveston, "Port Coordination Team Standard Operating Procedures," (Houston: AMSC-PCT, accessed October 30, 2005) available from http://www.amsc-hougal.com/support/pctprocedures.pdf; Internet

Asymmetric Migration

Stowaways, absconders, and deserters.

by LCDR Mike Cunningham
Legal Advisor, U.S. Coast Guard Inspections and Compliance Directorate

Asymmetric migration—stowaways, absconders, and deserters—is not only an immigration problem, but a port security problem as well. U.S. Customs & Border Protection (CBP) and the Bureau of Immigration and Customs Enforcement (ICE) are the agencies with primary responsibility for deterring, responding to, and taking remedial action for illegal entry, even in U.S. maritime ports. The Coast Guard has been working in close cooperation with CBP and ICE to combat the problem of asymmetric migration, not only to support other agencies in enforcing U.S. immigration laws and preserve the right of the United States to control its borders, but also to address the port security risk represented by these illegal migrants.

Generally, an absconder is a crewmember who, without legal authority, lands in the United States. A deserter is a crewmember who is permitted to land in the United States but overstays the legal authority to remain. A stowaway is a person who is secreted on a ship without the consent of the ship and who is detected onboard the ship after it has departed from a port.

Some crewmembers are further characterized as a high-risk, detain onboard crewmember or high-risk crewmember. This is a crewmember who has been denied permission to land in the United States and is a national of a country listed in the Coast Guard/CBP Standard Operating Procedures for responding to high-risk crewmembers.

ANNEX I
Minimum Standards for Contracted Crewmember Security Services

Contracted security guards who are not designated state or local law enforcement officers must provide full name and date of birth to CBP [Customs & Border Protection]. CBP will conduct a background check using CBP automated enforcement systems.

Contracted security services must meet or exceed the following standards to demonstrate competency and adequacy to perform the assigned task:

1. Contracted security guards must be armed with a firearm while on duty, consistent with the requirements and conditions of the facility, and the laws and regulations of local, state, and federal authorities. This includes proper credentialing, licensing, and permitting, as applicable.
2. Contracted security guards must display proper identification at all times, such as a laminated badge with a photograph that clearly identifies them as part of the contracted security service.
3. Contracted security guards must be fully apprised of all applicable use of force requirements and conditions within the particular jurisdiction, including requirements and conditions for use of force imposed by the facility.
4. Contracted security assigned to provide security services are to ensure that only those crewmembers authorized to disembark are allowed to do so. Pursuit of fleeing crewmembers and use of force in such situations must comply with the requirements and conditions of the facility, and the laws and regulations of local, state, and federal authorities.
5. Security services must be contracted before the vessel is given permission to enter port. Contract must ensure the security services are in place before the vessel is allowed to moor or anchor in close proximity to land.
6. Security services must have a copy of the entire crew list, with the names of those who are not authorized to go ashore highlighted. The security services must verify the identity of any subject requesting to come ashore, checking the subject's stated name against that found on the passport and/or seaman's book with proper VISA, and checking the subject's physical appearance against those descriptors found in the document presented and against the photograph on the identity document.
7. Contracted security guards assigned to provide security services at vessels on which CBP has detained crewmembers shall be capable of communicating with the facility security, police, security dispatcher, local CBP, local USCG, and vessel agent. Contracted security guards shall provide their own communications as part of the contractual agreement between the ship's agent and the security company as dictated by the situation. For example, if the terminal has a 24-hour operations center, radio communications may be appropriate; otherwise a cellular telephone or functional equivalent may be required.
8. Contracted security guards must be provided with sufficient shelter to protect against severe weather conditions such as high heat, oppressive sunshine, and extreme cold. The shelter must be in the immediate vicinity of the gangway but should not be so obstructed as to prevent the security guards from performing their assigned duties.
9. Contracted security guards must be provided with periodic breaks to use the restroom and eat meals at intervals not to exceed 4 hours, and no guard may stand watch for more than 12 hours in a 24-hour period.
10. Contracted security guards must have written operating procedures and contact numbers readily available. See Annex II for a sample format.

Stowaways

The Coast Guard takes the presence of a stowaway seriously. The presence of a stowaway indicates a security incident has occurred in which a person has improperly gained access to the vessel, circumventing vessel access control procedures. Clear grounds also exist that the vessel does not comply with Coast Guard maritime security regulations or the maritime security provisions of Chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS) and the International Ship & Port Facility Security (ISPS) Code.

Coast Guard units take appropriate action to ensure that the security, rights, and obligations of the United States are protected. This analysis includes an examination of actions taken by the vessel to detect, detain, and report the presence of stowaways prior to port entry, efforts that may reduce the security risk posed by the stowaway.

The Coast Guard stowaway response policy has two aspects: responding to stowaways present on vessels and addressing the security issues in the ports where stowaways originate. Response actions in a stowaway case are based on the facts and circumstances in each case. These actions also include Coast Guard and interagency boardings; regulatory compliance examinations, either for compliance with the ISPS Code or 33 C.F.R. part 104, to determine any deficiencies in the ship security system; support of CBP/ICE criminal investigations; and ensuring adequate security if the stowaway remains on board for repatriation.

With regard to the source of stowaways, the Coast Guard stowaway response policy includes provisions to increase scrutiny for vessels arriving from ports that generate significant numbers of stowaways. It also includes outreach efforts to the governments of source countries, through the Coast Guard International Port Security Program, to improve the security in those ports.

Absconders and High-Risk Crewmembers

To respond to the problem of high-risk crewmembers, the Coast Guard and CBP have entered into "Memorandum of Agreement Regarding the Detention of Certain High-Risk Crewmembers," which came into force December 22, 2004. The purpose of the MOA and its accompanying standard operating procedures (SOP) is to provide consistent, nationwide guidance; it also defines the respective roles of the Coast Guard and CBP regarding preventing high-risk, detain-onboard crewmembers from leaving their vessel and illegally entering the United States. Portions of the SOP are designated sensitive security information and are not available for public release.

CBP determines whether a foreign crewmember will be allowed to disembark a vessel upon its arrival into the United States. Foreign crewmembers may be denied temporary permission to land in the United States for a variety of reasons. When a crewmember has been denied temporary permission to land in the United States and poses a high security risk to the port, the Coast Guard may assist CBP by ensuring that the master, owner, agent, and/or operator of the vessel has provided effective security measures to keep the identified high-risk, detain onboard crewmember from gaining illegal entry into the United States.

The SOP provides guidance for coordinating CBP and Coast Guard efforts to identify high-risk crewmembers and ensure that effective security measures are

ANNEX II

Standard Operating Procedure For Contracted Crewmember Security

1. Security services must be in place before vessel arrives pier-side or onboard as per COTP Order.
2. Security services must have a complete crew list identifying those crewmembers that are not authorized to go ashore.
3. Security services must maintain a detailed log (times, reasons, etc.) of all persons going aboard and going ashore.
4. A muster of all individuals that are not authorized to go ashore shall be conducted every 4 hours.
5. Security services must have a communications plan that allows effective and continuous communications with appropriate security officials, to include the following:
   a. Facility Security (If applicable) (Contact frequency or telephone number)
   b. Police (Local phone number)
   c. Contract Security Dispatcher (Contact frequency or telephone number)
   d. CBP (Local phone number)
   e. Coast Guard (Local phone number)
   f. Agent (Local phone number)
   g. FBI (Local phone number)
   h. ICE (Local phone number)

   Consideration should be given to the need for language services to ensure that security personnel can properly communicate with the above officials and crew, especially high-risk crewmembers.
6. Valid crew must present proper documentation and must be cross-checked against the crew list provided by CBP. Only those crewmembers identified as being in D-1 or D-2 status are permitted to disembark the vessel. Questions related to whether a particular crewmember is allowed to disembark shall be forwarded to the ship's agent and, if necessary, CBP.
7. Non-crew, with proper identification, may board and leave the vessel. This may include vendors and service providers contracted to the ship (i.e., stevedores, agents).
8. Any attempt to disembark a vessel by persons not authorized to land (including stowaways) shall be reported immediately to local security services (facility guard posts, facility managers), CBP, USCG, ICE, FBI, local police department(s), and the vessel's agent.
9. If unauthorized individuals successfully disembark the vessel, contracted security services must immediately contact the agencies above, providing name, description, and circumstances surrounding the situation. If possible, contracted security services should coordinate with facility security personnel to locate and retrieve the absconding crewmember within the port facility.

ANNEX VI

Countries From 68 FR 2363, 16 January 2003

AFGHANISTAN
ALGERIA
BAHRAIN
BANGLADESH
EGYPT
ERITREA
INDONESIA
IRAN
IRAQ
JORDAN
KUWAIT
LEBANON
LIBYA
MOROCCO
NORTH KOREA
OMAN
PAKISTAN
QATAR
SAUDI ARABIA
SOMALIA
SUDAN
SYRIA
TUNISIA
UNITED ARAB EMIRATES
YEMEN

Total: 25 countries

put in place to prevent such crewmembers from gaining illegal entry into the United States. Furthermore, intelligence about a particular vessel, crewmember, or other circumstances may warrant implementation of other procedures, enforcement measures, or requirements similar to those of the SOP.

Annex I to the SOP is the minimum standards for contracted crewmember security services. Annex II to the SOP is the Standard Operating Procedures for Contracted Crewmember Security.

Annex VI of the SOP contains a list of countries from the Federal Register published at 68 FR 2363. Aliens from these countries have been determined to warrant additional monitoring in the interest of national security. Under the terms of the SOP, CBP will order the master to detain onboard any crewmember that is an alien from an Annex VI country—or that intelligence suggests is a risk to security—and that has not been permitted to land in the United States. The Coast Guard will provide the necessary enforcement authority to ensure that the vessel master, owner, agent, or operator has established effective security measures (Annexes I and II) to prevent high-risk crewmembers from absconding and damaging or threatening the port.

Local or regional plans and procedures implementing the SOP are acceptable as agreed upon in writing by local Captains of the Port (COTPs), CBP Port Directors, and CBP Border Patrol Chief Patrol Agents where assigned. COTPs, Port Directors, and Chief Patrol Agents retain discretion to modify security measures and plans as the situation dictates and may consider alternatives offered by the vessel's master or owner/operator that would provide an equivalent level of security to ensure that high-risk crewmembers are detained onboard. It is expected that security plans will not conflict with applicable laws or regulations.

In certain circumstances the terms of the SOP and requirements for contracted crew security may be extended to vessels with crewmembers who are not nationals of the countries identified by the SOP. These cases usually involve vessel owner/operators who have had significant patterns of absconders from their vessels.

Deserters

Coast Guard policy is that the vessel must report a desertion and update its notice of arrival information to reflect the changed crew. By regulation, 8 C.F.R. § 251.2, the vessel is also required to report deserters to CBP.

Deserters are crewmembers who have a valid visa and are permitted to land in the United States but fail to return to their vessel and depart as required. These crewmembers have gone through a pre-screening process that each crewmember must undergo prior to being permitted to land in the United States. Each crewmember must obtain a travel document such as a passport from his or her country and a visa from the Department of State. Each crewmember's name is compared against numerous criminal databases from the notice of arrival information provided to both CBP and the Coast Guard. Finally, each crewmember must undergo inspection by a CBP officer upon arrival and must be given specific authorization to land. CBP considers the vessel's history—with particular regard to deserters and absconders—in determining if a crewmember is permitted to land. CBP will only permit the crewmember to land if it determines that, in the unlikely event that he deserts, he will still not pose a security risk to the United States.

With regard to crewmembers that CBP has permitted to land in the United States, the Coast Guard generally takes no action. CBP has determined that these crewmembers pose an acceptable risk to the United States and, therefore, permit the crewmembers to land. If the vessel or its owner/operator has a recent history or pattern of deserters, Coast Guard action is normally not warranted, aside from notifying CBP of the pattern. Because the previous deserters were permitted to land and because CBP determined that the crewmember under consideration likewise is permitted to land, the crewmember does not pose a security risk to the United States.

Nevertheless, a significant pattern of desertion does elevate the security risk posed by the vessel, and Coast Guard policy recognizes this by allowing COTPs to require crew security plans for a 12-month period as with elevated risk absconders. A local Coast Guard commander may impose additional requirements in consultation with CBP if, after analyzing the facts and circumstances of a particular case, additional measures are determined to be necessary to ensure the security of the United States or to secure the rights and obligations of the United States.

About the author: *LCDR Mike Cunningham is a legal advisor with the Coast Guard Inspections and Compliance Directorate.*

The Evolution of TWIC

Coast Guard and TSA have teamed up to implement a common biometric identification card for use in the maritime industry.

by LCDR Jonathan Maiorine
Chief, Standards Branch, U.S. Coast Guard Office of Port and Facility Activities

In response to the Maritime Transportation Security Act (MTSA) of 2002, the Coast Guard has teamed up with the Transportation Security Administration (TSA) to work toward achieving one of the United States' most challenging security goals: develop, test, and implement a biometric transportation security card for an estimated one million U. S. maritime transportation workers, including all credentialed merchant mariners. While the requirement to issue a uniform identification credential for use across the entire maritime industry represented a significant task, the MTSA mandate to incorporate a biometric was immediately recognized as one of the most demanding aspects of the project for the Coast Guard.

Fortunately, when the Coast Guard joined the project in November 2004, TSA was actively engaged in researching and developing a Transportation Worker Identification Credential (TWIC) in response to the MTSA and the Aviation Transportation Security Act of 2001 (ATSA). The ATSA is aimed at strengthening airport access control points through the implementation of a secure credential. While the ATSA does not require the use of biometrics, language in the act does mandate that the use of biometrics be considered as a means of identifying airport employees.

TSA had already completed a technology review and had begun testing a biometric prototype TWIC when the Coast Guard offered to serve as a subject matter expert in implementing the TWIC first in the maritime mode. The ATSA required consideration of the use of biometrics in the airline industry, and the MTSA mandated the use of biometrics in the maritime mode. Therefore, teaming up Coast Guard and TSA in a joint rule-making project to implement a common biometric identification card in the maritime mode was a move in the right direction. It was also in step with Department of Homeland Security (DHS) policy advocating sharing of resources, technology, and information between agencies to enhance homeland security.

The Biometrics Challenge

On its Website, TSA defines biometrics as "automated methods of recognizing a person based on physiological or behavioral characteristics that are unique to an individual." Many people are familiar with the use of deoxyribonucleic acid (DNA) and fingerprints in law enforcement and forensic activities, but they may not realize that both fall into the broad category that is biometrics. While television and movies might project that the use of biometrics is common and fully established, in actuality, its use as a means of personal identity verification remains somewhat of an emerging industry.

Directed for use by such a large segment of the population, the TWIC will be the first of its kind in the United States. To establish a simple means by which a port worker can reliably identify himself or herself involves the use of a complex system. Such a system, however, will benefit national security, facility owners, and port employees by limiting unescorted access to secure areas and sensitive infrastructure to those individuals with a legitimate need and who also pass a security threat assessment.

Scope

Preliminary estimates indicate approximately one million workers will be enrolled in the TWIC maritime program. The MTSA-regulated industry, consisting of 3,500 facilities, 10,000 vessels, and 60 outer-continental shelf platforms, will be required to implement systems and policies to support the card and have their security plan updates approved by the Coast Guard.

