

U.S. Department
of Homeland Security

United States
Coast Guard



The Coast Guard Journal of Safety at Sea

PROCEEDINGS

of the Marine Safety Council



Maritime
Homeland Security

PROCEEDINGS



April-June 2003

Vol. 60, Number 2



On the Cover

Members of Port Security Unit 307 patrol Boston Harbor. Members of PSU 307, a reserve unit based in St. Petersburg, Fla., were deployed to Boston following terrorist attacks in New York City, Washington, DC and Pennsylvania. Photo by Public Affairs Officer Megan Casey, USCG.

A New Normalcy

- 6 Attack on New York ... *The First Response*
- 10 A Family of Security Plans
- 14 IMO Moves to Enhance International Maritime Security
- 19 U.S. Enacts Measure for Maritime Security
- 24 Citizens Assist in Keeping the Watch
- 27 New Security Measures in Mariner Credentials



Securing Our Ports

- 29 Port Security Assessments
- 34 TSA Administers Grants for Port Security Improvements
- 36 The Automatic Identification System & Port Security
- 42 Houston-Galveston Area: *On the Front Line*
- 48 Establishing a Port Security Committee



Industry Initiatives

- 51 Barge Industry Develops First Coast Guard-Approved Security Plan
- 53 Building Security Guidance in the Domestic Passenger Vessel Industry
- 55 Perspectives on U.S. Security Initiatives Affecting International Liner Shipping
- 61 Cruising with Heightened Security Standards
- 64 The Pilot's Role in Maritime Security
- 66 The Need for Vessel Security Officer Training



Expanded Protection

- 68 Coast Guard Remains Ready with Mobile Units
- 70 Increased Coast Guard Assets for Homeland Security
- 73 Homeland Security—*Foreign Passenger Vessel Security Program*
- 75 Operation Safe Commerce—Northeast: *Container Shipping Through Partnerships*



Looking Forward

- 78 Smart Card Technology in the Maritime Transportation Industry
- 82 Technology for Port Security
- 85 Improving Our Future Capabilities with the Integrated Deepwater System



Always On Deck

- 4 Assistant Commandant's Perspective
- 5 Champion's Point of View
- 90 PTP: *Beyond Traditional Application*
- 92 Mariner's Seabag: *What Can PREP Do for You?*
- Nautical Queries
 - 94 Engineering
 - 95 Deck

In Our Last Issue

In reference to the Uninspected Passenger Vessels issue of *Proceedings*, October–December 2002; Vol. 59, No. 4; p. 35, the caption should read as follows: The 12-pack *Endeavour* holds a Certificate of Inspection allowing it to sail with 32 passengers within one mile of shore, with 15 passengers within 20 miles of a harbor of safe refuge, 12 passengers overnight, or as a recreational vessel when no passengers are onboard. Photo by KOS Photography, courtesy J Class Management.



Icon Credits:
All are USCG illustrations.

Securing Our Ports skyline image; Expanded Protection monitor image; and Looking Forward binocular image are copyright © 2003 USCG and its licensors.

Industry Initiatives container image: courtesy Hyundai Merchant Marine Co.



Assistant Commandant's Perspective

by Rear Adm. PAUL J. PLUTA

Assistant Commandant for Marine Safety, Security & Environmental Protection

The landscape of the maritime community has changed dramatically in the past two years, when I first wrote in this space. Though we experienced one of the most horrific acts of terrorism on U.S. soil, the maritime community today is more secure because of the prompt measures taken by our partners in industry and other federal, state, and local governments. Maritime homeland security has become a principal mission and an integral element of our culture.

All sectors of our community now operate with greater awareness and cooperation as we move to make our marine transportation system more safe and secure. Several actions have recently been enacted to advance those goals on the national and international level. Most notable was passage of the Maritime Transportation Security Act (MTSA), signed by President Bush on Nov. 25, 2002. MTSA aligns with the new International Ship and Port Facility Security Code, which was adopted by the International Maritime Organization in December 2002. Additionally, as a symbol of our renewed focus on security, the Coast Guard was transferred to the new Department of Homeland Security on March 1, 2003. President Bush created the new department, composed of 22 previously disparate domestic agencies, to better protect against threats to our homeland.

Our challenge in implementing many new security measures has been finding the balance between facilitating the free flow of goods and services and protecting national security. This issue of *Proceedings* offers a look at some of the initiatives that the Coast Guard, other agencies, and industry have undertaken since September 11.

A continuation of our partnerships with industry and other federal, state, and local agencies is vital to our success in meeting our maritime homeland security mission requirements. Our relationships with other government agencies are crucial to ensure coordination of efforts and most efficient use of resources. Our partnerships with each of the industry groups are essential to ensuring the free flow of goods and services, while maintaining programs and systems to ensure greater awareness. As importantly, we rely on every mariner, every dockworker and every boater to aid in keeping our ports and waterways secure by increasing their own awareness of the maritime environment in which they work and play.

As I prepare to retire from active duty with the U.S. Coast Guard, I offer heartfelt thanks to the entire maritime community in cooperating to improve the security of our maritime homeland and the safety of our marine transportation system. Because of the many active partnerships we have developed with industry and other agencies, the Coast Guard is better prepared to confront its future challenges and protect the American people and our ports, waterways and coasts. Thank you for being members of a great American team. Semper Paratus!

Ed. Note: Rear Adm. Thomas Gilmour relieved Rear Adm. Pluta July 1, 2003.

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

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

Rear Adm. John E. Crowley
Chief Counsel
Chairman
U.S. Coast Guard

Rear Adm. Paul J. Pluta
Assistant Commandant
for Marine Safety, Security
& Environmental Protection
Member
U.S. Coast Guard

Rear Adm. David Belz
Assistant Commandant
for Operations
Member
U.S. Coast Guard

Cmdr. Laticia J. Argenti
Executive Secretary
U.S. Coast Guard

Steven Venckus
Legal Counsel
U.S. Coast Guard

Statement of Ownership, Management and Circulation

DIST (SDL No. 134)
A: ac(2); ebfghijklmnopqsuv(1).
B: nr(50); cefgipw(10); bklqshj(5);
xdmou(2); vyz(1).
C: n(4); adek(3); blo(2); cfgijmpqr
tuvwyz(1).
E: ds(5); abcdefghijklmnopqrstu
vwyz(1).
E: kn(2).
F: abcdehjkloqst(1)
List TCG-06

Editorial Team

Albert G. Kirchner Jr.
Acting Executive Editor

Ellen Rosen
Managing Editor

Jesi Hannold
Senior Graphic Designer/
Technical Writer

Proceedings (ISSN 0364-0981) 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

NMCPceedings@ballston.uscg.mil

Editor, *Proceedings* Magazine
U.S. Coast Guard
National Maritime Center
4200 Wilson Blvd., Suite 790
Arlington, VA 22203-1804

Subscription Requests/Changes

Please include mailing label information when changing address.

www.uscg.mil/proceedings

ProceedingsDistribution@ballston.uscg.mil

Subscriptions, *Proceedings* Magazine
U.S. Coast Guard
National Maritime Center
4200 Wilson Blvd., Suite 790
Arlington, VA 22203-1804

**View *Proceedings* Online at
www.uscg.mil/proceedings**

Champion's Point of View



by Rear Adm. LARRY HERETH
Director; U.S. Coast Guard Port Security

The articles in this Maritime Homeland Security edition of *Proceedings* highlight only a small portion of the many ongoing initiatives and entities involved in the monumental effort to improve our nation's security. Both U.S. Coast Guard members and our partners in this effort from the maritime industry and other agencies authored the articles. Included are discussions on how the maritime community will need to routinely operate under a **New Normalcy**, some specific efforts needed for **Expanded Protection for Securing Our Ports**, commendable **Industry Initiatives** taken voluntarily to improve the security of the maritime community, and, **Looking Forward**, research and development efforts to utilize technology and new acquisitions.

The need to rapidly improve security has also necessitated that government investigate how we can better organize to provide the services needed to protect our nation. An example of the Coast Guard's efforts to ensure the proper emphasis on security was the establishment of the Port Security Directorate under the Assistant Commandant for Marine Safety, Security and Environmental Protection (G-M). This new directorate combines and gives proper emphasis to all previous security efforts under G-M. It is only one of several new changes underway to better align the Coast Guard's missions and units to serve the public.

The most significant organizational change within the federal government is the move of several agencies into the new Department of Homeland Security (DHS). The Coast Guard's transition into DHS has proceeded smoothly. The new department has made it easier for the numerous agencies involved with homeland security to coordinate activities. The Coast Guard works with all five DHS Directorates and in particular, interacts closely on security issues with the Border and Transportation Security directorate, which includes the Transportation Security Agency (TSA) and the former U.S. Customs and Immigration and Naturalization Services, and with the Information Analysis and Infrastructure Protection (IAIP) directorate. As discussed in an enclosed article authored by a senior TSA official, the Coast Guard, TSA and the Transportation Department's Maritime Administration collaborate on the port security grant program. The Coast Guard is also working very closely with IAIP on the Port Security Assessment program discussed in another article.