The TWIC population, with regard to who is required to hold the credential, is mandated by the law itself, and this somewhat tangible data served as a cornerstone during the development of enrollment, card

Sample Transportation Worker Identification Credential (TWIC), front and back.

issuance, and data management plans. The development of the facility, vessel, and platform operational regulations, however, poses a unique challenge due to the broad range of operations, geographic locations, and varying numbers of workers requiring unescorted access to secure areas.

The law clearly mandated that a biometric card will be issued. Developing the "how to use it" regulations is the tough part. Impacted vessels vary from 30-foot passenger sport fishing boats to 800-foot cargo ships, and facilities range from small riverfront fueling docks to multi-acre container terminals, refineries, and chemical plants. The challenge is to propose useful and workable regulations and an implementation schedule to support the TWIC's enhanced security capabilities without overburdening industry. Currently, TWIC regulatory development teams are exploring the different card authentication tools available to provide maximum flexibility for regulated entities.

Impact

What are the security problems currently faced by the various modes of the U.S. transportation system and supply chain that TWIC aims to solve? According to Mr. John Schwartz, assistant director of maritime and surface credentialing (MSC) programs at TSA, these are: "the inability to positively identify individuals entering secure areas of the transportation system; the inability to assess the threat posed by individuals due to a lack of background information, or the lack of uniformly determined background information; and the inability to protect current credentials against fraud." He added, "the TWIC will positively tie the person to the credential, to the threat assessment."

In storing a transportation worker's physical biometric, fingerprints, the TWIC will enable a one to one match of the cardholder to the card itself with the assistance of an electronic reader. Through development and publishing of the standard to which readers must comply, TSA encouraged competition among private sector vendors and intends for customers to benefit from the use of off-the-shelf technology.

The issue of interoperability itself has challenged the biometrics industry as a whole. Due to the fact that manufacturers can use a unique and proprietary algorithm to convert fingerprint images to templates for storage within the TWIC, a card reader manufactured by a different company may not be able to read the information stored by another. According to an article by Mr. Thad Rueter of *Card Technology* magazine, "to overcome that hurdle, vendors have worked to develop interoperable templates, which are currently being tested by the National Institute of Standards and Technology."

The TWIC is designed to be more secure than many other forms of identification, in part due to the storage of encrypted information on a contactless chip. Other information, including the cardholder's name, photo, and biometric, will be stored within the card's integrated circuit chip. Another feature of the TWIC system is the ability to cross reference a TSA-managed database for expired or revoked cards and compare names to threat-intelligence databases or watch lists.

Understandably, privacy and collection of personal information concerns have been voiced by personal privacy advocates such as the Electronic Privacy Information Center (EPIC), who formally responded to TSA's public notification of intent to alter record systems in September 2004. According to EPIC, "TSA must take into consideration the privacy interests of those whose information is gathered, and take great care to guard this information from excessive use, misuse, or even use in furtherance of a terrorist act."

TSA maintains the TWIC program fully complies with all federal privacy laws and that all of the information stored within the card is encrypted for added security. In addition, no personal information outside of the holder's name and photo will be visibly displayed on the TWIC, unlike many driver's licenses and other forms of identification that display a social security number or home address.

Status

In April 2003 TSA initiated operational testing by conducting a six-month technology evaluation at 12 different transportation facilities, not all of them maritime. The evaluation successfully demonstrated TSA's ability to open and manage enrollment centers and to produce and issue cards and the TWIC's ability to support physical and logical access control. Most importantly, the evaluation period provided TSA the opportunity to evaluate the feasibility and reliability of existing card-based technologies in the field, including the integrated circuit chip, linear barcode, magnetic stripe, optical memory stripe, and the two-dimensional barcode.

The next phase of testing, protoype, was conducted from August 2004 to June 2005. These tests included use of the TWIC system at selected deepwater ports throughout the country. According to TSA, the prototype successfully tested advanced components of the TWIC, including its ability to manage a centralized and uniform card production system, physical access interfaces, and the operation of a centralized identity management infrastructure. While the actual number of cards used for access control was less than anticipated, the valuable lessons learned regarding the concept were incorporated in the planning stages for implementation.

After missing the initial target date for issuance in August 2004, Congress requested that the Government Accountability Office (GAO) conduct an audit of the TWIC program to identify the cause of the delay and to document future challenges facing timely implementation. In December 2004 the audit was complete and cited three main issues for the delay.

According to the report, the first reason for the delay was that TSA had difficulty in obtaining approval for the prototype test from the Department of Homeland Security. GAO did recognize that DHS was a newly formed agency at the time, with multiple legacy projects and urgent security responsibilities, especially in the aviation arena.

Second, TSA was tasked to work with DHS and Office of Management and Budget (OMB) officials to identify additional information needed for a second cost-benefit analysis and alternatives analysis. This required additional time, further delaying the prototype test.

The third reason cited by GAO for missing the August 2004 deadline was a congressional request to conduct additional tests of various card technologies, which resulted in another seven-month delay to the original testing schedule. Regarding the additional testing, GAO stated: "This analysis is typical of good program management and planning and, while it may have delayed the original schedule, the purpose of such assessments is to prevent delays in the future." The GAO report can be found in its entirety at www.gao.gov/new.items/d05106.pdf.

One Size Does Not Fit All

In developing the TWIC regulations, TSA has employed industry working groups, union representatives, other DHS offices, and internationally recognized standards organizations for assistance. The Coast Guard has also received valuable guidance and support from the National Maritime Security Advisory Committee's Credentialing Workgroup. Both agencies expect considerable feedback and recommendations from industry and labor organizations during the notice of proposed rulemaking comment period that will precede the regulations.

Impact on Merchant Mariners

Depending on their service, U.S. merchant mariners currently must carry a license (or Certificate of Registry, if a staff officer) or a merchant mariner's document (MMD) or both, and, if they sail beyond the boundary line, they must also carry a separate STCW Endorsement. These credentials are referred to generically as merchant mariner credentials (MMC).

As the MTSA requires all individuals holding an MMC to have a TWIC, regardless of a need to access secure areas, the Coast Guard's National Maritime Center has expressed concerns over adding yet another credential to the list of those already required for mariners. To address this issue, the Coast Guard is currently evaluating a draft proposal to combine all MMCs into a single form.

The current proposal would enable mariners to carry no more than two documents, with the TWIC serving as the identity document and the MMC, consisting of a combined license, MMD, and STCW endorsement, serving as the qualification document. Timing such a change to coincide with the TWIC roll-out would simplify the process for the more than 62,000 mariners who would benefit from this consolidation.

Conclusion

A significant contribution the Coast Guard brings to the project is the technical appreciation for the vast differences among the numerous MTSA-regulated facilities, vessels, and outer continental shelf platforms, which are not easily amenable to a uniform application of the TWIC. Also, because Coast Guard is responsible for the security plan approval process for all regulated vessels and facilities, it can assist with the integration of all TWIC requirements and components in the existing security plans. While the task is certainly not an easy one and the regulatory development process has taken much longer than expected, the final product will provide another tool to improve security at U.S. seaports, while enhancing commerce and protecting personal privacy.

About the author: *LCDR Jonathan Maiorine is currently serving as a TWIC project team member for the Coast Guard and is assigned as Chief, Standards Branch for the Coast Guard Office of Port and Facility Activities. He is also overseeing the current update to Title 33, Code of Federal Regulations Subchapter H, Maritime Security Regulations.*

Special thanks to LTJG Nanine Nyman for assisting with the drafting of this article. She is currently serving as both a member of the TWIC project team and biometrics subject mater expert for the Coast Guard's Office of Port and Facility Activities.

Port State Control Examination

Assuring compliance with ISPS and MTSA.

by LT Ryan Allain
Port State Control Specialist, U.S. Coast Guard Office of Vessel Activities

by LT Craig Toomey
Port State Control Specialist, U.S. Coast Guard Office of Vessel Activities

Congress mandated the original Port State Control program in the 1994 Department of Transportation Appropriations Bill. This bill required the Coast Guard to change its approach to foreign vessel examinations and hold those most responsible for substandard ships accountable, including owners, classification societies, and flag states.

Prior to September 11, 2001, the Coast Guard's Port State Control program was increasingly successful in reducing substandard shipping through the stringent enforcement of regulations pertaining to vessel safety and protection of the environment. After the terrorist attacks of 9/11, it became imperative for the Coast Guard to identify and mitigate threats in the maritime transportation infrastructure. The Coast Guard, in its traditional role as the lead federal agency for maritime transportation security, worked closely with the International Maritime Organization (IMO) to develop the International Ship and Port Facility Security (ISPS) Code.

The ISPS Code requires every vessel over 500 gross tons on international voyages, as well as facilities worldwide, to implement preventative measures to protect against security incidents. It also designates roles and responsibilities in the marine industry to ensure maritime security.

In addition to adopting the provisions contained in the

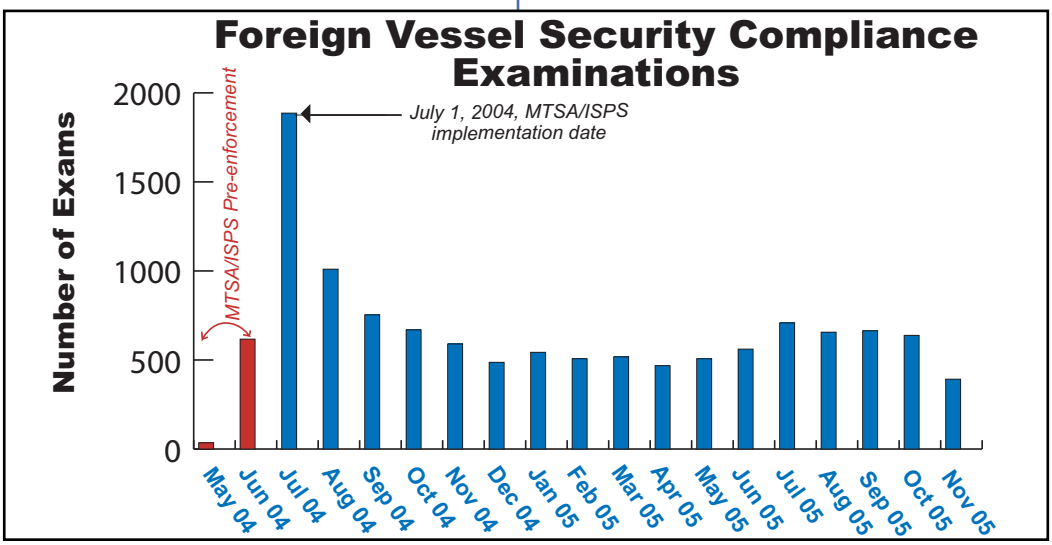


Figure 1: Foreign vessel security compliance examinations from May 2004 to November 2005.

ISPS Code, Congress passed the Maritime Transportation Security Act (MTSA) of 2002. MTSA requires commercial vessels over 300 gross tons on international voyages and U.S. facilities to conduct comprehensive security assessments, develop and implement security measures, and carry out operations in accordance with an approved security plan. MTSA applies to vessels, structures, and facilities located in, on, under, or adjacent to U.S. waters. The creation of MTSA and the ISPS Code required the Coast Guard's Port State Control program to expand significantly.

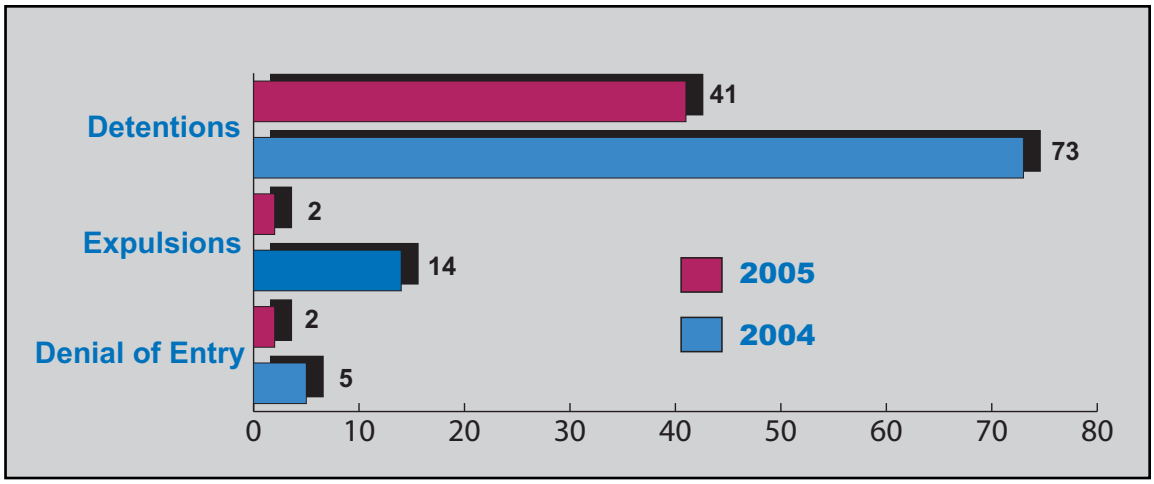


Figure 2: Foreign vessel major security control actions from 2004 and 2005.

The Coast Guard Port State Control program met this challenge by seamlessly integrating the enforcement elements of the new security standards with the traditional marine safety legacy missions of enforcing safety and environmental compliance standards. In the spring of 2004, the Coast Guard implemented an ISPS/MTSA pre-enforcement campaign that prepared the marine industry for complying with the new requirements before the July 1, 2004, deadline.

The pre-enforcement campaign also provided Coast Guard Port State Control officers with an opportunity to work in cooperation with industry to ensure their preparation. During the pre-enforcement campaign, inspectors verified the implementation of security programs onboard foreign vessels. If inspectors found a foreign vessel not yet in compliance with one or more aspects of the ISPS Code, the inspector issued deficiencies to the vessel, but did not impose a major control action. The inspector then entered this information into the Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database.

Since July 1, 2004, the enforcement of the ISPS Code and MTSA regulations have been integrated into the daily Port State Control activities throughout the Coast Guard (Figure 1). On a typical day, Coast Guard Port State Control teams carry out 25 ISPS security inspections.

The Targeting Matrix

The Port State Control program uses a risk-based tool, or matrix, to identify a foreign vessel for a security or safety examination. The matrix provides two benefits: First, targeting allows the Coast Guard to use its resources more effectively. Since more than 7,600 foreign vessels make over 60,000 U.S. port calls each year, the Coast Guard needs to use its resources wisely and focus inspections on foreign vessels with a history of poor performance. Vessels associated with a poorly performing flag state, owner, operator, or charterer or calling upon the United States from a country with poor ISPS compliance will likely get inspected. Using the matrix also benefits well-managed vessels. Those vessels receive less frequent examinations.

The targeting matrix, available on the Coast Guard Port State Control Website, www.uscg.mil/hq/g-m/pscweb/Publication.htm, provides the maritime industry with an incentive to maintain effective security and safety programs onboard their vessels. When the maritime shipping community does not implement effective security and safety programs, they risk delaying their vessels and incurring huge unexpected costs due to a Coast Guard imposed major control action.

The ISPS/MTSA Security Compliance Matrix contains five elements. Each element provides a score based on the risk factors due to ship management, flag state, the recognized security organization, security compliance history, and last ports of call. Once scores are determined for each of the five elements, the Coast Guard Captain of the Port adds them together to generate an overall total score for a particular vessel.

2004-2005 ISPS/MTSA Compliance

The Coast Guard attributes the successful implementation of the ISPS Code in the United States to the maritime industry's advance preparation and the

ISPS Code cite	Description of area of noncompliance	Number of enforcement actions taken	
		2004	2005
ISPS Code, Part A Section 7.2.2	Access Control	62	33
ISPS Code, Part A Section 7.2.4	Restricted Areas	48	20
ISPS Code, Part A Section 12.2	Ship Security Officer	37	9
ISPS Code, Part A Section 9.4	Ship Security Plan	21	10
ISPS Code, Part A Section 13	Training	13	5
ISPS Code, Part A Section 10.1	Logs/Records	11	5
ISPS Code, Part A, Section 7.2.7	Communications	7	2
ISPS Code, Part A Section 7.2.2	Screening Process	6	0
ISPS Code, Part A	Other (ISPS/Security Related Deficiencies)	6	2
ISPS Code, Part A Section 13.3	Shipboard Personnel	5	1
ISPS Code, Part A Section 13.4	Drills	3	3
ISPS Code, Part A Section 5	Declaration of Security	2	0
ISPS Code, Part A Section 9.4.12	Reporting Security Incidents	2	0
SOLAS, Chapter XI-1 Regulation 5	Continuous Synopsis Record	1	0
ISPS Code, Part A Section 9.4.4	Response Procedures	1	0
ISPS Code, Part A Section 9.4.6	Evacuation Procedures	1	0
ISPS Code, Part A Section 7.1	Vessel Security Level	1	1
TOTAL		**227**	**91**

Table 1: Leading causes of vessel detentions in 2004 and 2005, due to ISPS noncompliance.

Coast Guard's pre-enforcement campaign. After the ISPS Code took effect in July 2004, major control actions, detentions, and expulsions by the Coast Guard were much lower than expected (Figure 2). By the end of 2004, the overall percentage of major control actions was 1.5 percent. The current data from January to November 2005 show that this trend will continue and that this percentage will drop even lower. The Coast Guard will publish final results for 2005 in the Port State Control Annual Report, available in early 2006 on the Port State Control Website at www.uscg.mil/hq/g-m/pscweb/Publication.htm.

Major Control Action of Vessels

The two most commonly found ISPS deficiencies leading to vessel detention include a vessel's failure to meet restricted area requirements and maintain access control measures at the vessel point of embarkation (Table 1). In many of these cases, Coast Guard personnel walked freely into ISPS-designated restricted areas without crewmember escort or challenge.

The Coast Guard also identified crew and vessel security officer training shortfalls as another leading cause of vessel detentions. In most cases, vessel operators changed out personnel or quickly conducted emergency ship security officer (SSO) training sessions to meet the minimum levels required.

Wide ranging ship security plan (SSP) non-conformities also lead to many detentions. Some of the most common problems included missing required recognized security organization audits, improper safeguarding of the SSP, mismatches between SSP details and actual shipboard procedures, and inadequate procedures to handle security incidents.

Conclusion

The international maritime community, including the shipping industry and port facility stakeholders, should be congratulated for successfully taking on the huge challenge of implementing the security measures required by the ISPS Code and MTSA. Not only was the rate of compliance much higher than expected during the first few months of implementation, but all trends indicate increasing compliance rates. Ship operators who use the plan will protect the U.S. maritime infrastructure from terrorist attacks and other illegal activity.

About the authors: *LT Ryan Allain and LT Craig Toomey are both Port State Control Specialists in the Office of Vessel Activities, Foreign & Offshore Vessels Division, at U.S. Coast Guard Headquarters. LT Allain has served in the marine safety program for over seven years and was most recently stationed at Marine Safety Detachment Fort Myers, Fla., for three years, where he served as the supervisor. LT Toomey served on the CG Cutter* Spencer *for two years as a Deck Watch Officer and Assistant Navigator and has served in staff positions in Human Resources, Information Technology, and Marine Safety at Coast Guard Headquarters. LT Toomey was most recently activated from the Reserves under Title 10 to work with the Maritime Transportation Security Act Implementation Team.*

The Coast Guard welcomes comments on its programs. We frequently meet with vessel operators, flag state representatives, and classification societies to discuss matters of safety and security. We welcome your comments or would be happy to meet with you.

Please contact us at this email address:

fldr-G-MOC@comdt.uscg.mil.

Increased Port Security

Burden or benefit to port operations?

by Mr. Chris Austen
Chief Executive Officer, Maritime & Underwater Security Consultants (MUSC)

The International Ship and Port Facility Security (ISPS) Code, which was designed to reduce the threat of terrorist infiltration into foreign ports and, thus, into the United States by ship, has become weakened by indifference and complacency on the part of many governments and port authorities overseas. The ISPS Code was introduced by the International Maritime Organization (IMO) in response to the perceived threats to ships and port facilities in the wake of the September 11, 2001, attacks in the United States (Figure 1).

In testimony before the U.S. Congress in February 2004, RADM Larry Hereth, then-U.S. Coast Guard Director of Port Security, said, "Full deployment of the ISPS Code will greatly enhance the Coast Guard's port security posture by identifying and correcting weaknesses overseas, thus increasing our ability to prevent potential threats from reaching U.S. shores."

According to the latest IMO statistics, "almost 94 percent of the Contracting Governments to the SOLAS [Safety of Life at Sea] Convention have approved security plans for 97 percent of the declared port facilities, which in total number is excess of 9,600 worldwide." These assets had to be compliant with the ISPS provisions by July 1, 2004.

However, while many ports and terminals have gone through the paper process of implementing the code, many are not much more secure today than they were prior to July 1, 2004. This view is supported by discussions with cargo insurance underwriters, who see no signs of reduction in claims for cargo theft since the implementation date. The concern is that, if port cargo thefts have not decreased, how secure have ports and facilities become against infiltration of terrorists?

The apparent contradiction between the success of port and facility compliance and continued cargo thefts must be addressed and corrected. Identification of the problem and its solution lies with governments and port authorities who must make greater effort to understand the reasons for the code and the benefits to be reaped from its effective implementation.

Many ports are driven to address security matters not because of any directly perceived threat, but solely to comply with legislation. Security is seen as an unwelcome obstacle to the operation of the port, and improvements in security and efficiency are frequently seen as being incompatible.

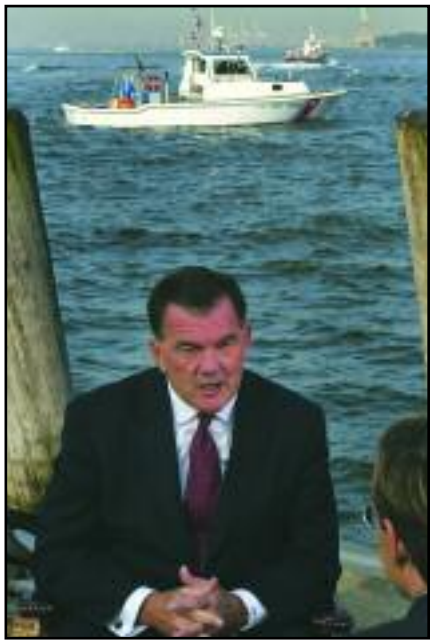


Figure 1: Mr. Tom Ridge, then-Secretary of the Department of Homeland Security, explains the implementation of the Maritime Transportation Security Act (MTSA) and Inter-national Ship and Port Facility Security (ISPS) Code. PA3 Mike Hvozda, USCG.

In the intensely competitive field of port operations, a commercial operator is reluctant to take on burdensome extra security costs if he sees his competitors somehow avoiding them. Concern about a potential terrorist attack is not high on the list of a port authority's priorities. It is not part of the daily grind and, therefore, not considered to be a net contributor.

In many cases, ports, and the terminal facilities within that port, are given no or minimal budgets for security. Such lack of investment can lead to poor security assessments and a consequentially weak and

meaningless security plan. The result too often is that the security investment has been largely squandered on an inefficient and ineffective security system, which may appear to offer superficial improvements but, in fact, presents scant deterrence to even petty thieves, let alone determined terrorists. Thereafter, the security effort becomes stalled, acts as a disincentive to staff, and often is seen as disjointed in its implementation in such areas as the installation of fencing, scanners, closed circuit television (CCTV) cameras, and access card readers. This negative attitude to security is usually manifest at management level, and, without support from managers, any initiative to improve security is almost certainly doomed to fail.

There are many benefits to commercial operators of a holistic approach to security. Ports and terminals that have efficient and effective security tend to show operational improvements in their businesses and higher degrees of motivation among their workforce. Good security can lead to spin-offs, such as better monitoring of workforce utilization; improvement in interagency cooperation, rationalization and sometimes reduction of guard force requirements; and reduction of losses through theft, smuggling, and human trafficking.

Critical Port Security Factors

To achieve an effective and sustainable security regime, some critical factors must be addressed. These include:

- **Strong governmental leadership:** Central and local governments must provide clear direction to ports and terminal operators to develop effective security. Governments must set standards for enforcement agencies, public bodies, and private companies. They should provide guidance and advice and have trained resources to monitor and enforce compliance.

- **Interagency cooperation:** A significant obstacle to effective security in ports is rivalry and reluctance to cooperate among agencies, such as police, customs, coast guard, and navy. Robust leadership from the heads of these organizations is needed to align the objectives of the various departments, to share information, and to agree on roles, boundaries, and interfaces.

- **Support from port or terminal managers:** Lack of commitment from senior management will have a direct effect on the performance of security officers, guards, and port workers. The attitude of senior management can be gauged by the behavior of the guards at the gate. Management is unlikely to be enthusiastic about supporting a system that it perceives as a waste of money, likely to slow down throughput, and affecting the port's competitive position.

- **Involvement of all port personnel in the security program:** Increasing the security awareness of port workers is perhaps the most cost-effective way of improving security. Through briefings and training, workers in the port collectively can act as the eyes and ears of the port security system. They detect, deter, and disrupt crime. An alert and watchful workforce will do much to persuade terrorists and criminals to look for an easier target. This workforce will look to their managers for support and encouragement.

- **Funding for security planning and implementation:** The problem of funding can be a difficult one to overcome. In the first instance, support from governments or, for developing countries, from donor organizations may be necessary to initiate the security process. As a side note, beware of the new breed of port security "expert" that has emerged after 9/11; many of these experts have had no previous experience in the subject. It is discouraging when ports are ill-advised and spend scarce resources on inappropriate and expensive equipment, usually with little or no improvement in security.

- **Business plan:** A business plan should be developed to allow the cost of security to be carried without degrading the competitive position of the port. Installing a security system is the first step. After that, the system should be refined, updated, and maintained. All this costs money and can have an effect on the operation of the entire port. The security planning process must take into account the long term funding for the security system.

In most cases these factors can be addressed most effectively on a whole port basis, rather than the piecemeal, facility-specific basis that many countries and ports have adopted.

The Port of Nigeria

While many ports have taken a superficial and ineffective approach to port security, there are some

instances where diligence and commitment to the planning and implementation of security are starting to show real benefits to port operations. One example of this is Nigeria.

The ports and coastal belt of West Africa suffer high rates of crime against ships. Illegal boarding, theft, extortion, kidnap of crews, and hijacking occur regularly. Criminal gangs operate in ports, and intercommunity fighting occasionally disrupts port operations. Problems are exacerbated by dilapidated port infrastructure, unreliable power supplies, and intermittent land and mobile communications. The challenge facing Nigeria to meet the requirements of the ISPS Code has been enormous. Nonetheless, the country has adopted a thoughtful and structured approach to meet the demands of the code that many other countries would do well to emulate.

Nigeria is one of the world's major exporters of oil. Ninety-five percent of the country's revenues are from oil exports, and the United States and Europe are its biggest customers. A security incident involving a tanker coming from Nigeria risks the shutdown of exports and massive damage to the economy. Nigeria, thus, is motivated to see real improvements in security in its ports and territorial seas.

About two years ago, Nigerian President Olusegun Obasanjo created the Presidential Implementation Committee on Maritime Safety and Security to improve security. The members are from various government ministries, the armed forces and enforcement authorities, representatives of the maritime industry, and port workers. A maritime security consultant was engaged as an adviser to the government on national maritime security strategy, training, and organizational development; national security planning; and the design and implementation of an integrated, nationwide maritime domain security program.

The program is an ambitious one: A national command, communications, and control system will be developed, providing real-time monitoring of activities in terminals at both regional control centers and at the maritime security authority's headquarters in Lagos. A system of radar stations and vessel tracking sensors will provide continuous tracking of SOLAS and non-SOLAS vessels in Nigeria's national waters. A national smart card identification (ID) system for seafarers and other port workers is being implemented.

The security surveys of the various ports have produced valuable information for the maritime authorities. Through data collected, programs have been initiated for rearrangement of services and removal of redundant and scrap equipment. The primary motivator for this activity has been to improve security, but the other benefits include more efficient port layouts, quicker cargo throughput, and the freeing up of wasted space for potential rental and additional income to the port.

Increased dialogue among agencies, workers' representatives, and employers is helping to improve relationships between agencies, between government and industry, and between employers and workers' organizations. By introducing better communications and control at regional and national levels, additional layers of supervision of the activities of government officials will help to inhibit and reduce the endemic problems of corruption in the ports. This will increase revenues to the government and improve the attractiveness of Nigerian ports to the shipping industry.

The maritime domain awareness system will help improve the government's effectiveness at collecting dues and other fees from ship operators, assist in enforcing the country's cabotage law, and, most importantly, monitor the activities of suspicious craft and stamp out hijacking, hostage-taking, and theft at sea.

Much work has been carried out to identify and appreciate the problems. Under the leadership of the Minister of Transport, Dr. Abiye Sekibo, there is a solid determination in government to instigate change and improvement. Much remains to be done, but the foundations are being set.

The Port of Venice

In Europe, the port of Venice (Figure 2) offers another example where a structured approach to security is enhancing the port's overall operations. Venice is the home of one of the world's busiest cruise line terminals, handling over one million passengers per year. Close by is the industrial port of Maghera, the second largest in Italy with over 30 terminals handling oil products, hazardous chemicals, containers, and bulk products. There is fierce competition between Venice and other ports in the Mediterranean, and, following the introduction of the ISPS Code, terminal operators in the port were concerned at the impact that the burden of additional costs for security would have on their business.

Although not legislated within the ISPS Code, the port authority recognized that the most effective way of introducing security to the port would be through a coordinated and integrated approach across the

Figure 2: The Port of Venice.

whole port. A security assessment of the entire port was carried out, along with those for each facility. From this, a strategy was developed based on an integrated security control center that would provide CCTV surveillance, perimeter and access control, and ID card management for all the terminal operators. The plan involves the construction of a new 12-lane entry point into the port with automated barriers, search and waiting areas, and facilities for container scanning and other forms of non-intrusive inspection. At the same time outdated roads are being upgraded and a new port access bridge is being built.

The new security system, operated and maintained under the control of the port, will allow the terminal operators to concentrate on their core businesses. Apart from better security, terminal operators will gain from better truck turnaround times and quicker cargo processing. By integrating port and terminal security operations, savings of over 30 percent in guard manning costs will be likely. Other benefits include better supervision of workforce timekeeping and improved management of movements of trucks and containers within the terminals. From a safety perspective, the system will provide the port with a real-time picture of the location of persons and vehicles within the port. This will allow more effective response to emergencies and better management of evacuation.