By the time you receive this edition, the well-publicized Temporary Interim Rules on maritime security, mandated by the Maritime Transportation Security Act of 2002, will have been published in the *Federal Register*. We have worked closely with our partner agencies in DHS, as well as DOT and other government agencies, to develop these important regulations. Our efforts have benefited from the recommendations of our industry partners provided both in writing and at public forums. As with all our homeland security initiatives, we look forward to working with all our partners on implementation of this historic rulemaking and encourage their comments as we prepare to further refine the requirements prior to publication of final rules this coming autumn.



Attack on New York

The First Response

by Capt. DANIEL R. CROCE

Governmental Public Affairs Officer; U.S. Coast Guard District 1 South

The movement of vessels and cargo through U.S. ports will forever be viewed differently as a result of the terrorist attacks on the World Trade Center on September 11. The U.S. Coast Guard, along with other government agencies and the shipping industry, has worked to improve the methods used to ensure safety and prevent terrorism while preserving the positive flow of commerce through the marine transportation system.

Through open communication, understanding and cooperation, mariners from all walks of life contributed to the continued flow of commerce and passengers through marine transportation in the Port of New York/New Jersey (NY/NJ) at a time of turmoil and chaos.

Immediately after the terrorist attacks on the World Trade Center, Coast Guard Activities New York (ActNY) directed the waterborne evacuation and rescue of approximately 350,000–500,000 civilians from Manhattan Island. All mass transit, including bus and rail terminals, was immediately shut down. Bridges and tunnels were closed to vehicular traffic and to subways over certain bridges. The only way out of New York City was to walk, or by boat.

In the critical hours that followed, five Coast Guard cutters, 12 small boats, and more than 100 public and private vessels maneuvered around the waters off Manhattan to rescue people off the sea walls and

support the emergency response effort. Professional and heroic mariners from commercial ferries to tug boats came to the aid of those who fell or jumped into the waters off Battery Park during their attempt to escape the clouds of debris chasing them from the collapsing towers.

Coast Guard personnel were immediately dispatched to coordinate the evacuation of Manhattan. The Sandy Hook Pilots volunteered their pilot boat *New York* to serve as an on-scene waterway command post with Coast Guard personnel onboard. Coast Guard marine inspectors and investigators from ActNY boarded ferries to ensure order and safety. The knowledge and experience of the Coast Guard and the local pilots enabled them to provide critical direction via VHF radio to facilitate an orderly evacuation.

Civilian vessels operated in a rescue mode and were sailing in unfamiliar and confined areas, initially with little or no visibility. The Coast Guard's prompt establishment of vessel marshaling areas and the professional actions of the mariners onboard ferry, tug, charter fishing, marine police and fire boats, minimized the potential of vessel collisions and further injuries to the evacuees.

The first official order given by the Coast Guard Captain of the Port, Rear Adm. Richard E. Bennis, was for the closure of the Port of NY/NJ to all incoming and outgoing vessel traffic. Since the city was under attack and no one knew what was going

to happen next, the Coast Guard believed it necessary to take this extreme precaution.

ActNY established an Incident Command Center at the main Coast Guard base on Staten Island where 1,500 active duty, reserve, and auxiliary personnel from Coast Guard stations nationwide were called in for around-the-clock duty. Twenty-six additional Coast Guard cutters and small boats were deployed to New York Harbor from units throughout the Northeast to support this operation.

Coast Guard personnel also were assigned as liaisons to the mayor of New York's Office of Emergency Management (OEM), the New York Police Department, the Port Authority of New York and New Jersey, and the Federal Emergency Management Agency. In these positions, the Coast Guard worked jointly with all other federal, state and local law enforcement agencies through the various OEM offices in New York and New Jersey.

The joint forces formulated a working team that developed a good line of communication among the Coast Guard, FBI, Joint Terrorist Task Force, U.S. Customs Service, the Immigration and Naturalization Service, Port Authority Police, New York and New Jersey state marine police harbor units, U.S. Navy bomb squads, local, county and city police departments, and emergency response units. A multi-agency security work group was formed to meet with the port facility security managers to exchange pertinent information needed to ensure the safety of marine terminals around the port.

The Port of NY/NJ is the largest container port on the East Coast, with approximately 6,000 containers handled inbound and outbound daily. Following the closure of the port, the captain of the port was faced with two opposing missions: the protection of vulnerable and valuable targets, and the continuation of port commerce through the marine transportation system. To maintain a balance between the two, the port reopened on Sept. 13 to vessel traffic with the following restrictions in place:

- Access to security zones was only allowed with the permission of on-scene Coast Guard assets;
- Recreational vessel traffic was restricted to weekdays from 8 a.m. to 4 p.m. with a maximum speed of 10 knots in major waterways, and no recreational vessel traffic was permitted on restricted waterways;
- Passenger vessels carrying more than 50 passengers and operating in certain zones within the port were required to have a uniformed security person onboard;
- Commercial vessel movements were allowed only with proper Coast Guard approval;
- All vessels were boarded at



Tug boats at Battery Park evacuate people from Manhattan to New Jersey, Staten Island, Brooklyn and Queens. Photo by Public Affairs Officer Brandon Brewer, USCG.

sea by a Coast Guard law enforcement boarding team and marine inspectors.

Vessels over 300 gross tons, especially foreign-flagged vessels, had many other restrictions imposed upon them. Before entering port, the following requirements had to be fulfilled:

- The vessels were required to enter the port via Ambrose or Sandy Hook Channel only;
- The vessel or agent had to provide the advance notice of arrival to the local Coast Guard office in New York 24 hours prior to arrival at the sea buoy;
- A certified copy of the crew list, including the nationality of the crew, had to be provided;
- The vessel could not enter port until it had been satisfactorily inspected by a Coast Guard boarding team;
- The vessel was required to have a pilot onboard;
- The vessel was required to have a two-tug escort when transiting in the harbor less than 1 nautical mile south of the Verrazano Narrows Bridge or the Outerbridge Crossing, with a speed restriction of 8 knots.

The vessel's agent had to confirm that the vessel's berth was ready to receive the ship and provide the names of the escort tugs prior to the vessel's entry. Anchorages were either closed or restricted to lightering operations. No bunkering was allowed at anchorage.

To keep the local port community informed and involved in port operations and changes, the Coast Guard, the Port Authority and the Harbor Safety,

Navigation, and Operations Committee of the Port of NY/NJ coordinated outreach meetings to provide information on the status of the port and to listen to their questions and concerns. These meetings opened a good line of communication among all agencies and companies involved with restoring efficient marine transportation in the port.



A man waiting to evacuate Manhattan crawled out on a ledge at the Staten Island Ferry Terminal about an hour after the World Trade Center towers collapsed. Photo by Public Affairs Officer Brandon Brewer, USCG.

Rapid dissemination of information to the port stakeholders concerning vessel movements and restrictions was vital during the first hours and days after September 11. To facilitate this, ActNY's Waterways Management Division developed a single consolidated Traffic Management Plan (TMP). They used an Internet-based "burst fax" service to notify 3,000 port community recipients simultaneously of the TMP changes. This information was also made available online.

Another Coast Guard mission affected by the terrorist attacks was the Container Inspection Program. The Coast Guard has always inspected containerized cargo carrying hazardous materials, but with the realistic threat of a weapon of mass destruction or a dirty bomb entering the port through such a container, the Coast Guard, Customs, and the Port Authority needed to rethink how to handle container inspections.

Therefore, immediately after September 11, additional Coast Guard container inspectors were brought to New York to increase the inspection volume. Containers were inspected not only to ensure the proper loading of hazardous materials and to assess the condition of the container, but also were inspected depending on the country of origin or the port through which they were trans-shipped.

Containers targeted for inspection were put through mobile or stationary Vehicle and Container Inspection Systems (VACIS), located throughout the port, prior to being examined or opened for inspection. A VACIS is an X-ray machine large enough to handle a container. The Coast Guard and Customs conducted these container inspections by forming teams dispatched daily to perform joint inspections throughout the port. This was a better use of manpower and improved productivity; up to 500 containers were physically inspected each day. Throughout the various operational and procedural changes necessitated by the attacks, the Coast Guard worked closely with the Port Authority and the maritime community through the Harbor Safety, Navigation, and Operations Committee of the Port of NY/NJ to establish a new normalcy in continuing marine operations in the port. Consequently, many of the new vessel movement restrictions had been modified or were lifted as the Coast Guard and its partners gained a better understanding of potential threats and how to prepare for them.

The 24-hour notice of arrival to port was extended to 96 hours. This regulation requires certain pre-arrival information to be phoned, faxed or e-mailed to the centralized National Vessel Movement Center. Two reasons for this requirement were: (1) To gather the appropriate information about an incoming vessel in enough time to perform the proper investigative/background checks on the crew; and (2) To determine if a vessel boarding is necessary and if so, to complete this as expeditiously as possible so as not to delay the vessel's entry into the port.

Targeted high-interest vessels are required to have a Coast Guard sea marshal onboard during transit into port. No vessel will be screened or permitted to enter the port unless a certified crew and passenger list is submitted, and the 96-hour notice requirement is met and verified through the Ship Arrivals Notification System database by the Coast Guard Port State Control Arrivals Desk watchstander.

Throughout this time, the Coast Guard worked closely with the Port Authority and the Harbor Safety, Navigation, and Operations Committee of the Port of NY/NJ to continue the marine operations in the port. Amongst the confusion from relocations of displaced personnel who lost offices at the World Trade Center and the sadness of the loss of life of co-workers, all concerned continued to move forward. They reached out to the port community and to federal government officials to gather information and provide input into the newly developing maritime security regulations.