The port is now able to extend its value-added services to terminal operators and, thus, increase its revenues. By centralized purchasing and installation of security equipment, the port authority and the terminal operators can take advantage of economies of scale, thus optimizing procurement and maintenance budgets.

Raising standards of security in ports can have a significant cost, both in the initial capital spent and in ongoing operation and maintenance. However, by careful and structured discussions with the various stakeholders in the port and its terminals, those involved in enhancing security can also bring better safety, improved administration, and improved operational efficiency, while at the same time reducing cargo theft and the risk of terrorist intervention.

About the author: *Mr. Chris Austen, chief executive officer of Maritime & Underwater Security Consultants (MUSC), based in London, England, has worked on a variety of counter-terrorism, anti-piracy and crime prevention operations in Europe, Nigeria, Angola, Algeria, Indonesia, Malaysia, and Central America. He provided input to the International Maritime Organization for the development of the ISPS Code and to the World Customs Organization for supply chain security.*

National Maritime Security Advisory Council

NMSAC is the primary and lead advisory committee for maritime security.

by Mr. John Bastek
Executive Secretary, NMSAC

The National Maritime Security Advisory Committee (NMSAC) is the newest advisory group for the Coast Guard. The Maritime Transportation Security Act (MTSA) of 2002 established NMSAC in Section 70112. The committee was formed to advise the Secretary of Homeland Security through the Commandant of the Coast Guard on matters relating to national maritime security. Members were chosen based on their affiliation to a specific sector within the maritime industry or a recognized maritime association, in order to represent the interests of a wide segment of the maritime population (Figure 1). Each member is required to have at least five years of experience in maritime security operations, and all of the members are vetted and approved by the Secretary of Homeland Security.

Congress made the NMSAC subject to the Federal Advisory Committee Act (FACA), which requires an annual report, among other things. General information on FACA committees can be found on the FACA Website at http://www.gsa.gov/.

Members and Committee Makeup

The members are from very diverse elements within the maritime community—port management, facilities, organized labor, vessel owners/operators, supply chain, and academia. A wide array of views is represented, which is the value of this group. They can discuss every facet of a situation from individual perspectives and, thereby, provide quality advice to the Department of Homeland Security or to the Coast Guard.

Each member can also solicit input from others within their specific maritime industry segment or element or recommend others to participate on NMSAC workgroups. This capability ensures, again, that advice and recommendations provided by NMSAC are built upon the foundation of broad maritime industry expertise.

The original 20 members selected to the NMSAC are:

Christopher L. Koch	President & CEO, World Shipping Council (NMSAC Chairman)
Lisa B. Himber	Vice President, Maritime Exchange for the Delaware River and Bay (NMSAC Vice Chair)
Joseph H. Langjahr	Vice President & General Counsel, Foss Maritime Company
Thomas E. Thompson	Executive Vice President, International Council of Cruise Lines
John C. Dragone	Vice President – Operating Division, Maritrans Operating Company L.P.
Mary Frances Culnane	Manager, Marine Engineering, San Francisco Bay Area Water Transit Authority
Basil Maher	President and Chief Operating Officer, Maher Terminals
Charles Raymond	Chairman, President, and CEO, Horizon Lines
Alice K. Johnson	Senior Supervisor, PPG Industries, Inc.
Timothy J. Scott	Global Director, Emergency Services & Security - The Dow Chemical Company
Mark Witten	Sr. Regulatory Advisor, Gulf of Mexico Deepwater Business Unit, ChevronTexaco
Robert R. Merhige III	Retired Chief of the Port Police; Virginia Port Authority
Jeffery W. Monroe	Director of Ports and Transportation, Portland, Maine
Wade M. Battles	Managing Director - Port of Houston Authority
John Hyde	Director, Security & Compliance, Maersk Sealand Inc.
William Eglinton	Seafarers International Union of North America, AFL-CIO
James Stolpinski	President, Local 1233 ILA
David Halstead	Chief, Domestic Security Preparedness, FL Department of Law Enforcement
Theodore L. Mar	Chief, Marine Safety Branch - CA Dept of Fish and Game
Victor Zaloom	Director, Engineering Graduate Programs & Lamar University Center for Ports and Waterways

Figure 1: First row, from left: John Dragone, Maritrans; Jeffrey Monroe, Port of Portland (ME) Port Director; Basil Maher, Maher Terminals; Bill Eglinton, Seafarer's International Union; Victor Zaloom, Lamar University; Robert Merighe, Retired Chief of Police, Virginia Port Authority; CDR Tina Burke, USCG. Second row, from left: Mary Frances Culnane, San Francisco Water Taxi Authority; Mark Witten, Chevron/Texaco; Ted Mar, State of California; Chris Koch, World Shipping Council, Chair; Joseph Langjahr, Foss Maritime Company; James Stolpinski, International Longshoreman's Association; John Bastek, Executive Secretary. Third row, from left: Capt Frank Sturm, USCG; John Hyde, Maersk; Thomas E. Thompson, ICCL; David Halstead, State of Florida; Lisa Himber, Delaware Marine Exchange, Vice Chair.
(Not pictured: T.J. Scott, Dow Chemical; Alice Johnson, PPG Industries; Chuck Raymond, Horizon Lines; and Wade Battles, Port of Houston.) YN1 Birchfield, USCG.

The Designated Federal Official and Executive Director for the NMSAC is CAPT Frank Sturm, the Chief of Port and Vessel Security at U.S. Coast Guard Headquarters. Capt Sturm himself has much maritime experience with which to provide guidance and assistance to the committee.

NMSAC Purpose and Charter

NMSAC is chartered "to advise, consult with, and make recommendations to the Secretary of the Department in which the Coast Guard is operating, via the Commandant of the Coast Guard, on matters affecting maritime security, including, but not limited to:

- developing a national strategy and policy to provide for efficient, coordinated and effective action to deter and minimize damage from maritime-related transportation security incidents;
- recommending actions required to meet current and future security threats to ports, vessels, facilities, waterways, and their associated inter-modal transportation connections and critical infrastructure;
- promoting international cooperation and multilateral solutions to maritime security issues;
- addressing security issues and concerns brought to the committee by segments of the maritime transportation industry, or other port and waterway stakeholders; and,
- such other matters, related to those above, that the Secretary may charge the committee with addressing."

Relation to Other Advisory Committees

NMSAC, however, is only one of many federal advisory committees with an interest or charter dealing with homeland security issues. Thus, as a new federal advisory committee, it is important to identify the role of NMSAC in relation to these other existing advisory committees.

Figure 2 is a visual representation of some of these relationships. NMSAC is the primary and lead advisory committee for maritime security. The figure, however, shows where the interests or roles and responsibilities of other federal advisory committees are concurrent with or intersect with those of NMSAC. A key activity, then, as the agenda for

NMSAC evolves, is to maintain awareness of the issues being undertaken in other venues and to coordinate NMSAC's work or interests with these other committees as appropriate.

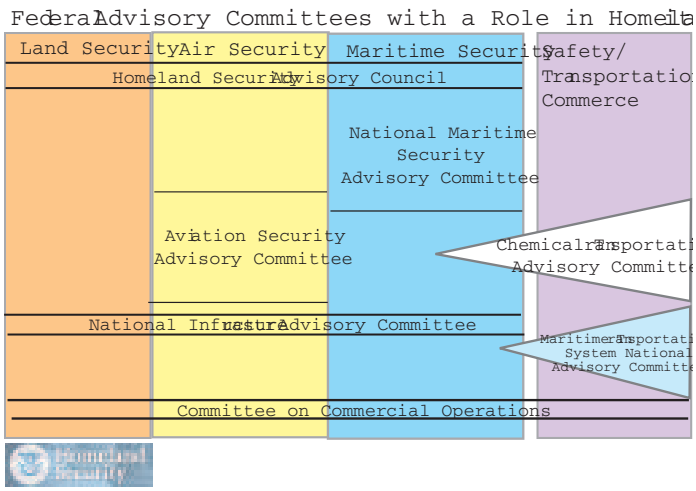


Figure 2: NMSAC's relationship with other federal advisory committees.

Summary of Meetings, Accomplishments, Current Activities

NMSAC met for the first time in March 2005, and the committee meets at least once a year by statute. At the inaugural meeting, the Commandant of the Coast Guard spoke to the NMSAC members about his vision for the committee, set high expectations with respect to how the committee could help in furthering the goal of national maritime security, and expressed his appreciation for each member's participation. RADM T.H. Gilmour, the Assistant Commandant for Marine Safety, Security, and Environmental Protection (now Assistant Commandant for Prevention), as well as RADM Larry Hereth, the Director of Port Security at that time, also participated in the inaugural meeting. They framed issues for consideration by the committee and helped set the work of the committee off on the right path. As a result of those initial discussions, five initial workgroups were conceived: the Communications, Consistency, Asymmetric Migration, Single Window (Data) Reporting, and Transportation Worker Identity Card (TWIC) workgroups.

Shortly following the inaugural meeting, the Transportation Security Administration and the Coast Guard asked the NMSAC TWIC workgroup to develop recommendations that would assist with the drafting of a notice of proposed rulemaking (NPRM) for the TWIC. The task statement requested that the workgroup address 13 different areas of concern regarding potential TWIC processes and impacts. Given approximately one month to complete this complex task, the TWIC workgroup quickly commenced work and, after numerous conference calls and document exchanges, presented their recommendations in May 2005. The workgroup received high praise for rapidly responding to this important task and providing comprehensive recommendations, which are proving extremely useful to the government regulation drafting team in understanding the industry's stance on the issues presented.

Most recently, at the November 1, 2005, session, the committee accepted a task from the Coast Guard to identify maritime private sector subject matter experts (SMEs) from all appropriate maritime business and industry sectors. These SMEs are needed to provide advice and consultation to the Coast Guard and other DHS agencies on national level maritime matters during transportation security incident (TSI) response or recovery operations. Communications between government and private sector is a key element in the realm of homeland security. Establishing communication mechanisms supports strategies and goals outlined in the Maritime Transportation Security Act of 2002, the National Strategy for Maritime Security, the National Response Plan, and several other guiding documents.

Engagement on Future Maritime Security Challenges

Despite the progress of the nation, the Department of Homeland Security, and the United States Coast Guard on matters of maritime homeland security, there is still much work to be done to continue thwarting the ever-present terrorist threat. The National Strategy for Maritime Security, signed in September 2005, and the eight supporting plans directed by Homeland Security Presidential Directive (HSPD)13 outline concepts and recommendations to bring collective efforts to the next level. Overall, the eight supporting plans together serve to enhance international cooperation while maximizing Maritime Domain Awareness. This will create necessary layers of security meant to stop or deter threats against the United States, as far from our shores as possible, while also assuring continuity of the maritime transportation system. NMSAC is expected to play an important role in providing private sector perspectives and advice to the government during implementation of these significant plans and strategies.

About the author: *Mr. John Bastek is currently the Executive Secretary of NMSAC for the Coast Guard. He has worked for the Coast Guard for two years as a civilian after a 30-year active duty career. He has also held positions on the International Council for Cruise Lines, in the Maritime Group for Preston Gates LLP, and as a private consultant. He is a graduate of the Coast Guard Academy, the University of Miami School of Law, and the Industrial College of the Armed Forces.*

Airborne Use of Force

Arming Coast Guard aviation.

by LCDR Melissa Rivera
Special Missions Program Manager
U.S. Coast Guard Office of Aviation Forces, Office of Counterterrorism and Special Missions

by CDR Aaron C. Davenport
Deputy Chief
U.S. Coast Guard Office of Counterterrorism and Special Missions

> *"Securing the American Homeland is a challenge of monumental scale and complexity. But the U.S. government has no more important mission."*
>
> - President George W. Bush, in the National Strategy for Homeland Security

> *"The Coast Guard will adjust to that change and be ready to do what is necessary to ensure that maritime homeland safety and security are guaranteed."*
>
> - ADM Thomas Collins, Commandant of the U. S. Coast Guard

The U.S. Coast Guard transferred from the Department of Transportation into the newly created Department of Homeland Security in March 2003. For a service that traditionally considered search and rescue as one of its primary missions, this move was more than the physical shifting of departments. It required a shift of many age-old paradigms about Coast Guard missions, as well as the way the service conducts its day-to-day business.

Figure 1: A Coast Guard gunner sights in on a target from a Coast Guard helicopter.

Maritime Strategy for Homeland Security

To prepare for this move, the Coast Guard released the Maritime Strategy for Homeland Security in December 2002. In this document, the Coast Guard provided its maritime homeland security (MHS) mission statement:

"Protect the U.S. Maritime Domain and the U.S. Marine Transportation System and deny their use and exploitation by terrorists as a means for attacks on U.S. territory, population, and critical infrastructure. Prepare for and, in the event of attack, conduct emergency response operations. When directed, as the supported or supporting commander, conduct military homeland defense operations."

In support of this mission, the service's strategic objectives in maritime homeland security are:

- Prevent terrorist attacks within, and terrorist exploitation of, the U.S. Maritime Domain.
- Reduce U.S. vulnerability to terrorism within the U.S. Maritime Domain.
- Protect U.S. population centers, critical infrastructure, maritime borders, ports, coastal approaches, and the boundaries and seams among them.
- Protect the U.S. Marine Transportation System while preserving the freedom of the U.S. Maritime Domain for legitimate pursuits.
- Minimize the damage and recover from

attacks that may occur within the U.S. Maritime Domain as either the lead federal agency or a supporting agency.

Airborne Use of Force

With the creation of the Helicopter Interdiction Tactical Squadron (HITRON) in 1999, the main focus of the Coast Guard's Airborne Use of Force (AUF) from helicopters was on counter drug operations. After September 11, 2001, a Coast Guard workgroup was formed to research expanding AUF capability for application in maritime homeland security missions. This workgroup was comprised of key personnel from across the service; the group explored multiple AUF concepts and evaluated the rotary-wing fleet size needed to execute new mission sets.

As a follow-on, Aviation Training Center Mobile, Ala., established itself as the Coast Guard's AUF Center of Excellence. Within this command, the Aviation Special Missions Branch was created to provide training and standardization support to AUF initiatives, including:

- aerial tactics;
- vertical insertion (fast roping);
- rotary wing air intercept;
- joint surface/air tactics;
- CBRNE (chemical, biological, radiological, nuclear explosive) operations; and
- aerial gunnery.

Arming Coast Guard helicopters is critical to meeting the Department of Homeland Security's missions (Figure 1). Coast Guard armed helicopters have been used to meet maritime security requirements, including interdicting drugs, performing maritime security patrols, and protecting the public in U.S. ports and waterways during national special security events. These events have included the Group of Eight (G8)

Figure 2: A Coast Guard aviation gunner provides aerial security during a boarding exercise.

summit in Georgia, the national political party conventions in Boston and New York City, and President Reagan's funeral in California. Armed helicopters operating from the decks of Coast Guard cutters have interdicted record amounts of illegal drugs in the Caribbean and Eastern Pacific. Eight Agusta Bell MH-68s provide the majority of this capability, basing from HITRON in Jacksonville, Fla. However, due to this small number of armed helicopters, many airborne homeland security missions are currently being conducted by unarmed aircraft.