Today, Coast Guard personnel onboard cutters, aircraft, boats and vehicles remain on aggressive watch, patrolling domestic ports and coastlines to provide an offshore security presence in their important role of homeland security and enhanced maritime domain awareness, and continue to contribute to evolving maritime security regulations while working together with our interagency partners under the new Department of Homeland Security.

Tugboats, ferries and Coast Guard vessels evacuate people from Lower Manhattan on September 11. The Coast Guard Battery Park Building is at the far right. Photo by Public Affairs Officer Bob Laura, USCG.





A Family of Security Plans

by Lt. KEVIN ODITT
U.S. Coast Guard Office of Port, Vessel, & Facility Security

More than 95 percent of our foreign trade passes through our marine transportation system (MTS). Our MTS consists of more than 1,000 harbor channels, 25,000 miles of inland, intra-coastal, and coastal waterways, and more than 3,700 terminals at over 350 seaports located throughout the country. Waterborne cargoes include nearly 2 billion tons of freight and 3 billion tons of oil. Maritime commerce contributes nearly \$1 trillion to our nation's gross domestic product. As the economy of the 21st century becomes increasingly globalized, the safe, secure, and efficient operation of our MTS becomes ever more important to our nation's economic well-being as well as our national security.

September 11 exposed numerous national security shortcomings. To ensure our enormous MTS infrastructure is adequately protected from disruption by those hostile to our country, the Coast Guard has re-energized its port security role.

This article provides a brief background on the U.S. Coast Guard's historic role in port security and highlights many of the actions we're taking to improve our ability to detect, deter, and disrupt terrorist or other unlawful activities that are detrimental to the safe and secure operation of our MTS. Central to our port security regime is the "Family of Security Plans" concept.

Background

Port security has long been a responsibility of the Coast Guard. This responsibility has been

addressed in a number of U.S. laws. The Magnuson Act of 1950, amended by Executive Order 10173, clearly established the Coast Guard's role in port security. The Ports and Waterways Safety Act of 1972 reaffirmed the Coast Guard's authority and responsibility. These existing authorities provide the Coast Guard with the legal foundation to address today's MTS security challenges.

September 11 re-awakened the nation to the reality that we are not isolated from world events, and our critical transportation infrastructure, including our MTS, is vulnerable to terrorist attacks. However, concerns about MTS security shortcomings were raised prior to September 11, most notably in the August 2000 "Report of the Interagency Commission on Crime and Security in U.S. Seaports." The report identified our ports, waterways and coastal areas as being particularly vulnerable to a broad range of criminal activity. Indeed, the Coast Guard, along with our other federal, state and local law enforcement partners, has for many years been engaged in drug and illegal migrant interdiction efforts. Similarly, the Coast Guard has partnered with a diverse array of port stakeholders to improve MTS safety through vessel traffic control schemes, safety zones and other initiatives aimed at improving harbor safety. The terrorist attacks of September 11 have compelled the Coast Guard to re-evaluate and strengthen our abilities to protect the nation's ports, waterways, and coastal areas from possible attack.

Direction

In December 2001, the Commandant reaffirmed the Coast Guard's maritime homeland security mission. The mission is to work in coordination with the Department of Defense (DOD), federal, state, and local agencies, owners and operators of vessels and maritime facilities, and others with interests in our nation's MTS to detect, deter, prevent, and respond to attacks against U.S. territory, population, and critical maritime infrastructure by terrorist organizations. The Commandant defined five goals of the mission to include:

- build maritime domain awareness (MDA);
- ensure positive/controlled movement of high-interest vessels;
- enhance presence and response capabilities;
- protect critical infrastructure and enhance Coast Guard force protection; and
- increase domestic and international outreach.

The Coast Guard is also listening to the public, Congress, and the international maritime community. In January 2002, the Coast Guard held a public workshop in Washington, D.C., that included more than 300 individuals including members of the public and private sectors, port, facility, and vessel security workgroups, and members of the international marine industry. They collectively expressed the urgent need for security planning and uniformity in the application and enforcement of requirements.

In addition to the January 2002 public workshop, the Coast Guard held seven public meetings across the country from January 27, 2003 to February 11, 2003. During these meetings the Coast Guard discussed requirements for security assessments, plans and specific security measures for ports, vessels, and facilities. These discussions helped to aid the Coast Guard in determining the types of vessels and facilities that pose a risk of being involved in a transportation security incident.

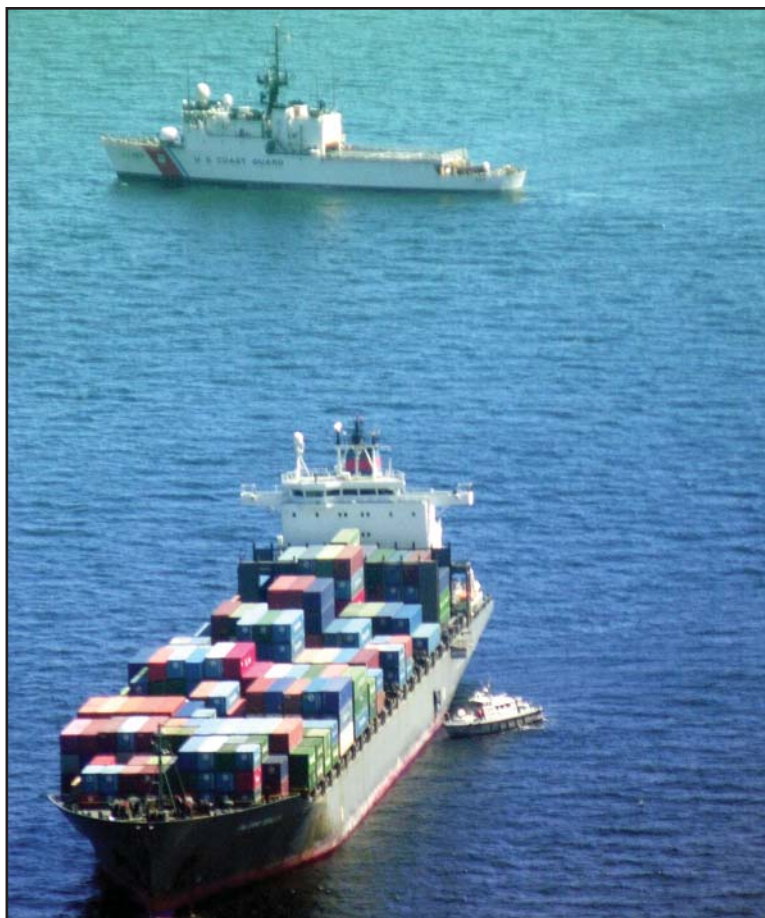
On November 25, 2002, President Bush signed into effect Public Law 107-295, the Maritime Transportation Security Act (MTSA) of 2002. MTSA's key requirement is to prevent a maritime transportation security incident (TSI)—defined as any incident that results in a significant loss of life, environmental damage, transportation system disruption, or economic disruption to a particular area. Preventing incidents has long been a core Coast Guard mission and the MTSA has empha-

sized our security specific mission and given us even broader authorities to implement it.

MTSA is a tremendously significant piece of legislation. It will fundamentally change the security culture of the entire maritime community, both domestically and internationally. It aligns with the new International Ship and Port Facility Security Code (ISPS) because the congressional staffs developed it with input from the Coast Guard (which serves as U.S. lead to the International Maritime Organization [IMO]).

Some of the areas addressed by the MTSA include: requiring vessel and facility security plans; establishing seaport security committees; requiring port vulnerability assessments; and periodic exercising of port security plans.

Maritime security is an international responsibility. The IMO has recognized the need to address and establish appropriate measures to enhance the security of ships and of port facilities. It has amended the Safety of Life at Sea (SOLAS) Convention by



The Coast Guard Cutter *Escanaba* enforces a security zone around the M/V *Palermo Senator* as a small boat carrying a multi-agency inspection team approaches the cargo ship six miles off the New Jersey shore. Photo by Public Affairs Officer Eric Hedaa, USCG.

adding, among other things, a mandatory “Ship and Port Facility Security Code” for the purpose of enhancing maritime security.

The “Family of Plans” Concept

Maritime security protocols must encompass the entire MTS. All aspects of the port, its infrastructure, its geographic and strategic value, and its use by the public and private sectors must be considered when strategies are developed to protect it from attack. Strategies must be appropriate for normal working conditions as well as when security threats arise. Traditional port infrastructure, such as passenger terminals, commercial vessels, anchorages, and waterfront facilities, must be included, as well as those assets not typically addressed in existing regulations, such as public park areas on the waterfront, other transportation infrastructure supplying waterfront areas, power supply infrastructure, and uninspected commercial and recreational vessels. The MTSA will provide the first national, wide-ranging security planning requirements for all modes of transportation converging at a seaport. In anticipation of the MTSA being approved, the Coast Guard had already provided a framework for implementing a comprehensive plan that is aligned with the expectations set out in the MTSA. Similar to the model that was used to construct the national pollution response plan, the framework of this plan will require a “family” of interrelated security plans. The Port Security Plan, Facility Security Plan, and the Vessel Security Plan will be interrelated and united to form a comprehensive set, or virtual “family,” of plans. Each set of plans would be developed by the public or private entity most responsible for implementation.

What is a Security Plan

The purpose of security plans is to provide a framework to communi-

cate, identify risks, and coordinate resources to mitigate threats and consequences. Each plan must address the four principles of homeland security: awareness, prevention, response, and consequence management. Each security plan will be based on a security assessment and will document the following elements:

- designation of security responsibilities and duties;
- performance standards for training and exercising;
- establishment of protective measures to identify and take preventive measures against security incidents; and
- measures to ensure appropriate response and consequence mitigation actions.

All plans must provide for coordinated scalable actions to detect, deter, prevent, and respond to threats at varying threat levels. The Coast Guard has established Maritime Security (MARSEC) levels 1, 2, and 3 to describe increasing threat levels and

corresponding activities to meet the threats. MARSEC will be linked to the Homeland Security Advisory System (HSAS) and will serve as the maritime sector’s tool for communicating threats.

Port Security Plan

The Captain of the Port (COTP) will be responsible for establishing port security committees (PSC). The main goals of the PSC under the leadership of the COTP will be to develop, coordinate, and evaluate the port security plan (PSP). Port security committees may be security subcommittees of existing harbor safety committees or have port readiness committees as subcommittees. A PSC can be developed by the COTP as best fits the needs of the port community. Port security committees will bring together marine



Lee Christopherson, of Vessel Traffic Service (VTS) Puget Sound, Wash., plots a vessel's position—part of an international cooperative traffic system governing the Straits of Juan de Fuca by both the American and Canadian VTSS.

transportation system representatives in port areas with the specific objective of maritime homeland security (MHLS).

The COTP will work with Coast Guard units (including groups, stations, and air stations), DOD, federal, state and local agencies, and owners and operators of vessels and facilities, and other MTS stakeholders, including port authorities, service providers, labor, and recreational boating communities to develop a PSP. The PSP is the document that provides the framework for detecting, deterring, disrupting, and responding to MTS threats.

The PSP would not replace existing contingency plans like area contingency plans or other response plans. However, these existing contingency plans could be modified to account for new or additional security requirements in the PSP. The PSP is a coordination tool for the port community and must be available to all of the appropriate law enforcement and port agencies with port security responsibilities. The PSP will be developed by the PSC to complement other security plans. PSPs will also be used to satisfy the evolving international port facility security requirements for ports receiving certain ships on international voyages, which was finalized in December 2002.

The Coast Guard has already begun overseeing security assessments of selected port areas. These port security assessments will result in a comprehensive report that includes an assessment of port vulnerabilities, impact analysis of damage/loss to critical port assets, interdependencies of critical port assets, recommendations for mitigating vulnerabilities, and other information pertinent to the development of the PSP.

Facility Security Plan

All facilities will be responsible for developing and implementing facility security plans. In addition to addressing the security needs of the facility, they must also address the coordination and interface of security initiatives with both the port and vessel security plans. As mentioned earlier, the facility may be the only link between the vessel and the port.

Currently, IMO is working on security requirements for facilities that receive vessels on international voyages. These requirements would mandate security assessments and facility security plans for these facilities. It is measures such as these that will increase the level of security and awareness worldwide.



Assets not typically addressed in existing regulations, such as public park areas on waterfronts, must be included in the MTS family of plans concept. Copyright © 2003 USCG and its licensors.

Vessel Security Plan

The security of vessels is an emerging concern. Their operations provide a target of opportunity for those desiring to do harm to the interests of the United States. Owners and operators of vessels have the primary responsibility for ensuring the physical security and safety of their vessels.

The Coast Guard has been working both domestically and internationally to implement requirements and guidance for vessel security plans (VSP). With more than 7,000 different foreign ships calling on U.S. ports, it is essential that an international standard for VSP be developed and implemented. IMO is developing security requirements for all vessels required to comply with SOLAS. These security requirements would mandate that vessels perform a security assessment and develop and implement ship security plans.

A majority of vessels will be responsible for developing and implementing VSPs. Those vessels that are not responsible for implementing a VSP will be captured by the PSP. As has already been mentioned, a critical component of the VSP will be the coordination of its security initiatives with the facility and port security plans.

Conclusion

With our nation's reliance on maritime commerce, the Coast Guard has stepped up to provide the way forward to a safer and more secure MTS. As Coast Guard Commandant Adm. Thomas Collins stated, "We must do all we can to provide needed maritime security to ensure the freedom of our country, without endangering liberty itself. Obviously we can't do it alone. Despite our plans we have major gaps in capability now, which will probably remain well into the coming years...but we will press on to correct these gaps with a great sense of urgency." Together, the execution of the "family of plans" will enable the Coast Guard and maritime community to fill these gaps to ensure the security of the nation's MTS.



IMO Moves to Enhance International Maritime Security

by Cmdr. SUZANNE E. ENGLEBERT
U.S. Coast Guard Marine Safety, Security & Environmental Protection

While the United States rapidly implemented many measures after September 11 to enhance domestic maritime security, the Coast Guard concurrently achieved international security improvements through the International Maritime Organization (IMO). At a seemingly impossible pace by pre-September 11th standards, the U.S. delegation to the IMO created an aggressive plan to substantially tighten security throughout the world.

A Breakneck Pace at the International Level

In November 2001—merely two months after two commercial airliners collided with the World Trade Center buildings in New York—the IMO Assembly adopted resolution A.924 (22). The IMO adopted the resolution, Review of Measures and Procedures to Prevent Acts of Terrorism Which Threaten the Security of Passengers and Crews and the Safety of Ships, on the recommendation of the United States and numerous other nations, with the goal of significantly enhancing maritime security and maritime domain awareness. This resolution directed the organization to develop appropriate measures to increase maritime security.

By February 2002, the intersessional working group (ISWG) meeting of IMO's Maritime Safety Committee (MSC) drafted substantial amendments to the 1974 Convention of Safety of Life at Sea

(SOLAS) to enhance security. Additionally, the ISWG drafted a framework for a mandatory security code and guidance measures to prevent terrorism.

In May 2002, at the 75th session of IMO's MSC, several countries proposed the work of February's ISWG to the delegation. The MSC established a maritime security working group to discuss matters during the session. The working group made significant progress in developing a global maritime security infrastructure. Building on the concepts developed at February's ISWG, they developed a revised draft text of amendments to SOLAS Chapter XI and a new mandatory International Code for the Security of Ships and Port Facilities (ISPS). The committee approved the draft text and submitted it to the December 2002 Diplomatic Conference for adoption.

In September 2002, a second ISWG meeting was held. The goal of the meeting was to clarify issues from MSC 75 and further refine the proposed regulations and the ISPS Code. Another important aspect to the ISWG meeting was the further development of non-mandatory guidance in Part B of the ISPS Code for ships and port facilities. Significant progress was also made on the proposed amendments to SOLAS for port state control measures.

The Diplomatic Conference on Maritime Security: The Culmination of a Year of Intensive Work

From Dec. 9-13, 2002, the Diplomatic Conference was held. Representatives from 109 contracting governments to the SOLAS Convention attended the conference. United Nations specialized agencies, intergovernmental organizations and non-governmental international organizations also sent observers to the conference. Efforts in November 2001 and February, May and September 2002 refined a number of key items, leaving relatively few issues to be resolved at the conference itself.

Coast Guard Commandant Adm. Thomas Collins headed the U.S. delegation. Adm. Collins said the conference represented strong collective resolve in precluding a maritime parallel to the September 11 terrorist attacks. Noting that shipping was an international business and that terrorism is an international threat requiring long-term multilateral solutions, Adm. Collins told delegates that “the eyes of the world” were on the IMO member states as they responded to the urgent challenge to safeguard the physical and economic welfare of their citizens from the threat of terrorism.

On Dec. 13, 2002—just more than a year since the terrorist atrocities in September 2001—the conference adopted the SOLAS amendments, the most far-reaching of which is the ISPS Code. Given the pivotal role shipping plays in the conduct of world

trade, new international regulations are of crucial significance not only to the international maritime community but the world community as a whole.

Highlights of Adopted Measures

Amendments to SOLAS

In total, the Diplomatic Conference adopted 11 resolutions that will enter into force on July 1, 2004. Resolution 1 provided amendments to SOLAS.

Among other effects of the amendments, Resolution 1 created a new SOLAS chapter dealing specifically with maritime security. Don't be confused by the new numbering! The existing SOLAS Chapter XI, Special Measures to Enhance Maritime Safety, was renumbered as Chapter XI-1. A brand-new Chapter XI-2, Special Measures to Enhance Maritime Security, was added after the renumbered Chapter XI-1. The new SOLAS chapter contains the mandatory requirement for ships and port facilities to comply with the ISPS Code.

While not an exhaustive list, amendments to the SOLAS Convention included automatic identification systems; ship-to-shore alert systems; port state control; continuous synopsis record; responsibilities of various parties; threats to ships; and equivalent and alternative security arrangements.

Automatic Identification Systems (AIS)

The Conference adopted modifications to Chapter V, Safety of Navigation with overwhelming



IMO's headquarters in London. Photo courtesy IMO.

consensus. The Conference voted to accelerate the timetable for installation of shipboard AIS. Ships, other than passenger ships and tankers, will be required to fit AIS no later than the first safety equipment survey after July 1, 2004 or by Dec. 31, 2004, whichever occurs earlier.