The Coast Guard intends to equip all of its HH-65C and HH-60J helicopters—a total of 137 aircraft—with the ability to be armed, providing weapons as funding permits. This will give the Coast Guard the ability to respond quickly to emerging security threats wherever it operates. These armed helicopters will also continue to conduct all Coast Guard missions they currently perform (Figure 2).

Capability

Coast Guard aviation continues to adapt to the maritime homeland security mission. All air stations and aircraft type are supporting this mission with patrols offshore, in the ports and waterways across the nation. In addition, tremendous efforts are being made to determine how to provide a more robust aviation capability in the new department. One such program is the armed helicopter proof of concept.

In fall 2003 and spring 2004, the Coast Guard began an HH-60J airborne use of force proof of concept at Air Station Cape Cod, Mass. The primary purpose of the proof of concept was to measure operational effectiveness, compared with the impact of fielding a maritime homeland security AUF capability at an established Coast Guard air station, in terms of manpower, training, and other resource costs. Based on feedback and lessons learned during this project, the Coast Guard intends to use the model developed in Cape Cod to spread AUF capability within its helicopter fleet.

In 2005, the Coast Guard modified all of the HH-60J Jayhawk helicopters at Air Station San Diego for the AUF mission. This aircraft equipment includes:

- mounted M240 area fire weapons;
- shoulder-mounted backup M14 weapons;
- aircraft hardening (armor);
- pilot head-up display (HUD);
- upgraded forward-looking infrared/electro-optical (FLIR/EO) equipment;
- an upgraded radio to allow for better communications with local agencies; and
- body armor for aircrews.

Beginning this year, a core group of pilots and gunners at San Diego will be trained in day and night tactics and aerial gunnery.

Key to AUF capability is interoperability with the Coast Guard's tactical, maritime homeland security, and traditional law enforcement forces. Through research and the AUF proof of concept, the preliminary estimated costs of developing this capability have been learned. With time, the cost of various types of AUF capabilities and the scalability will be more accurately determined.

In July 2005, the Coast Guard established the Office of Homeland Security Operations & Tactics, with responsibility for tactical policy and requirements. This new office will combine the efforts of the diverse aspects of the Coast Guard's MHS package. Research, testing, and tactics development are well underway in the arenas of aircrew chemical, biological, and radiological equipment; rotary wing air intercept; and airborne designated marksman capability.

While striving to serve the American public in the maritime homeland security mission, Coast Guard aviation continues to examine and expand its capabilities to meet the service's strategic objectives.

About the authors: *LCDR Melissa Rivera is a 1991 graduate of the U.S. Coast Guard Academy and an HH-60J Instructor Pilot/Flight Examiner with more than 10 years of flight experience. Currently, she is a Coast Guard Airborne Use of Force/Aviation Special Missions Program Manager. LCDR Rivera is a recipient of aviation awards from the Fraternal Order of Daedalians, Association for Naval Aviation, Naval Helicopter Association and a heroism award from the Coast Guard Foundation.*

CDR Aaron C. Davenport is a 1984 graduate of the U.S. Coast Guard Academy and a 1995 graduate of the University of California at Los Angeles. He has served in Coast Guard boat force, afloat, and marine safety operational commands, and his staff assignments include Combatant Command Headquarters and Logistics Command Atlantic. CDR Davenport's most recent assignment was command of Coast Guard Cutter Valiant. *He has been selected for promotion to Captain and for the 2006 RAND Corporation Military Executive Fellowship.*

Safeguarding the United States

Enforcement of Coast Guard safety and security zones.

by LCDR Brad Kieserman
Chief, Operational Law Group, U.S. Coast Guard Office of Maritime & International Law

by LCDR Christopher F. Murray
Legal Advisor, U.S. Coast Guard Office of Law Enforcement, Headquarters

by LCDR Mike Cunningham
Legal Advisor, U.S. Coast Guard Inspections & Compliance Directorate

After the terrorist attacks of September 11, 2001, there was an immediate and overwhelming focus on domestic maritime security law enforcement operations. The Coast Guard received unprecedented numbers of requests to establish security zones at high-value assets, such as naval vessels and facilities, critical port infrastructure, and nuclear facilities, to name just a few. The need for such zones quickly outgrew the Coast Guard's law enforcement resources. To meet increased security requirements in U.S. ports, waterways, and coastal areas, with limited Coast Guard resources, many Coast Guard field commanders turned to state and local authorities for assistance in enforcing these security zones (Figure 1).

Law Enforcement

While it was clear that the Captain of the Port (COTP) could request other entities to assist in enforcing security zones, and that federal case law long recognized that states had the ability to confer arrest authority for federal criminal violations, many states had concerns as to whether or not their state law enforcement officers could enforce a federal safety or security zone. To resolve the problem, Congress inserted a provision in the Coast Guard and Maritime Transportation Act of 2004 (CGMTA)[1] to resolve these concerns. President George W. Bush signed CGMTA into law on August 9, 2004.

Figure 1: A Boston Police boat and a Coast Guard 25-footer secure Rowes Wharf during the 2004 Democratic National Convention. PA3 Mike Lutz, USCG.

Figure 2: A Coast Guard boat and a boat from the Alabama Marine Patrol work to maintain a Coast Guard safety zone. PA3 Jonathan McCool, USCG.

Section 801 of the CGMTA created a new § 70119[2] in title 46, United States Code. Section 70119 clarified authority for state law enforcement officers. Officers with state criminal arrest powers may make felony arrests for violations of most Coast Guard-established safety and security zones, employed for domestic port security operations.[3]

Before enactment of 46 U.S.C. § 70119, the Coast Guard contended that, consistent with well-settled law, state law enforcement officers are permitted to enforce federal statutes where such enforcement activities do not impair federal regulatory interests.[4] Many state agencies, however, desired congressional clarification of that view.

Statute 46 U.S.C. § 701109 reads as follows:

§ 70119. Enforcement by State and local officers

(a) In general.—Any State or local government law enforcement officer who has authority to enforce State criminal laws may make an arrest for violation of a security zone regulation prescribed under section 1 of title II of the Act of June 15, 1917 (chapter 30; 50 U.S.C. 191) or security or safety zone regulation under section 7(b) of the Ports and Waterways Safety Act (33 U.S.C. 1226(b)) or a safety zone regulation prescribed under section 10(d) of the Deepwater Port Act of 1974 (33 U.S.C. 1509(d)) by a Coast Guard official authorized by law to prescribe such regulations, if—

(1) such violation is a felony; and

(2) the officer has reasonable grounds to believe that the person to be arrested has committed or is committing such violation.

(b) Other powers not affected.—The provisions of this section are in addition to any power conferred by law to such officers. This section shall not be construed as a limitation of any power conferred by law to such officers, or any other officer of the United States or any State. This section does not grant to such officers any powers not authorized by the law of the State in which those officers are employed.

Statute 46 U.S.C. § 70119 does not create new authority for the Coast Guard, nor does it involve the exercise of Coast Guard law enforcement authority by state and local officers. Instead, § 70119 grants federal arrest power in limited circumstances to state or local government law enforcement officers who have authority to enforce state criminal laws, provided that the controlling state law does not preclude such officers from exercising federal arrest power. Accordingly, employment of state and local officers to enforce Coast Guard security and safety zones must be predicated on a review of the applicable state law providing law enforcement powers to the officers, with a view to ensuring that state law does not bar them from enforcing federal felony statutes.

Safety Zone Enforcement

Even in those states where state law enforcement officials are precluded from enforcing federal law, they still may be able to effectively enforce a security or safety zone (Figure 2 & 3). These state law enforcement officials, while without power to enforce federal law, would be exercising their state powers to enforce state law.

For this scenario to be applied practically, the behavior prohibited by the security or safety zone must also be prosecutable as a violation of state law, such as trespassing. This would be similar to the situation where Department of Defense officials have arrested individuals for trespass under 18 U.S.C. § 1382, whereby the waters included within a security zone were essentially treated as part of a Naval reservation for purposes of the trespass statute. Government ownership of the underlying water areas is not a requisite for enforcement.[5]

In situations where state law enforcement officials are precluded from enforcing federal law, the state law enforcement agency may assist by providing a platform from which Coast Guard boarding officers can engage in law enforcement activities.

Figure 3: A Coast Guard boat patrols Boston Harbor. PA3 Andrew Shinn, USCG.

In the absence of an express state law bar, therefore, appropriate state and local government law enforcement officers may make arrests for, and thereby enforce, felony and misdemeanor violations, including attempts, of Coast Guard safety and security zones. These include nearly all the zones typically employed in domestic port security.

Coast Guard/Law Enforcement Cooperation

Regardless of the form the assistance takes, whether it is direct enforcement of federal law, enforcement of an underlying state law, or providing assistance in the form of boarding platforms, the Coast Guard seeks to establish agreements, typically in the form of a memorandum of agreement (MOA). An MOA outlines how the Coast Guard and the state agencies will assist each other. These agreements, which are developed by the cognizant Coast Guard district commander, are thoroughly vetted by Coast Guard attorneys.

A memorandum of agreement ensures that lead agency and respective roles are clearly identified and that the MOA and its contemplated activities are authorized by law and in accordance with current Coast Guard and state policy. Additionally, these agreements tend to address potentially valuable assistance, including patrolling or monitoring of safety and security zones, informing others of the existence of the zone, and detecting and reporting targets of interest.

To date, the Coast Guard has signed memoranda of agreement on law enforcement assistance with a number of states, including Maine, New Jersey, Delaware, Pennsylvania, Maryland, Virginia, and Florida. A typical MOA is quite detailed and specifies to the greatest degree possible legal authorities, common definitions, and, perhaps most importantly, the roles and responsibilities of each agency. These agreements can also contain addendums to address local needs below the state level.

Coast Guard districts are continuing discussions with a number of other states, and Coast Guard hopes that more MOAs are signed. These agreements, along with the assistance provided by state and local law enforcement, have been a powerful force multiplier in helping to ensure U.S. port security.

Endnotes

1. Coast Guard and Maritime Transportation Act of 2004, Pub. L. No. 108-293, 118 Stat. 1028.
2. There is some question as to whether § 70119 is properly numbered. Until Title 46 is republished, the subject section's precise location will be unknown. This memorandum refers to the subject section as "§ 70119" or "section 70119," reflecting the language in the CGMTA.
3. The enumerated zones include "security zone regulation[s] under section 1 of title II of the Act of June 15, 1917 (chapter 30; 50 U.S.C. 191) or security or safety zone regulations under section 7(b) 24 of the Ports and Waterways Safety Act (33 U.S.C. 1226(b)) or [ ] safety zone regulation[s] prescribed under section 10(d) of the Deepwater Port Act of 1974 (33 U.S.C. 1509(d))." CGMTA, Section 801.
4. Ker v. California, 374 U.S. 23 (1963); Florida Avocado Growers, Inc. v. Paul, 373 U.S. 132 (1963); Op. Off. Legal Counsel, U.S. Department of Justice, Assistance by State and Local Police in Apprehending Illegal Aliens (Feb. 5, 1996).
5. See, for example, U.S. v. Allen, 924 F.2d 29 (2d Cir. 1991); U.S. v. De Jesus, 108 F.Supp.2d 68 (D. PR. 2000).

About the authors: *LCDR Brad Kieserman is Chief of the Operational Law Group, U.S. Coast Guard Office of Maritime and International Law.*

LCDR Christopher Murray is Legal Advisor, U.S. Coast Guard Office of Law Enforcement. He served previously as XO, Coast Guard Cutter Neah Bay. LCDR Murray is a 1995 graduate, with honors, of the U.S. Coast Guard Academy and a 2003 graduate, summa cum laude, of Ohio State University School of Law, where he was an articles editor of the OSU Law Review.

LCDR Mike Cunningham is the legal advisor to the Inspections & Compliance Directorate at Coast Guard Headquarters. Previous field assignments include MSO/Group Los Angeles-Long Beach and MSO Puget Sound. Previous legal assignments include the Office of Maritime & International Law, the Office of Legislation, and the Office of Legal Policy & Program Development.

Maritime Safety and Security Teams

A force for today.

by CDR Aaron C. Davenport
USCG Deputy Chief, Office of Counterterrorism and Special Missions

In September 2005, the National Strategy for Maritime Security (NSMS) was promulgated, pursuant to National Security Presidential Directive 41 and Homeland Security Presidential Directive 13. These directives state that forces must be trained; equipped; and prepared to detect, deter, interdict, and defeat terrorists throughout the maritime domain. The United States must build rapid-reaction forces (Figure 1) to support first responders with capabilities to respond to terrorist incidents that occur in the maritime domain.

Due to the unconventional nature of adversaries' tactics, the United States' traditional military and law enforcement capabilities are stretched thin and, in some scenarios, insufficient to counter a skilled and determined enemy, willing to sacrifice their lives for their cause. U.S. senior executive leadership has recognized that additional specialized law enforcement and counterterrorism capabilities need to be developed and ready for use at a moment's notice, to rapidly deter and counter any attack. Responses must be swift and effective, with highly controlled and deliberate action that limits collateral damage and instills public confidence.

Figure 1: A 25-foot Homeland Security response boat enforces a security zone for foreign naval vessels.

Forces capable of such response must be highly proficient in close-quarters engagement and the use of precision weapons and advanced tactics in law enforcement scenarios. This level of proficiency requires forces trained to a higher standard than has previously existed, outside of a small select group of special operators in the military and law enforcement communities.

Maritime Safety and Security Team

To answer the call, the U.S. Coast Guard has built the Maritime Safety and Security Team (MSST). The MSST is a prototype-integrated package that not only meets this emerging need by filling the gaps in advanced law enforcement and counterterrorism capability, but also enhances U.S. ability to more effectively execute traditional law enforcement and public safety missions. Maritime Safety and Security Teams are capable of providing safety and security operations in ports where they are assigned to operate and to deploy and respond to higher threat areas if necessary.

Twelve MSST units are currently in their initial operational capability and are not yet fully staffed to support all of their operational responsibilities. They are also not yet fully trained to a standard that allows them to safely conduct full-spectrum specialized skills such as close-quarter combat tactics. Working in their initial capacity, MSST units have further determined a need for additional capabilities to mitigate the risks in

continued on pg. 85

Port Security

A look from below the surface.

by Mr. Kenneth McDaniel
Homeland Security Program Analyst,
U.S. Coast Guard Office of Defense Operations

The Coast Guard's ongoing efforts to improve its presence, response, and recovery capabilities in the Ports, Waterways, Coastal Security (PWCS) mission area are generating new safeguards and additional layers of port security. The Coast Guard recently unveiled one of its newest tools in the ongoing efforts to detect, deter, and mitigate maritime threats during a demonstration of an underwater port security system at Coast Guard Integrated Support Command, San Pedro, Calif.

Figure 1: Maritime Safety and Security Team divers conduct a pier search.

"Terrorists are always looking for ways to attack elements of our infrastructure critical to our economy and our freedom," said Coast Guard Pacific Area Commander VADM Harvey Johnson during the demonstration of the system. "Our ports are absolutely vital to this nation, and we are constantly looking for ways to improve our ability to protect them."

Figure Figure 2: ET2 Jachob Smith prepares to deploy a remotely operated vehicle to conduct a pier inspection.

Underwater Port Security System

The Underwater Port Security System (UPSS) can detect, track, classify, and interdict intruders and allows for the inspection of hulls and pier structures. The UPSS adds an additional layer of protection to U.S. ports and, due to its modular and portable design, is capable of being deployed nationwide on short notice.