Ship-to-Shore Alert Systems

The Conference adopted a requirement for ships to be equipped with a silent alert system to signal ashore that a security incident is occurring or imminent to facilitate coastal state response.

Port State Control

The SOLAS amendments covered both ships already in port and ships intending to enter port. They specified when port state control officers might verify that ships comply with SOLAS and ISPS Code requirements. They also allowed port state control officers to take appropriate measures in response to any deficiencies found, including denial of entry to, or expulsion from, port.

Continuous Synopsis Record

Ships will be required to maintain a continuous record of registry, ownership, operational control, etc. This will facilitate the ability of the port state control officers to assess the security-related risks posed by a ship.

Responsibilities of Various Parties

The amendments spelled out the responsibilities of administrations, ships, companies and port facilities to comply with SOLAS and the ISPS Code, including responsibilities to designate security officers and develop threat assessments and implement security plans, leaving the details to the ISPS Code.

Threats to Ships

This amendment detailed the responsibilities of the contracting governments regarding the security of ships traveling in their waters.

Equivalent and Alternative Security Arrangements

This provision allows contracting governments the flexibility to negotiate alternative security arrangements with concerned administrations, yet ensures the new SOLAS requirements are met.

Adoption of the ISPS Code

In addition to the above-mentioned Resolution 1, amendments to SOLAS, the Diplomatic Conference adopted Resolution 2: the ISPS Code. This Code:

- established an international framework involving cooperation between contracting governments, government agencies, local administrations and the shipping and port industries. These parties will cooperate to detect and assess security threats. They will also take preventive measures against security incidents affecting ships or port facilities used in international trade;
- established the respective roles and responsibilities of the parties at the national and international level;
- ensured that security-related information is collated and exchanged efficiently;
- provided a methodology for security assessments. Thus, plans and procedures will be in place to react to security levels if they change; and
- ensured confidence that adequate and proportionate maritime security measures are in place.



The head of the U.S. Delegation, Coast Guard Commandant Adm. Thomas Collins, told the IMO member states, “The eyes of the world” were on them.

When the ISPS Code is implemented, varying security levels will reduce the risk of a security incident. Security levels, set by government agencies, will be based on changes in threat. They will trigger the appropriate port and vessel security measures. Measures will be tailored to each independent vessel or facility depending on its risk of assessment and vulnerabilities.



IMO Secretary-General William A. O'Neal addressing the IMO Assembly in November 2001, in which it adopted Resolution A.924 (22)–Review of Measures and Procedures to Prevent Acts of Terrorism Which Threaten the Security of Passengers and Crews and the Safety of Ships. Photo courtesy IMO.

Part A of the ISPS Code contains mandatory provisions, while Part B contains non-mandatory guidance. Highlights of the ISPS Code include setting security levels; port facility, company and ship security officer responsibilities and qualifications; control measures; international ship security certificates; a Declaration of Security; contents of port facility and ship security plans; and recognized security organizations.

Setting Security Levels

The ISPS Code defined three security levels: normal, heightened and exceptional. Provisions of ship and port facility security plans must contain specific measures to achieve the different security levels without undue delay.

Port Facility, Company and Ship Security Officer Responsibilities and Qualifications

This specified the duties and qualifications of security officers.

Control Measures

This elaborated on control provisions of the SOLAS amendments by spelling out grounds for determining when a ship is not in compliance with the applicable regulations. It also expanded control and compliance measures to include expulsion from port and denial of port entry.

International Ship Security Certificates

Administrations will issue certificates to ships that

comply with the SOLAS regulations and ISPS Code.

Declaration of Security (DOS)

A DOS ensures that security is seamless between the ship, the shore and other ships. This tool is used when clarification of responsibilities is needed for multiple parties that implement SOLAS regulations. The ISPS Code provided guidelines for when a DOS can be requested.

Contents of Port Facility Ship Security Plans

Part B in particular provided considerable detail on the types of issues that should be covered by security plans and included the assessments used to develop the plans.

Recognized Security Organizations

The ISPS Code specified the tasks contracting governments may designate to recognized security organizations and laid out substantial competencies to ensure a high minimum standard.

Other Adopted Resolutions

In addition to the adoption of amendments to SOLAS (Resolution 1) and the ISPS Code (Resolution 2), the Conference adopted the following additional resolutions. These resolutions reinforce SOLAS amendments and persuade ports and vessels not specifically incorporated by the Code to apply many of the new security measures.



IMO Assembly members sign the final act of the Diplomatic Conference on Maritime Security Dec. 13, 2002. On this day the members adopted the SOLAS amendments. Photo courtesy IMO.

Resolution 3 provided for IMO preparation of an impact assessment of long-range ships' identification and tracking, the development of performance standards and guidelines (if found necessary) and training and guidance on ship and port security. It also called for the review of existing IMO resolutions on port state control procedures, safe-manning principles and the prevention of drug smuggling; ships' security when interfacing with floating production storage units; facilitation of maritime traffic (in the context of security); and guidance on control and compliance measures not covered by the ISPS Code.

Resolution 4 provided for future amendments to Chapter XI of SOLAS without the prior requirement to convene a diplomatic conference.

Resolution 5 called for increased assistance to developing countries to fund security-related expenses. It also asked the Secretary General to consider the feasibility of establishing a Maritime Security Trust Fund.

Resolution 6 urged SOLAS party governments to quickly ratify the amended Convention and to meet security plan and certification requirements in advance of July 1, 2004. The resolution points out that extensions are not authorized for the implementation dates of the maritime security measures, and recommended that contracting governments develop certification processes for vessels and port facilities prior to the July 1, 2004 implementation date to alleviate any non compliance issues.

Resolution 7 encouraged governments to establish suitable procedures to increase security to vessels and facilities not covered by Chapter XI-2 of SOLAS, such as mobile offshore drilling units and fixed and floating platforms.

Resolution 8 called on the International Labor Organization to continue its work on seafarer documents as a high priority issue.

Resolution 9 invited the World Customs Organization to act quickly on issues such as the security of international movements of closed container transport units.

Resolution 10 called for prompt member-country action to implement long-range identification and tracking of ships, including the measures necessary to prepare for automatic response to INMARSTAT C polling and other existing satellite systems.

Resolution 11 emphasized humanitarian concerns, such as shore leave for crewmembers, and encouraged Convention parties to report instances in which implementation of Convention or the ISPS Code provisions impact negatively on seafarers' welfare.

Since shortly after September 11, the Coast Guard was an integral part in enhancing maritime security worldwide. From November 2001 to December 2002, the rapid adoption of the SOLAS amendments and the ISPS Code demonstrated impressive international cooperation at the UN specialized agency. The SOLAS amendments and ISPS Code complement provisions in the recently enacted U.S. Maritime Transportation Security Act and will facilitate U.S. implementation of that legislation in an internationally agreed manner. The entire maritime community now has an aggressive plan to substantially tighten security throughout the world.

All amendments to SOLAS and the text of the ISPS Code can be found at IMO's Web site, www.imo.org.



U.S. Enacts Measure for Maritime Security

by Cmdr. STEVEN D. POULIN
Legal Advisor; U.S. Coast Guard Port Security Directorate (G-MP)

On Nov. 25, 2002,

President Bush enacted the Maritime Transportation Security Act of 2002 (MTSA). This legislation requires the Secretary of the U.S. Department of Homeland Security to implement regulations that provide a comprehensive aegis for maritime security. The vast majority of the Secretary's maritime security authorities and responsibilities will be delegated to the Commandant. The U.S. Coast Guard is the primary federal agency developing these regulations and will similarly have primary enforcement responsibility for them. The Coast Guard's regulatory efforts are supported by close partnerships with the Border and Transportation Security Directorate (Transportation Security Administration and the Bureau of Customs and Border Protection) and the Department of Transportation (Maritime Administration). The regulations will not only carry out the intent of the key security provisions of the MTSA, but also will generally reflect the new international maritime security requirements recently adopted in December 2002 by a diplomatic conference convened under the auspices of the International Maritime Organization (IMO). (See related article, page 14.)

Among other requirements, the regulations will compel regulated vessels and facilities to conduct security assessments and to develop detailed

security plans to address vulnerabilities revealed by those assessments. Except where international obligations otherwise dictate, the assessments and security plans must generally be submitted to the Coast Guard for approval. The regulations also will contain requirements for the designation and competency of security personnel, including standards for training, drills and exercises. The regulations will further establish the framework for area maritime security committees to assist the captains of the port, as the local federal maritime security coordinator, in conducting area security assessment and developing area security plans. These plans will have to support and be consistent with a National Maritime Transportation Security Plan that provides the overarching strategy for protecting the marine transportation system. This "family of plans" approach establishes a layered system of protection that involves all maritime stakeholders.