The UPSS is composed of two elements: the underwater inspection system and the integrated anti-swimmer system (IAS). The underwater inspection system uses divers who are trained to inspect ships' hulls, piers, and conduct harbor-bottom searches (Figure 1). It also includes remotely operated vehicles that can be deployed underwater, when it may be too dangerous to use a diver (Figure 2).

"The Coast Guard has been lacking in this area for awhile," said Petty Officer 2nd Class Jachob Smith, an electronics technician previously assigned to the Maritime Safety and Security Team (MSST) in San Pedro. "Before we had this system, it was all about crews standing lookout watches. We were really limited as to what we could see. Now, we can see very well, in even cloudy or murky water."

Figure 3: Maritime Safety and Security Team divers prepare for a search.

The second element of the UPSS is the integrated anti-swimmer system. The IAS is comprised of commercially available sonar sound heads, which are

integrated to work with an advanced government-designed processor that automatically detects and tracks potential underwater threats, classifies underwater contacts, and alerts system operators to their presence.

Testing the System

IAS is capable of guiding Coast Guard security forces to the threat and provides high-frequency sonar images to positively identify the contact as a swimmer or diver, as opposed to marine life or some other object. Smith said MSST divers have been sent underwater to try to trick the system and to test its detection parameters, and, so far, the system has proven infallible.

"We've had the divers go at the system at all speeds and from all angles, and it detects them every time," he said.

In most instances when the system is deployed, the Coast Guard will notify the public that specific security zones have been put in place. Should someone innocently enter a security zone, the Coast Guard will make reasonable efforts to communicate warnings to them using underwater loudhailers before using more forcible measures.

Many agree that this system is the next generation in port security and gives the Coast Guard the upper hand in detecting a threat (Figure 3).

"This system adds a layer of security to our ports by providing specific protection from underwater threats, and it reduces the chances of success for a possible means of attack," said Johnson. "It is by no means a guarantee, but it is an important step forward."

About the author: *Mr. Kenneth McDaniel is a program analyst in the Commandant's Office of Defense Operations and serves as project manager for Underwater Port Security. He is a retired lieutenant from the Fairfax County, Va., Fire and Rescue Department and a U.S. Coast Guard Reserve Chief Warrant Officer with more than 26 years of combined active duty and reserve service.*

Figure 2: A Coast Guard canine substance detection team searches a merchant vessel for explosives.

security operations. This recognition led to the development of specialized threat detection functions, such as dive operations and explosive detection canine teams (Figure 2), which have been built within some MSST units as collateral duties.

Organization

MSST units provide a dedicated active duty force package that possesses specialized skills, capabilities, and expertise to perform a broad range of port security and harbor defense missions. Modeled after the Port Security Unit (PSU) and Law Enforcement Detachment programs, MSST units offer a complementary Coast Guard capability that will be able to close significant readiness gaps in U.S. strategic ports. MSST units are trained in maritime law enforcement (MLE) practices, enabling them to augment Coast Guard forces during major marine events, contingencies, and other Coast Guard law enforcement operations.

MSST units are organized into a command cadre, two mobile security teams, plans and support sections. Each mobile security team consists of a waterside security section and an MLE/force protection section that can be deployed within 12 hours nationwide. MSST units will be fully mission-ready to conduct

operations, without the need for supplemental training or additional outfitting, through all MARSEC levels. The waterside security section is equipped with armed response boats and staffing to support round-the-clock boat operations.

The waterside security section is principally designed to combat external threats and protect military load outs, enforce security zones (moving and fixed), defend critical waterside facilities, and provide shoreside force protection for own unit and high interest vessels. The waterside security section is skilled in high-speed boat interdiction tactics and use of force expertise that eclipse current Coast Guard capabilities. Security tactics include active patrolling, establishing a deterrent presence, and building awareness of legitimate and suspicious activities in the port.

The MLE/force protection section is staffed by qualified MLE boarding officers and boarding team members, and includes marine science technicians who provide knowledge in port state control and other marine safety activities. The MLE/force protection section is equipped with nonintrusive inspection and detection systems, which significantly enhance Coast Guard capabilities to detect stowaways; chemical, biological, radiological, nuclear explosive (CBRNE) agents; and other contraband aboard commercial vessels. Coupled with armed fast boat capabilities, the MSST offers an integrated force package that can provide both internal and external security and a law enforcement presence for high interest vessels that is unmatched by other Coast Guard units. This section is also trained in antiterrorism/force protection tactics.

MSST units have the capability to establish a secure perimeter along waterside and shoreside approaches for its own unit, a limited number of high-value assets and critical infrastructure where Coast Guard jurisdiction permits, and are available to augment Coast Guard forces during pulse operations such as mass migrations. The command cadre and plans section leverage all mission area knowledge and expertise to accomplish the many missions in the port. The plans section provides expertise in marine safety and regulatory responsibilities and connects the MSST to the sectors, ensuring unit familiarity with port activities including:

- port security and other contingency plans;
- critical infrastructure;
- port vulnerabilities;

Figure 3: A Coast Guard gunner fires 7.62 MM rounds from a M240B machine gun.

- threats; and
- risk mitigation strategies.

Working in unison with sectors, the plans section helps exercise and evaluate Area Maritime Security plans, which are crafted by Area Maritime Security Committees, comprised of government and private-sector stakeholders. Today's port security mission requires security zones enforced by boat crews trained together in standardized, multi-boat tactics, with use of force expertise that enables them to make deadly force decisions with minimal reaction time.

Port security in the new normalcy and in heightened threat homeland defense situations requires professional boat handling and weapons skills on par with those associated with combat boat tactics (Figure 3). The Coast Guard Special Missions Training Center (SMTC), formally the PSU training detachment, has been training MSST personnel since 2001. SMTC is staffed with 50 officers, enlisted personnel, and civilians and continues to offer training in advance tactics and close-quarter combat skills. Special mission tactics, techniques, and procedures are trained by a cadre of highly qualified instructors. Upon completion of the course, MSST members are capable of performing and conducting high threat law enforcement and responding to counterterrorism events.

About the author: *CDR Aaron C. Davenport is a 1984 graduate of the U.S. Coast Guard Academy and a 1995 graduate of the University of California at Los Angeles. He has served in Coast Guard boat force, afloat, and marine safety operational commands, and his staff assignments include Combatant Command Headquarters and Logistics Command Atlantic. CDR Davenport's most recent assignment was command of Coast Guard Cutter* Valiant. *He has been selected for promotion to Captain and for the 2006 RAND Corporation Military Executive Fellowship.*

National Response Options Matrix

Senior leadership's quick response card to a maritime transportation security incident.

by CAPT Wayne C. Dumas
Chief, U.S. Coast Guard Contingency Exercises

Since the events of September 11, 2001, tremendous resources have been expended by industry and government to prevent another terrorist attack against the U.S. and to protect critical infrastructure and key resources. In the past few years, the Department of Homeland Security (DHS) has been formed and interagency and public/private sector partnerships have been developed to thwart terrorist and criminal activity that would threaten U.S. interests, borders, and way of life. The Coast Guard stepped forward as the lead DHS agency for maritime security and, with the passage of the Homeland Security Act of 2002 and the Maritime Transportation Security Act (MTSA) of 2002, has made Ports, Waterways and Coastal Security (PWCS) a primary mission.

But what if a terrorist attack should occur in a major U.S. port or within the U.S. Maritime Domain? How, and where, should the Coast Guard respond? Will the response actions mitigate further attacks or will they damage the U.S. economy and erode public confidence?

Before the Senate Commerce, Science, and Transportation Committee on September 9, 2003, the Commandant of the Coast Guard, Admiral T.H. Collins, stated: "…a terrorist incident against our Marine Transportation System would have a devastating and long-lasting impact on global shipping, international trade, and the world economy. As part of a recent port security training exercise, a maritime terrorist act was estimated to cost up to $58 billion in economic loss to the United States."

This statement underscores the importance of immediate responses to maritime transportation security incidents (TSI), which are incidents resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. This response must appropriately and proportionally address the local level, but also the national level, to keep public confidence in government high and the U.S. economy strong. To this end, the National Response Options Matrix (NROM) was developed.

NROM Features

NROM provides senior leadership with pre-planned responses for immediate use following a maritime transportation security incident, or imminent threat of a maritime TSI, in one or more of U.S. ports, waterways, or coastal approaches. In essence, this matrix is a quick reaction card or decision aid for use by senior leadership to direct a security posture that may transcend Coast Guard Areas (Atlantic Area and Pacific Area); significantly impact the maritime industry; change the Maritime Security (MARSEC) Level; and perhaps affect or involve other DHS agencies or federal departments. For example, U.S. Customs and Border Protection (CBP) has already joined the Coast Guard in development of an interagency NROM, with specific actions focused on response and recovery. NROM is also available electronically to the Coast Guard Captains of the Port to engage their Area Maritime Security Committees for planning and awareness training and to gain possible feedback for response and recovery option improvements.

The NROM goal is to provide senior Coast Guard and CBP leadership with immediate, pre-planned, short-term security options to prevent further attacks; protect the marine transportation system, maritime critical infrastructure and key assets, and high-density population centers; and recover from a TSI, through:

- changes in MARSEC Level governing security activities of Coast Guard forces and the maritime industry;
- closure or control of ports by specific port, regionally or nationally;
- expanded CBP law enforcement boardings to screen crewmembers and remove detained-on-board crewmembers for immediate repatriation;

- restriction of certain port activities and access to certain facilities or vessels;
- deployment of specialized Coast Guard or CBP security capabilities and law enforcement assets;
- an increase in vessel, crew, and cargo screening;
- denial of entry or expulsion of certain vessels, directing vessels to anchorages or safe berths;
- potential changes in Coast Guard force protection level; and/or
- identification of other agency points of contact for notification or coordination of activities on a national level, regionally, or by specific ports; may also include port-specific Area Maritime Security Committees or the maritime industry representatives on the National Maritime Security Advisory Committee (NMSAC). NMSAC is comprised of members from various sectors of the maritime industry and was established to provide advice to the Secretary of Homeland Security, through the Commandant of the Coast Guard, on matters of maritime security.

Confidence is high that, at the affected port level, the Coast Guard Captain of the Port/Federal Maritime Security Coordinator, in coordination and cooperation with CBP and other federal, state and local agencies and industry stakeholders, will respond appropriately to mitigate the effects of a maritime TSI. Additional and heightened security measures will be imposed in the specific port of attack. MTSA requires the creation and approval by the Coast Guard, exercise and updates to Area Maritime Security Plans. Port Security Assessments, and vessel and facility security plans to deter, deny, prevent, protect, and respond to maritime TSIs. Elements of these plans will be ordered into effect by the Captain of the Port.

NROM addresses the security posture needed beyond the affected port by helping senior leadership answer the question: What additional or heightened security measures need to be implemented immediately to prevent further attacks and protect the marine transportation system, maritime critical infrastructure, key assets, and high-density populated areas from follow-on attacks on a regional or national basis? These security measures may only target certain aspects of the marine transportation system, while at the same time maintaining the legitimate flow of commerce and use of the maritime environment. By having pre-planned response options, senior leadership can react quickly to immediately direct field units, industry and other governmental agencies to act appropriately and proportionately to prevent further terrorist attacks and disruption of maritime transportation.

Preplanned response options buy time. NROM security measures are immediate and short-term actions. Concurrently with NROM measures, planning teams will prepare more robust and comprehensive plans based on additional intelligence information, situational analysis, and appropriate and available capabilities and will coordinate with other agency partners and with industry representatives via the NMSAC.

Rapid Interagency Information Sharing

The quick response to the credible threat of terrorist activity, or an actual TSI event, requires the rapid sharing of information vertically and horizontally throughout the Coast Guard, Customs and Border Protection, the Department of Homeland Security, other federal and state agencies, and the maritime community. The Coast Guard Command Center has developed an incident reporting system, Critical Incident Communications, to rapidly disseminate initial, limited information about critical incidents throughout the Coast Guard and interagency partners. Security measure decisions based on the NROM will be communicated quickly to areas, districts, field units, and, as appropriate, to the maritime industry via the Area Maritime Security Coordinator.

Both the Coast Guard and Customs and Border Protection have extensive authorities within the maritime environment. The Coast Guard Captain of the Port is responsible for all vessel movements, including ordering vessels to depart ports and permitting vessels to return to ports. The Coast Guard is responsible to ensure that vessels, including crew, passengers, and cargo, do not pose a threat to the United States. The Coast Guard is also responsible for the protection of maritime infrastructure.

The CBP priority mission is to prevent terrorists and terrorist weapons from entering the United States. The CBP is responsible for the clearance of vessels, persons, and cargo arriving from foreign ports. CBP has the authority to approve the lading and unlading of cargo and the embarkation and disembarkation of crew and passengers. CBP has the authority to examine, detain, and seize cargo and penalize carriers. By partnering on the National Response Options Matrix, both agencies have created a model tool for rapid decision making and interagency security coordination to prevent attacks and protect the marine transportation system, maritime critical infrastructure and key assets, and coastal high-density populated areas.

The National Response Options Matrix is a model tool for interagency security cooperation and coordination. Perhaps other federal agencies will join the Coast Guard and Customs and Border Protection in this collaborative effort to rapidly thwart terrorist attacks, while preserving the flow of maritime commerce and legitimate use of the maritime environment.

About the author: *CAPT Wayne C. Dumas is a Coast Guard Reserve officer who, for the past five years, has been on active duty in the Office of Port Security, Planning and Readiness and been an adjunct member of the G-OPD/G-MPP Homeland Planning Team. He was previously at PACAREA on the Maritime Homeland Security Planning Team. CAPT Dumas was Commanding Officer of Port Security Unit 313 and N3/N5 of Naval Coastal Warfare Unit 113. CAPT Dumas is currently assigned to G-RPE, Chief, Contingency Exercises.*

Counterterrorism Force

Building the Coast Guard Maritime Security Response Team.

by LCDR Jose L. Rodriguez
Chief, Operations and Training Division, U.S. Coast Guard Office of Counterterrorism and Special Missions

by LTC Michael Kichman, U.S. Army (ret)
Special Counterterrorism Advisor, U.S. Coast Guard Office of Counterterrorism and Special Missions

On September 11, 2001, the dynamic of national security shifted drastically, with attacks on U.S. soil for the first time since the beginning of World War II. Unlike the Japanese attacks on Pearl Harbor, the terror attacks of 9/11 were aimed not at military targets, but at innocent civilians and the economic heart of the United States. These attacks signaled a distinct shift from the Cold War paradigms that had dominated U.S. strategic thinking and defense planning for more than 50 years.

Suddenly, the tools of security and defense the United States had relied on were no longer effective at guaranteeing the safety and security of the country or its people. This reality dictated a new maritime security response posture from the U.S. Coast Guard. Today, at the forefront of this emerging security mission is the new Coast Guard Maritime Security Response Team (MSRT) based in Chesapeake, Va. (Figure 1).

Developing the Force

Initial Coast Guard efforts to fill this capability gap in the post-9/11 world resulted in the development and fielding of a prototype unit, designated the Enhanced Maritime Safety and Security Team (EMSST) in Chesapeake, Va. Based on specific authority and guidance in the Maritime Transportation Security Act of 2002, the Coast Guard began to equip, train, and deploy this new EMSST to execute a wide range of anti- and counterterrorism and advanced interdiction missions. Specifically, this unit was designed as an integrated air, surface, and maritime military/law enforcement force, capable of executing at-sea takedowns of hostile vessels or vessels seized by hostile forces.