The IMO diplomatic conference adopted significant changes to the International Convention for the Safety of Life at Sea, 1974 (SOLAS), primarily a new Chapter XI-2 containing enhancements for maritime security and a complementary International Ship and Port Facility Security (ISPS) Code. The ISPS Code contains a mandatory Part A and recommendatory guidelines in Part B. The SOLAS amendments and the ISPS Code will come into force July 1, 2004, through the tacit amendment



Boarding team members of the Coast Guard Cutter *Thetis* conduct a boarding on a high-interest vessel while at sea.

process for all contracting parties to SOLAS, of which the United States is one. These internal instruments are an important achievement for two reasons. First, the new requirements were adopted by more than 100 nations at the diplomatic conference, with IMO member states negotiating them from concept to reality in a little more than a year's time. Second, the SOLAS amendments and ISPS Code provide remarkable detail regarding the recommendatory measures and guidelines that must be taken into account in meeting the required performance standards.

As the SOLAS amendments and ISPS Code were being negotiated at IMO, Congress was developing the MTSA. The MTSA is a diverse piece of legislation. It passed unanimously by voice vote in the Senate and without object under suspension of the rules in the House of Representatives, indicating its broad bipartisan support. Title I of the Act addresses the new requirements and standards for enhancing maritime transportation security. Title II contains maritime policy improvements, mostly waivers of cabotage and coastwise trade restrictions

as well as vessel-specific exemptions for certain statutory and regulatory requirements. Title III includes many new authorities to improve Coast Guard personnel practices, as requested by the Administration, extensions of advisory committees, and numerous authorities supporting Coast Guard operational programs. Title IV of the Act similarly contains a range of additional authorities and congressional directives regarding Coast Guard administrative and operational activities, including certain reporting requirements. Title V contains the traditional Coast Guard authorization provisions setting year-end personnel strengths, training targets and funding levels.

The Title I provisions are the most referenced when discussing the MTSA. Section 102 of that title, which is codified at 46 U.S.C. Chapter 701, contains the key domestic maritime security requirements. In passing the MTSA, Congress made an express finding that it is in the "best interests of the United States" to adopt and implement the IMO instruments because they contain the "essential elements" for enhancing global maritime security. The SOLAS

amendments and the ISPS Code generally align with the requirements of 46 U.S.C. Chapter 701 and will be the mechanism by which the statutory requirements are implemented. 46 U.S.C. Chapter 701 does not prescribe a precise regulatory timeline. However, the MTSA does establish certain regulatory benchmarks based on the promulgation of an "interim final rule." The term "interim final rule" is a misnomer and should more properly be labeled a "temporary interim rule." The temporary interim rule must be promulgated "as soon as practicable" (emphasis added). The MTSA waives the Administrative Procedure Act (APA) for this purpose, indicating the importance Congress attached to promulgating meaningful security requirements as soon as possible.

The new international maritime security requirements enter into force on July 1, 2004, with the exception of the requirements for installation of an automated identification system and a ship security alert system. Working backwards from the SOLAS and ISPS Code entry into force date, and applying the benchmarks in 46 U.S.C. Chapter 701, the Coast Guard intends to issue the temporary interim rule no later than July 1, 2003. The temporary interim rule expires on Nov. 25, 2003 (12 months after enactment of the MTSA). The final rule implementing 46 U.S.C. Chapter 701 must be published by that date to ensure the continuity of enforceable requirements. However, the APA waiver does not apply to the final rule, suggesting

it must be promulgated with a 30-day delay in effective date. Simply, the Coast Guard must target Oct. 25, 2003 for publication of the final rule.

Where applicable, vessels and facilities have to submit their security plans to the Coast Guard by January 2004, giving the Coast Guard until July 1, 2004, to approve those plans. For foreign vessels required to comply with SOLAS, consistent with U.S. treaty obligations, the Coast Guard intends to accept flag administration approval of a ship security plan as meeting the review and approval provisions of 46 U.S.C. Chapter 701, provided the security plan meets the requirements of SOLAS and Part A of the ISPS Code, having fully applied the relevant provisions of Part B of the ISPS Code. To further ease the administrative burden of plan approval and provide additional flexibility for the maritime industry, while at the same time ensuring enhanced security mandated by 46 U.S.C. Chapter 701, the Coast Guard also intends to permit the use of approved industry alternative plans. For example, owners and operators of vessels or facilities that are similar in design and operation may be able to submit a single plan to the Coast Guard for approval. If approved, the owner and operator may implement the plan for a specifically identified fleet of vessels or facilities. The Coast Guard is further considering the use of industry model plans, whereby a particular industry can petition the Coast Guard for permission to use a plan that would apply to a particular segment of industry.

Editor's Note - Security Rules Published July 1, 2003

The Maritime Transportation Security Act Temporary Interim Rules were published July 1, 2003. The comment period for the rulemaking closed July 31, 2003. The regulations may be reviewed on the Federal Register Web site: www.access.gpo.gov/su_docs/fedreg/a030701c.html. Scroll down to "Coast Guard" where you will find links to the six rules and the AIS notice.

The regulations, together with comments from the public, may also be accessed through the Internet on the public docket at [HTTP://DMS.DOT.GOV](http://DMS.DOT.GOV). When accessing the Docket Management System, the following docket numbers correspond to the listed parts of Title 33 of the Code of Federal Regulations:

Docket 33 CFR Part

- | | |
|-------------|--------------------|
| • 14792 101 | • 14759 106 |
| • 14733 103 | • 4757 AIS |
| • 14749 104 | • 14878 AIS Notice |
| • 14732 105 | |

Regulation 9 of new SOLAS chapter XI-2 describes the control and compliance measures to be taken by port states for a ship's non-compliance with the new international requirements. Given that more than 90 percent of the goods entering U.S. ports are carried aboard foreign-flagged vessels, this regulation is of critical importance. It contains two important prongs. First, it incorporates traditional IMO port state control practice. This traditional approach accepts and defers to the International Ship Security Certificate as validating the ship's

compliance with the maritime security requirements. Unless there are clear grounds for believing the certificate is invalid or the ship is not in compliance, the port state control officer may not conduct a further inspection of the vessel. However, where clear grounds do exist, the port state control officer may detain the vessel until the deficiency is rectified to the port state control officer's satisfaction.

The second prong expands port state control practice to allow control of the vessel outside of the port and specifically includes denial of port entry and expulsion from port as enhanced port state control mechanisms. The standard of clear grounds was retained as a threshold for exercising these enhanced port state control mechanisms. Moreover, in a departure from traditional port state control practice, clear grounds can be based on conditions exterior to the ship itself. For example, Part B of the ISPS Code permits port states to consider the non-compliance of a facility at which the ship called, or the non-compliance of another ship with which the ship subject to control had interacted, as factors in the port state control decision matrix. Even then, any control exercised under regulation 9 must be proportional to the threat posed by the ship. In cases where the ship has been unduly delayed or detained, the ship shall be entitled to compensation. However, the right to take actions when necessary for self-defense or national security, consistent with international law, is not constrained by the new port state control regime.

The Coast Guard will accept the International Ship Security Certificate as reflecting the ship's compliance with the new maritime security requirements, including the relevant requirements in 46 U.S.C. Chapter 701, provided the ship has fully applied the applicable provisions of Part B of the ISPS Code. Essentially, the Coast Guard will use Part B as the barometer for measuring compliance with SOLAS chapter XI-2 and Part A of the ISPS Code, and hence the regulation promulgated under 46 U.S.C. Chapter 701. If a ship has not implemented one of the prescribed measures in Part B of the ISPS Code, its security plan must have an approved alternative measure that achieves an equivalent level of security to meet the performance standards in Part A of the ISPS Code. At the 77th Session of IMO's Maritime Safety Committee, the United States is proposing that an optional mechanism be established for the flag administration to attest to the ship security plan's application of Part B of the

ISPS Code as a means of reducing the potential for delays to verify compliance.

46 U.S.C. Chapter 701 reinforces the port state control regime under SOLAS. For example, vessels or facilities located on or adjacent to waters subject to the jurisdiction of the United States that may be involved in a transportation security incident may not operate without an approved security plan more than 12 months after publication of the temporary interim rule. Furthermore, the Secretary is required to conduct assessments of foreign port security. If the Secretary, in consultation with the Departments of State and Defense, finds that a foreign port is not maintaining effective anti-terrorism measures, the Secretary may deny entry into the United States to any vessel arriving from that port or mandate that any such vessel implement additional security measures. Lastly, the regime established by 46 U.S.C. 701 and its implementing regulations is supported by potential civil penalties of \$25,000 per violation.

Neither the SOLAS amendments, the ISPS Code, nor the MTSA amends or alters the existing authority of the Coast Guard to control vessel movement under the Ports and Waterways Safety Act (PWSA) or the Magnuson Act. Under the PWSA, Coast Guard captains of the port can control the movement and operation of vessels subject to the jurisdiction of the United States when there is reason to believe that the vessel does not comply with conditions of port entry or any applicable law or treaty. There also is specific authority in the PWSA for the Coast Guard to take any measures necessary to prevent or respond to acts of terrorism. The Coast Guard's independent authority under the Magnuson Act is a delegation of national security authority to Coast Guard captains of the port. This authorizes captains of the port to control the operation of vessels in the territorial sea and internal waters of the United States when necessary to prevent damage or injury to vessels, harbors, ports and waterfront facilities from sabotage or subversive acts, or to secure the observance of rights and obligations of the United States. The PWSA and Magnuson Act authorities are typically exercised by imposing specific requirements on vessels and facilities through an order issued by the captain of the port or by establishing and controlling access through security zones. The PWSA and Magnuson Act also provide broad authority to take similar actions and impose necessary requirements on "public and commercial structures" and "waterfront facilities," respectively.