Figure 1: The Maritime Security Response Team conducts vertical insertion drills on a 270-foot, medium endurance Coast Guard cutter.

The EMSST was designed around direct action sections; a boat detachment; a chemical, biological, nuclear, radiological, and explosive (CBNRE) detachment; and lift and support aviation assets. These capabilities were designed to operate in concert to provide the Department of Homeland Security (DHS) with a highly capable maritime counterterrorism force for employment in the domestic Maritime Domain. Additionally, the EMSST could deploy in direct support of Department of Defense requirements under the Coast Guard's Title 10 authorities. Prior to the stand-up of this force, no U.S. government agency, outside the Department of Defense Special Operations Command, was capable of such integrated and complex maritime counterterrorism (CT) operations.

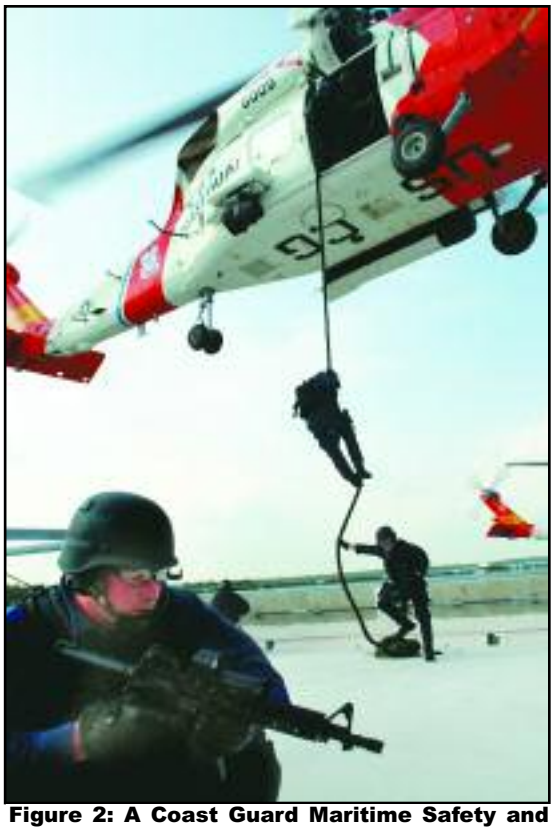


Figure 2: A Coast Guard Maritime Safety and Security boarding team is delivered onto a vessel, via vertical insertion, from an HH-60 Jayhawk.

From its inception in spring 2004, EMSST was deployed in support of domestic maritime security requirements, both for Coast Guard law enforcement missions and in support of other U.S. government agencies. As requirements are refined in emerging national maritime security strategies and plans, the demand for EMSST capabilities continues to grow. This growing demand, as well as a full recognition of the seam in U.S. maritime defenses, has resulted in EMSST capability becoming a permanent part of the Coast Guard force structure. This transition was recently marked by recognition of EMSST as an official part of the Coast Guard, with its redesignation as Maritime Security Response Team.

Today, the Coast Guard stands ready to protect and defend U.S. maritime borders with a highly capable maritime counterterrorism force (Figure 2). As the unit continues to refine its capabilities, there is much work still to be done. The MSRT needs additional assets and training to be fully mission-capable, as well as further integration into all national CT response plans. The latter is especially critical to ensure that no seam is left uncovered for U.S. enemies to exploit.

The Long-Term Solution

While closely examining maritime security issues and potential gaps in strategic counterterrorism response capabilities, DHS and National Security Council staff members came to a clear consensus that certain security requirements must be addressed in the near-term within the Maritime Domain, as well as other geographic parts of the country. To accomplish this goal, the Coast Guard is working with its partners within DHS and the executive branch to ensure that the U.S. maritime shield has the assets necessary to protect U.S. borders from all levels of threat. MSRT has been asked to fill an articulated security gap in the Maritime Domain.

These enhancements to existing Coast Guard maritime capabilities are intended to provide the United States an integrated maritime shield, with a sharpened sword, fully capable of defeating all maritime threats on the immediate horizon. While this Coast Guard vision provides a solution to combating maritime threats, the question of a fully resourced program remains. As the United States' only multi-mission, military / law enforcement force, spanning the homeland security to homeland defense seam, the Coast Guard is uniquely positioned to house a national maritime counterterrorism force. In an era of limited resources and unlimited security challenges, the Coast Guard also provides a logical home for the development of enhanced maritime interdiction and counterterrorism forces, capable of employment either in the law enforcement or defense arenas.

As the United States continues to resource assets to fill seams identified by the currently emerging maritime security strategies and plans, it is likely the Coast Guard will be called upon once again to leverage its unique place in the national security structure, in defense of U.S. maritime borders.

About the authors: *LCDR Jose L. Rodriguez has served in the U.S. Coast Guard for 25 years and is an expert on Coast Guard Special Missions. His experience includes command of Maritime Safety and Security Team Chesapeake, Tactical Law Enforcement Team South, Officer in Charge Riverine Section, USMC Special Operations Training Group, IIMEF, and MLE School Instructor. LCDR Rodriquez deployed throughout Latin America in support of Department of Justice, OPERATION SNOWCAP.*

LTC Michael Kichman, U.S. Army (ret), is a special counterterrorism advisor to the U.S. Coast Guard Office of Counterterrorism and Special Missions.

Get In-Depth Information on the Maritime Industry

U.S. Department of Homeland Security

United States Coast Guard

The Coast Guard Journal of Safety at Sea

PROCEEDINGS

of the Marine Safety & Security Council

Maritime Homeland Security

STCW

Recreational Boating Safety

Uninspected Passenger Vessels

Towing Vessels

Large Passenger Vessels

...Lots more

For a **FREE** Subscription
Email or Fax the following information

Name: _____

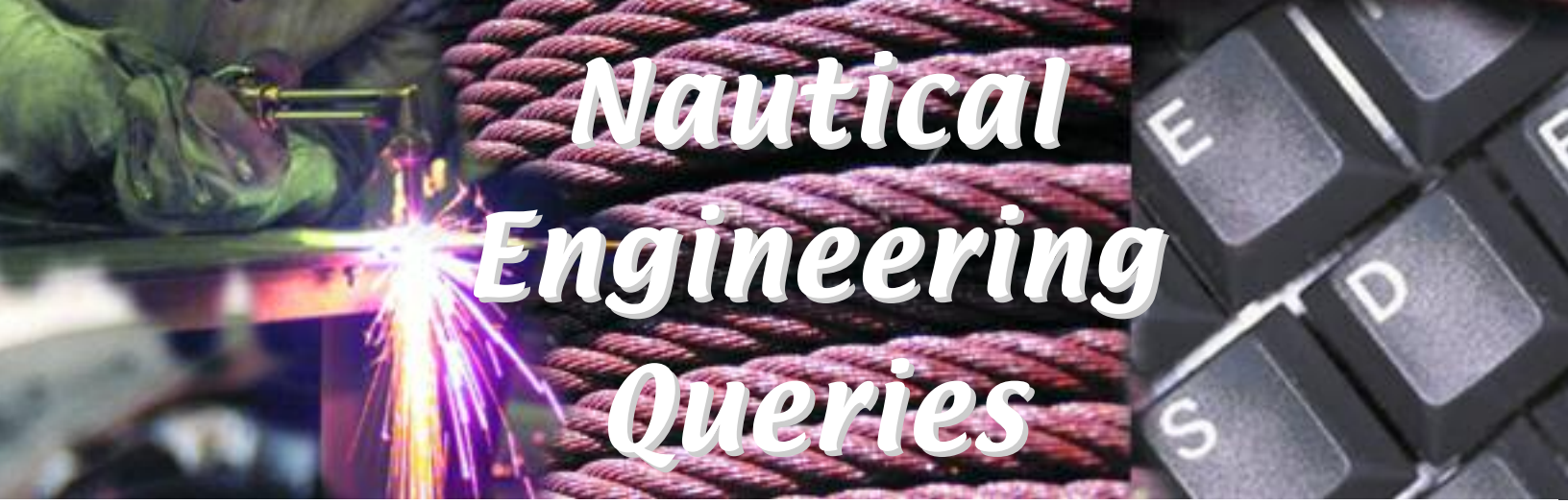
Title: _____

Company: _____

Address: _____

_____

Subscribe online at www.uscg.mil/proceedings
Fax this form to: (202) 493-1061, *Attn: Proceedings Distribution*
Or Mail: Commanding Officer (NMC-3), *Attn: Proceedings Distribution Manager,*
U.S. Coast Guard, 4200 Wilson Blvd., Suite 730,
Arlington, VA 22203-1804



1. The ignition quality of diesel fuel becomes less critical as _____.

Note: Ignition quality is the ability of a fuel to ignite when it is injected into the compressed-air charge in the diesel engine cylinder. A fuel with a good ignition quality ignites readily, with a minor ignition delay resulting in a smoother running engine with less noise and vibration. A fuel with a poor ignition quality will be delayed in its ability to ignite. The ignition quality of a fuel affects the ease of starting the engine and its performance.

A. the amount of lube oil additives increase
Incorrect: Lube oil additives only provide for specific operational improvements of the lube oil to reduce friction while the engine is in operation. Additives such as foam inhibitors, detergents, viscosity index improvers and TBN additives that neutralize acid formation have no effect on the actual combustion characteristics of the fuel during normal engine operation.

B. piston speeds increase
Incorrect: Since piston speed is a function of piston stroke and engine RPM, an increase in piston speed will result from an increase in engine speed. This will decrease the available period for total combustion during the power stroke, thereby becoming a critical factor and requiring a high quality fuel with a rapid ignition characteristic.

C. injection pressures decrease
Incorrect: Low quality fuels require higher preheat temperatures to reduce viscosity, which, if not provided, would result in higher injection pressure in order to properly atomize and mix the fuel charge with combustion air for complete combustion.

D. engine speeds decrease
Correct Answer: A decrease in engine speed provides an increase in the period of time available for total combustion of the fuel during the power stroke and provides additional time to compensate for ignition delay when using low quality fuels.

---

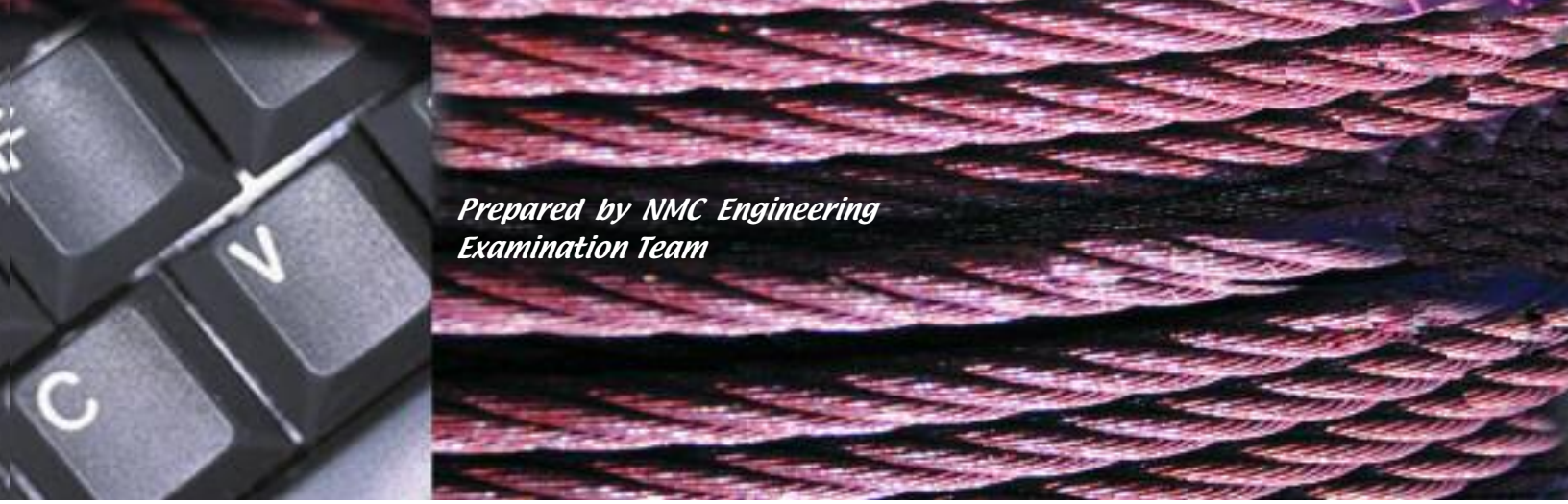
2. Which of the following statements is TRUE concerning lifejackets?

A. Buoyant vests may be substituted for lifejackets.
Incorrect: A life preserver is designed and constructed with material and workmanship to perform its intended function in all weather conditions. Buoyant vests are designed for use only under ideal conditions and are not substitutes for lifejackets nor are they required to meet minimum life preserver requirements.

B. Kapok lifejackets must have plastic-covered pad inserts.
Correct Answer: Kapok pad inserts are to be covered with a flexible vinyl film not less than 0.006 inches in thickness as cited by 46 CFR Part160.002-3(d).

C. Lifejackets must always be worn with the same side facing outwards.
Incorrect: Lifejackets are designed to be donned correctly without prior demonstration, instructions, or assistance by at least 75% of the persons unfamiliar with the design. To meet this specification, it is required that the lifejacket is capable of being worn inside out.

D. Lifejackets are not designed to turn a person's face clear of the water when unconscious.
Incorrect: Lifejackets are designed to support the wearer in the water in an upright or slightly backward position, and are to provide support to the head so that the face of an unconscious or exhausted person is held above the water.



3. The opposition to the establishment of magnetic lines of force in a magnetic circuit is called the circuit's _____.

A. resistance
Incorrect Answer: Resistance is the opposition to current flow through the components of a circuit.

B. reluctance
Correct Answer: The strength of magnetic flux is partly determined by the permeability of the material being magnetized. Reluctance is inversely proportional to permeability. As an example, iron has high permeability and low reluctance while an air gap has low permeability and high reluctance. Generator and motor magnetic circuits are designed with minimum air gaps to minimize losses due to reluctance and maximize magnetic flux strength.

C. impedance
Incorrect: Impedance is the total resistance of an AC circuit and its components including inductive and capacitive reactance.

D. inductance
Incorrect: Inductance is the characteristic of an AC circuit, which causes a delay in the change of magnitude of current flow due to the effects of a generated magnetic field produced in the circuit.

---

4. A vessel, which is subjected to "hogging", has its _____.

A. main deck under compressive stress
Incorrect: When the main deck plating encounters compressive stresses, the vessel is said to be in a condition known as "sagging." This occurs when the vessel is supported mainly by wave crests at the bow and stern.

B. main deck plating under tensile stress
Correct Answer: When the main deck plating of a vessel is encountering tensile stresses, the vessel is said to be in a condition of "hogging." This condition is most pronounced when the buoyant force of a wave is midship to the vessel, resulting in the bow and stern deflecting downward.

C. bottom plate under shearing stress
Incorrect: Shearing stress is the tendency of one part of a body to slide over another part. This condition causes materials to be cut or sliced.

D. bottom and deck plating under compressive stress
Incorrect: A "hogging" condition will cause only the bottom hull plating to be under compressive stresses, while, at the same instant, the main deck will be under tensile stress. A ship's hull is essentially a hollow box beam, and, when at rest, neither tensile nor compressive stresses are present.

1. If your vessel has a list to port due to negative GM and off-center weight, the first corrective measure you should take is to _____.

Note: A negative metacentric height or "negative GM" is the result of an unstable condition when the center of gravity is above the vessel's metacenter. Action must be taken to reestablish stability either by removing weight from above the center of gravity or by adding weight below the center (or both) before continuing with cargo operations.

A. move port-side main-deck cargo to the starboard side

Incorrect: Moving weight horizontally will initially lessen the list but will contribute nothing to improving the ship's stability. Because the ship's center of gravity is above its metacenter, the ship will continue to remain unstable and list suddenly to starboard as soon as the relocated mass passes the vessel's longitudinal centerline.

B. fill the starboard double-bottom

Correct Answer: By filling a double-bottom tank, the ship's center of gravity is being lowered as weight is being added as low as possible. The most desirable action to take immediately is to ballast all double-bottom tanks that are empty until positive stability is established.

C. pump water from the port double-bottom to the starboard double-bottom

Incorrect: This action is essentially the same as that in choice "A." Shifting weight from port to starboard will not correct the ship's instability.

D. pump water from the port double-bottom over the side

Incorrect: The removal of weight from below the center of gravity will increase instability.

---

2. Which type of GPS receiver has at least four channels to process information from several satellites simultaneously?

Note: A navigational receiver aboard a vessel is able to track six to 10 GPS satellites simultaneously. There are four satellites, in each of six orbits, broadcasting navigational data. At the time of this writing, the GPS "constellation" consists of 29 satellites because five of the orbits contain a new satellite for the replacement of an older one.

A. Sequential

Incorrect: The original GPS receivers of the 1980s were "sequential," meaning that the receiver had to receive input, then switch reception in sequential order from one satellite to the next as only one channel was available. These receivers were only able to track the satellites "within view" through one receiving cycle at a time, resulting in a "slow" position determination. Because these receivers were hampered by the relatively time-consuming process of switching satellite reception, they were not useful to the aviation industry. The main reason for this initial design was to minimize cost and power consumption during the initial phases of GPS development. Sequential receivers are no longer manufactured.

B. Continuous

Correct Answer: The significance of the "four channels" referred to in this question is that this is the minimum number of satellites from which the receiver must acquire information in order to provide the user with an accurate position. Since six to 10 satellites are being monitored simultaneously, there is no time delay required to switch from one satellite to another in sequential order. Quality GPS receivers, such as those used for maritime navigation, are now designed with at least 12 channels. It is unnecessary for GPS receivers to be designed with more than 12 channels as no more than 10 satellites may be "visible" at any one time.

C. Multiplex

Incorrect: Multiplex reception is an improvement over the original sequential receiver. The receiver must still switch from one satellite to another, but now accomplishes this at a much faster rate of (typically) 50 Hertz, versus the 5 to 10 Hertz rate of the original "sequential" receivers. A multiplex receiver acquires navigational data from one satellite for a predetermined "slice of time," then switches to another satellite, for the same "slice of time," to receive additional navigational data. If it is able to perform the switching fast enough, the receiver seems to be tracking all of the satellites simultaneously. The hand-held receivers designed in the mid to late 1990s are multiplex, and many of them are still being used.

D. None of the above

Incorrect: Choice "B" is correct.

3. Before operating a non-oceangoing ship greater than 100 gross tons, it must have a fixed piping system to discharge oily mixtures ashore. This system must include _____.

Note: Oceangoing ships of 400 gross tons and greater are required to have this equipment. (33 CFR 155.360)

A. approved oily-water separating equipment

Incorrect: Although many small ships operating on U.S. Inland Waters are equipped with oily-water separators, this equipment is not required on a non-oceangoing vessel.

B. a fixed or portable containment system at the shore connection

Incorrect: A containment system is not required at the shore connection to the oily-water discharge piping. This must not be confused with the required containment on deck at the cargo piping shore connection (33 CFR 155.310) or the required containment under the fuel tank vent goosenecks during fueling operations. (33 CFR 155.320)

C. a spare pump in case the main pump is inoperative

Incorrect: For the purpose of discharging an oily mixture ashore, only one pump is required, even if "good engineering" recommends two pumps.

D. at least one outlet accessible from the weather deck

Correct Answer: The required piping system must have at least one outlet fitted with a stop valve accessible for connecting a discharge hose from the weather deck. This connection must be compatible with the facilities in the vessel's area of operation. (33 CFR 155.410)

---

4. In a tropical cyclone in the southern hemisphere, a vessel hove-to with the wind shifting clockwise would be _____.

Note: Wind blows from an area of high pressure toward—or into—an area of low pressure. Because of the effect of the earth's rotation, the wind direction is diverted to the left in the southern hemisphere (right in the northern hemisphere) as viewed from above. Therefore, wind circulates clockwise around a "Low" in the southern hemisphere. Don't confuse this clockwise cyclonic rotation with the direction that the wind is "shifting," as observed from aboard a vessel experiencing the cyclone. Shifting is defined as the gradual, progressive change in wind direction, as the cyclone approaches and passes a vessel. By monitoring this directional change, in addition to monitoring the barometer, mariners can determine their location relative to the cyclone's center. When a vessel is ahead of an approaching storm, the barometer will be falling, and as the storm passes, the barometer will begin rising. The direction of cyclonic rotation can never change from clockwise to counterclockwise, or vice-versa, because a tropical cyclone cannot cross the equator. Often, the best possible action is to hold the ship with its bow into the wind (hove-to) to minimize rolling. The condition to be avoided is having either (port or starboard) side to the wind and seas (broach-to).

A. ahead of the storm center

Incorrect: The wind direction will remain constant if the vessel is on the storm's track.

B. in the dangerous semicircle

Incorrect: If a ship in the southern hemisphere is in the dangerous semicircle, the wind will be shifting counterclockwise as the storm approaches and passes. This semicircle is the one to the left of the storm's track in the southern hemisphere versus the right in the northern hemisphere. The semicircles are named "dangerous" and "navigable" because of the difference in wind speed between them. For example, if the rotational wind speed is 80 knots, and the storm is moving at 20 knots along its track, the actual wind speeds in the dangerous and navigable semicircles are 100 and 60, respectively.

C. directly behind the storm center

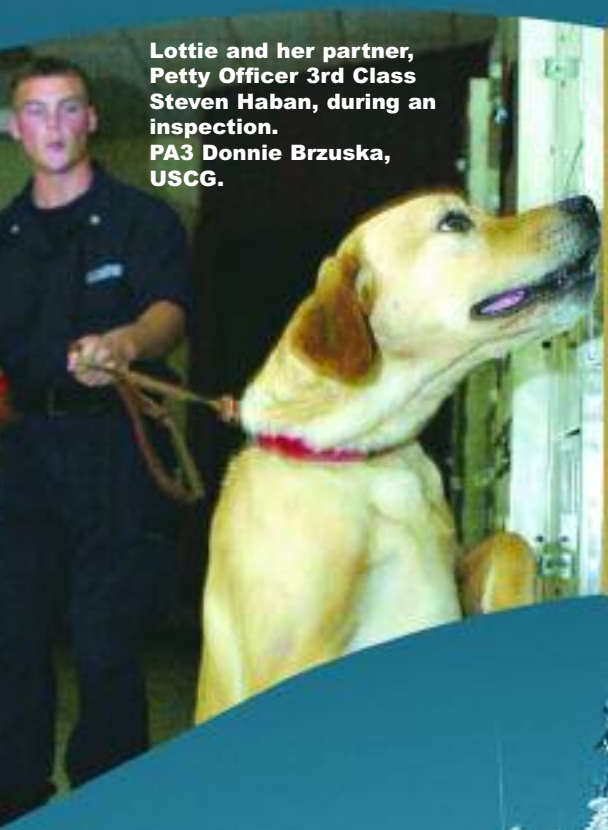
Incorrect: The wind direction will remain constant if the vessel is on the storm's track.

D. in the navigable semicircle

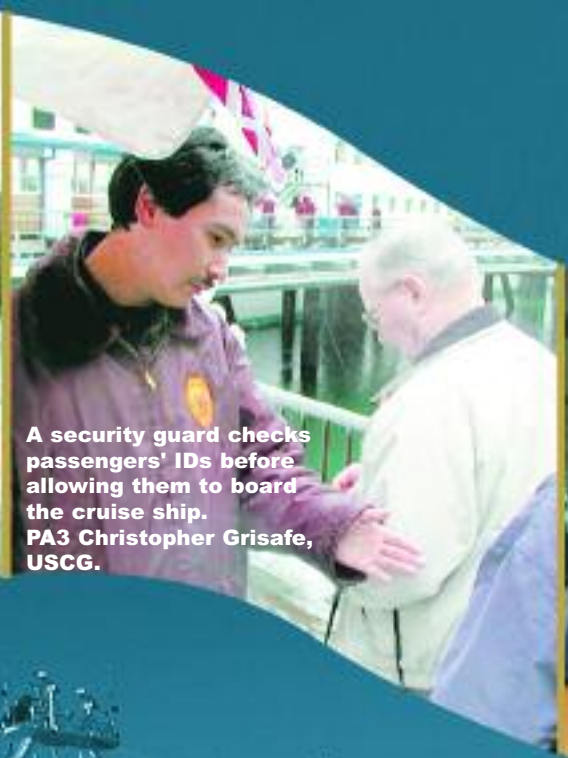
Correct Answer: If a ship is coming into the navigable semicircle of a westbound approaching storm in the southern hemisphere, it will first encounter a southwesterly wind becoming westerly while the barometer is falling. Then, the wind will become northwesterly and the barometer will begin rising as the storm passes.

U.S. Department
of Homeland Security

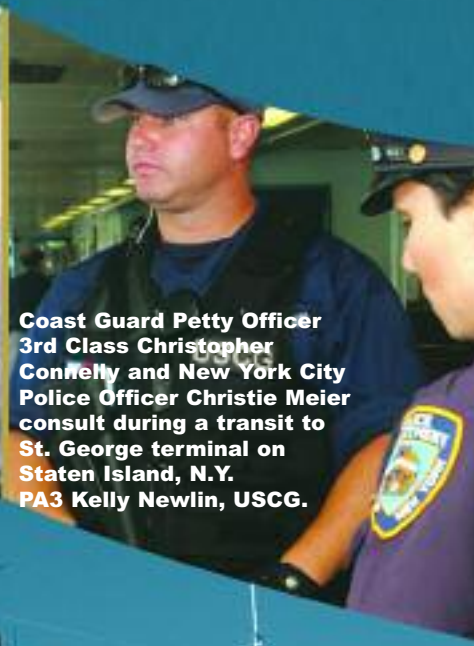
United States
Coast Guard



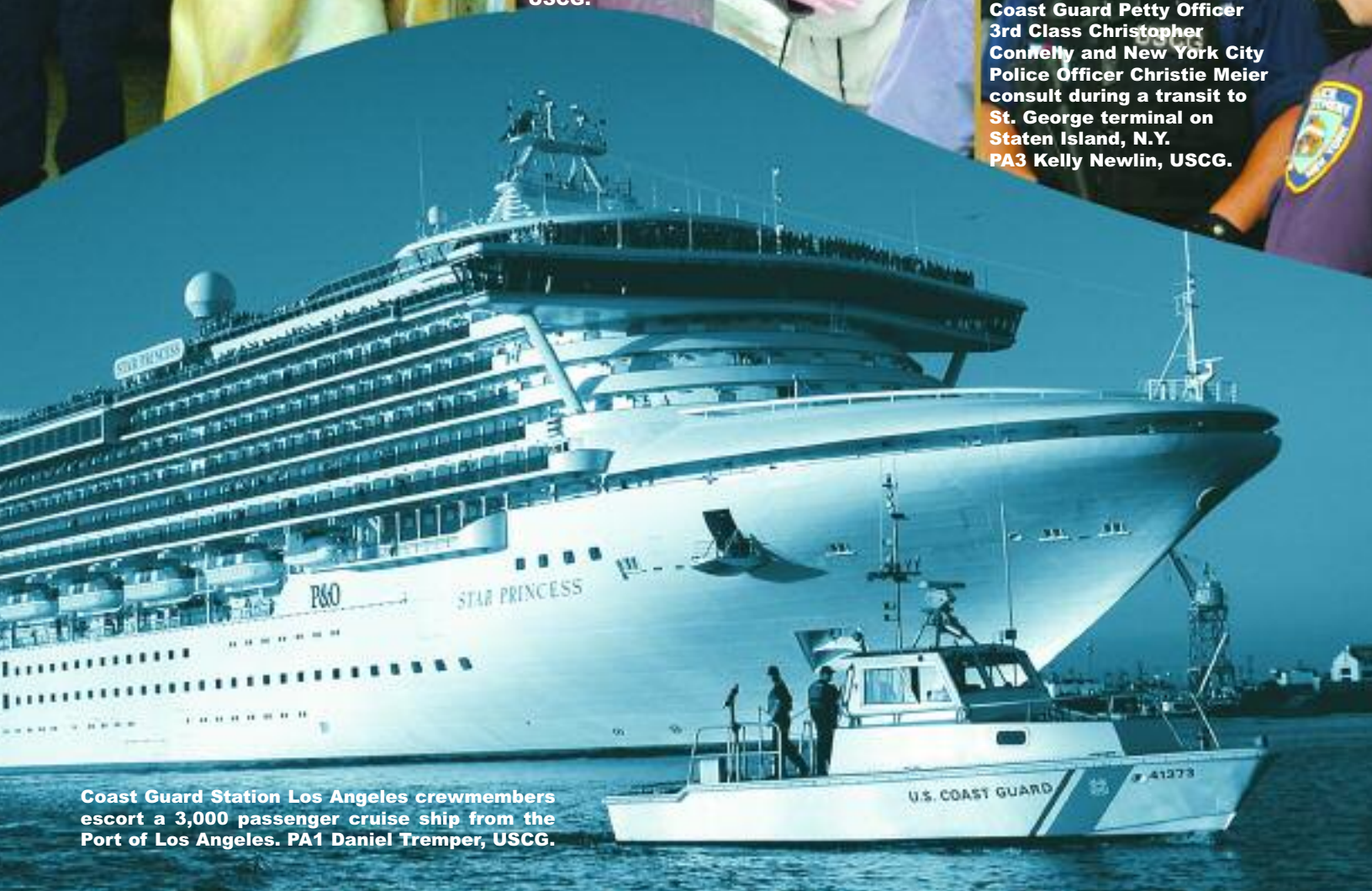
Lottie and her partner, Petty Officer 3rd Class Steven Haban, during an inspection.
PA3 Donnie Brzuska, USCG.



A security guard checks passengers' IDs before allowing them to board the cruise ship.
PA3 Christopher Grisafe, USCG.



Coast Guard Petty Officer 3rd Class Christopher Connelly and New York City Police Officer Christie Meier consult during a transit to St. George terminal on Staten Island, N.Y.
PA3 Kelly Newlin, USCG.



Coast Guard Station Los Angeles crewmembers escort a 3,000 passenger cruise ship from the Port of Los Angeles. PA1 Daniel Tremper, USCG.