The PWSA and Magnuson Act are supported by severe civil and criminal sanctions for non-compliance. These will no doubt continue to be an important part of the Coast Guard’s toolbox for ensuring the security of the marine transportation system through the direct regulation of the maritime industry. The new authorities in 46 U.S.C. Chapter 701 cannot be considered in isolation, but rather as one element in the larger legal structure supporting the Coast Guard’s lead role for maritime security.

The key principles that guided the U.S. delegation’s negotiations at IMO will also influence the Coast Guard’s regulatory strategy. Primarily, the Coast Guard’s approach will balance the need for enhanced security with the free flow of commerce. To that end, the regulations will be risk-based by focusing on the vulnerabilities of those vessels and facilities that are likely to be involved in a transportation security incident. Additionally, the security measures outlined in the security plans will be structured to address escalating threat levels. Understanding that the activities and operations of vessels, facilities and ports are very diverse and that one size does not fit all, the regulations will further establish performance standards instead of prescriptive requirements to provide additional flexibility for the maritime industry. This ensures consistency and avoids the economic inequities that would result from disparate requirements. Alternatives will be allowed, provided they meet a level of security that is equivalent to the established performance standards. Finally, the regulations will avoid duplication or conflicts with the security initiatives of other federal agencies. The development of the regulations has been a model for interagency cooperation and coordination.

The regulations implementing 46 U.S.C. Chapter 701, the SOLAS amendments, and the ISPS Code will likely be the first step in an iterative regulatory process. Implementing the core maritime security requirements now paves the way for additional improvements that will come about through subsequent initiatives to improve identification credentials and processes, establish security training programs, and implement cargo and container initiatives to improve the security of the supply chain. The task is daunting, but enhanced maritime security is an “all-hands evolution.” Failure is not an option—the consequences are too high if we collectively fail to shore up the vulnerabilities plaguing the marine transportation system.

The Department of Homeland Security (DHS) developed the Homeland Security Advisory System (HSAS) to inform people of specific threat levels. The higher the threat condition, the greater the risk of terrorist attacks. These risks include both the probability of an attack occurring and its potential severity.

The Coast Guard sets Maritime Security (MARSEC) Levels that correspond to HSAS threat conditions. The HSAS threat conditions warn of potential threats, while Coast Guard MARSEC levels are security protection levels that correspond to specific actions to be taken to ensure the security of our nation’s ports and waterways. While MARSEC levels generally correspond with HSAS threat conditions, captains of the port may raise MARSEC levels in their respective port to address an immediate threat to the marine transportation system (MTS). The Coast Guard MARSEC levels are part of an international maritime protective system that was established because of the inherently global nature of maritime transportation.

The following chart shows how the Coast Guard aligns MARSEC protection levels with HSAS threat levels.

Homeland Security Advisory System (HSAS) Threat Conditions	Corresponding Coast Guard MARSEC Levels
Low = Green	MARSEC 1
Guarded = Blue	MARSEC 1
Elevated = Yellow	MARSEC 1
High = Orange	MARSEC 2
Severe = Red	MARSEC 3



Citizens Assist in Keeping the Watch

by Cmdr. PATRICK GERRITY
MSO Detroit

A key component of the U.S. Coast Guard's maritime homeland security mission is maritime domain awareness (MDA). MDA is achieved a number of ways: by gathering information through air, boat and vehicle patrols; by assessing intelligence; and by working with various port entities. A valuable yet relatively untapped source of MDA information are the thousands of citizens who work, recreate or live along our nation's waterways. To access the observations of our citizens, Marine Safety Office (MSO) Detroit created the "River Watch Program," a preventive law enforcement program modeled after the "Neighborhood Watch Program."

Though developed by MSO Detroit, the River Watch Program is supported by Detroit-area offices of the FBI, the Immigration and Naturalization Service (INS), the Border Patrol, U.S. Customs and the Michigan State Police. Therefore, not only is the U.S. Coast Guard a benefactor of information from our citizens, our law enforcement partners are, too. In addition, the agencies pool their talent to ensure the program stays active and their funding helps to pay for the cost of program materials. The goals of the River Watch Program include:

- Increasing waterfront surveillance
- Providing another means of deterrence
- Increasing public confidence
- Improving interoperability among agencies
- Enhancing overall security

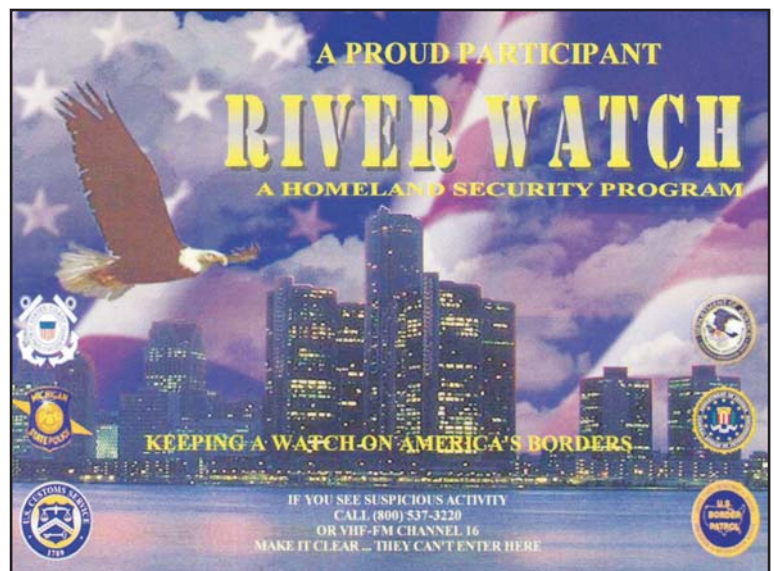


Image courtesy MSO Detroit.

Preventive law enforcement programs have long proven to be an effective tool in thwarting unlawful activity in participating neighborhoods. One of the primary reasons the program works is that it causes potential criminals to be uncertain about their detection. By implementing the River Watch Program we will not only get assistance from the public, but also cause uncertainty in the minds of potential terrorists and criminals.

River Watch participants receive program materials, which include a decal, a wallet card and a pamphlet. We expect citizens to affix the decal to the windows of their homes or businesses or to their vehicles or boats; it is our hope the decal sends

a message to anyone planning an untoward act in southeastern Michigan that people are watching! The wallet card contains the phone number and radio channel to use if suspicious activity is observed. The pamphlet provides basic information about the types of suspicious activities citizens should be alert to and areas on and along the water that we feel require extra awareness, such as bridges, marinas, and fueling facilities.

Each agency has agreed to provide information to a wide variety of organizations. The Coast Guard in southeastern Michigan has used various approaches to deliver River Watch Program materials to the public. MSO Detroit personnel have provided information to facility operators, commercial vessel operators and various industry groups. Coast Guard small boat stations have provided River Watch Program information to marinas; and the auxiliary has provided program information to boaters and to the public at boat shows. The River Watch Program has been adopted by every MSO in the 9th District and it is spreading to other districts. Each MSO has modified the program slightly to address specific geographic concerns, but the tenets of River Watch remain consistent throughout the 9th District. The River Watch Program is easily adaptable to other geographies, it's relatively inexpensive and so far we have found the public to be extremely eager to assist us in protecting the country from incidents of terror.

In May 2002 Air Station Detroit launched the River Watch Program during a media event. Among others, Sen. Carl Levin; Commander 9th Coast Guard District Rear Adm. Ronald Silva; and U.S. Attorney for the Eastern District of Michigan, Jeffrey Collins, spoke at this event. In addition, senior representatives from the Michigan State Police, the FBI, the INS, Customs and Border Patrol participated in the media event. Numerous federal, state and local law enforcement organizations were in the audience and the event was widely covered by a broad array of regional television, radio and newspaper reporters. By involving the public, MSO Detroit has expanded the source of its MDA information and is better able to keep the watch.

To obtain more information on the River Watch Program, contact MSO Detroit at (313) 568-9490.

Information Inside the River Watch Program Brochure

WHAT SHOULD I LOOK FOR?

For Recreational Boats:

- Fishing/hunting in locations not typically used for fishing/hunting
- Unattended vessels
- Unusual boat characteristics
- Any aggressive activities
- Unusual filming activity
- Unusual diving operations
- Recovering or tossing items into/onto the waterway or shoreline
- Unusual number of people onboard
- Lights flashing between boats and shore at night
- Frequent trips between borders

For Commercial Vessels:

- Operating/transiting in an area not typically transitted
- Anchored in an area not typically used as an anchorage area
- Unattended vessels
- Unusual vessel characteristics
- Any aggressive activities
- Filming activity
- Divers near vessel
- Recovering or tossing items into/onto the waterway or shoreline
- Unusual transfer of personnel or items while transiting
- Unusual night operations

Waterfront Facilities and/or Other Structures Including Bridges:

- Fishing/hunting in locations not typically used for hunting/fishing
- Suspicious activity
- Unattended vehicles in unusual locations
- Unusual vehicle characteristics
- Any aggressive activities
- Filming activity
- Divers entering water near facility or bridge
- Recovering or tossing items into/onto the waterway or shoreline
- Unusual night operations
- Observed security changes or lack of usually observed security
- Missing fencing, lighting, etc ...

Places of Particular Interest:

- Under and around bridges
- Around entrances to tunnels
- Near or around power plants
- Near or around water intakes
- Near or around oil facilities
- Near or around chemical facilities
- Near or around fuel docks
- Near or around military bases



New Security Measures in Mariner Credentials

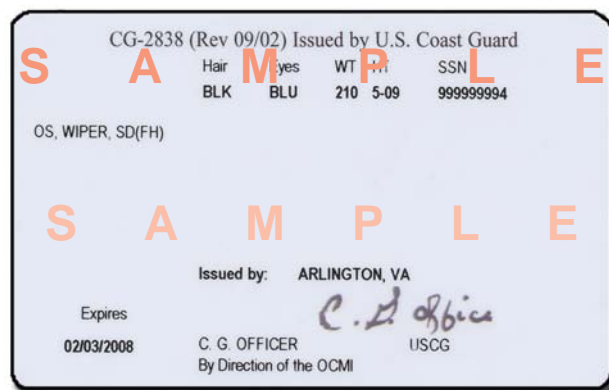
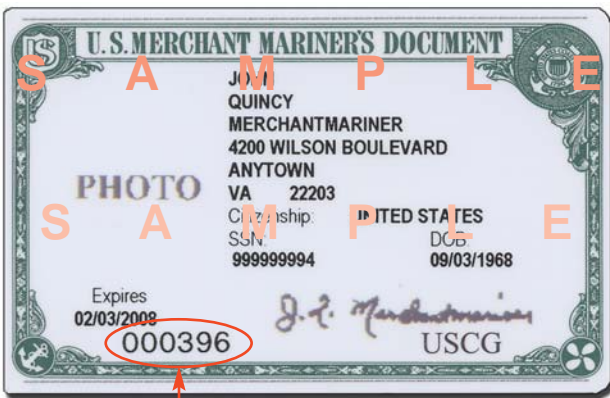
by Lt. Cmdr. TINA BASSETT
National Maritime Center

A Merchant Mariner Document (MMD) is a unique and important credential. It indicates a mariner's qualifications, serves as a photo ID, allows access to sensitive ports, and may serve as a passport in certain situations. After the terrorist attacks of September 11, the Coast Guard, along with other government agencies, looked for ways to improve the security and safety of U.S. citizens. The marine safety program recognized that there were problems in the mariner credentialing system that could result in fraud, and that an increased risk of marine safety incidents exists if unqualified persons obtain an MMD. Additionally, the potential for exploitation of these credentials by criminal or terrorist organizations is real and poses a threat to national security.

In response to these concerns, the Coast Guard began implementing new procedures designed to ensure MMD holders do not pose a safety or security threat. The Coast Guard is working within exist-

ing statutory authority to implement enhanced screening procedures for current MMD holders and applicants for original MMDs. Application procedures are essentially the same for the mariner, with the exception that renewals can no longer be completed entirely through the mail. Applicants must now appear in person at a Coast Guard Regional Exam Center (REC) sometime during the application process to provide fingerprints and prove their identity with two forms of government-issued identification, one of which must be a photo ID. Once mariners have completed this new process they will be issued a new, more secure and tamper-resistant MMD card that was being developed prior to September 11. These new cards, in turn, may someday be replaced by the high-tech Transportation Workers Identification Card (TWIC), which is a "smart card."

The Coast Guard is working closely with the maritime industry and individual mariners to



The front of this Merchant Mariner identification card (above left), displays an individual serial number in the lower left corner. This new card is being phased-in to the Coast Guard's new security process. This will be a replacement for cards that do not show a serial number.

implement these new changes smoothly and minimize any inconvenience. Additional staff is being added to 14 of the 17 RECs nationwide to help reduce the backlog of applications. A priority system has also been implemented to ensure that applications of mariners vital to our nation's military efforts and industry are processed as quickly as possible:

- Priority one is assigned to mariners who are, or are about to be, employed on a vessel directly involved with a military operation. A letter from the shipping company, labor union, ship management company, or government agency attesting to the ship's military purpose and the mariner's position is needed for this priority.
- Priority two is given to mariners who are actively sailing. Evidence of current or scheduled employment onboard a vessel, such as a letter or recent certificate of discharge, is needed for this priority.
- Priority three is for all other transactions based on date of receipt.

The Coast Guard encourages mariners to renew their documents well in advance to minimize the potential impact any processing delay may have

(regulations allow renewal 12 months prior to expiration). Submitting copies of identification and, if applicable, proof of Immigration and Naturalization Service status with the application (CG-719B) will speed the screening procedures. Additionally, applicants are urged to carefully and honestly consider their responses to questions in Section III of the application (Narcotic, DWI/DUI, and Conviction Record). Incomplete or incorrect responses in this section may cause significant delays and could result in denial of the MMD.

Currently, only mariners conducting normal transactions (renewal, upgrade, endorsement, or duplicate), and original applicants are receiving the new MMD card through the new process. At the time this article went to press, the Coast Guard had not made a determination on accelerating the replacement of all active MMDs. If that decision is reached, the Coast Guard will begin immediate outreach to mariners and industry.

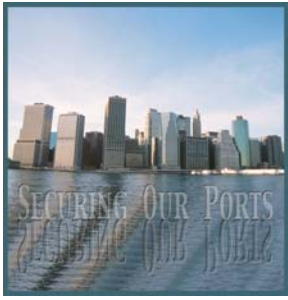
If you have additional questions, contact the National Maritime Center at the following address: Commanding Officer, USCG National Maritime Center (MMD Team), 4200 Wilson Blvd., Suite 630, Arlington, VA 22203-1804, (202) 493-6798. The NMC Web site is www.uscg.mil/hq/g-m/nmc/web/index.htm.

Before submitting your application, did you remember:

- Complete Sections I-V of the application – sign it!
- Sea Service (if applicable)
- Fees
- Medical examination
- Drug test or proof of enrollment in a program
- Two passport sized photos
- Proof of citizenship (and if applicable, INS status)
- Copies of identification

At the REC, remember to bring original or certified copies of:

- Two government-issued IDs; one must be a photo ID
- The IDs submitted with your application (if different from above)
- Proof of INS status (if applicable)
- You do not need to bring fingerprint cards; the Coast Guard will take your prints at the REC



Port Security Assessments

by Lt j.g. AARON DOWE
U.S. Coast Guard Office of Port Security Planning & Readiness

Background

“The federal government should establish baseline vulnerability and threat assessments for terrorism at U.S. seaports as soon as possible. Priority should be given to Strategic Seaports, Presidential Decision Directive 40 ‘Controlled Ports,’ and economically significant strategic seaports...”

Recommendation 7, Report of the Interagency Commission on Crime and Security in U.S. Seaports; Fall 2000

After more than a year of study, the Interagency Commission on Crime and Security in U.S. Seaports concluded what some involved with port security have believed for a long time—that U.S. ports are vulnerable to crime and terrorism. The Commission developed a long list of specific problems, including:

- No process for evaluating the vulnerabilities of seaports to terrorist attack;
- No minimum security standards or guidelines for seaports and their facilities; and
- Inconsistent coordination with non-law enforcement agencies and significant private entities.

To address these issues, the Commission recommended that the U.S. Coast Guard conduct vulnerability assessments and make those results available to all appropriate public and private entities. Additionally, the commission recommended creation of a “model port concept” that included “risk-based best practices for use by terminal and

vessel operators.” Covering a wide range of topics, from physical security, credentialing, and accreditation of private security, this product would serve as a framework for voluntary security improvements by private and public entities at the local level.

Efforts Before September 11

The current port security assessment (PSA) effort builds on two years of groundwork conducted by the Coast Guard’s Office of Waterways Security. The most significant part of this early effort was a joint Department of Defense/U.S. Coast Guard project to conduct vulnerability assessments on five militarily significant U.S. ports: Baltimore, Md.; Apra Harbor, Guam; Pearl Harbor, Hawaii; Charleston, S.C.; and Savannah, Ga. The Coast Guard provided port operations experience, and the Department of Defense (DOD), through the Defense Threat Reduction Agency (DTRA), provided technical expertise. This program employed a modified version of the Balanced Survivability Assessment (BSA)—a program designed to identify threats to significant military and civilian infrastructure from an attack by weapons of mass destruction (WMD).

This PSA methodology covered many of the issues of concern to marine transportation system (MTS) stakeholders and the reports it generated have become valuable post-September 11 assets. The captains of the port (COTP) involved endorsed this product and have provided feedback on ways to improve the process.



Petty Officer 2nd Class Walter Reilly boards a Hanjin motor vessel. Reilly is one of many inspectors at Group/MSO Los Angeles/Long Beach who have been working on the front lines by initially boarding all deep draft vessels that enter the ports of Los Angeles and Long Beach since the September 11 terrorist attacks. Photo by Petty Officer 2nd Class Daniel Tremper, USCG.

Coast Guard Port Security Program

Congress, recognizing the criticality of port security as an integral component of a more robust and terrorism-resistant transportation security environment following September 11, provided the Coast Guard the means to make urgently needed investments in the security of the nation's ports and waterways.

In the late fall of 2001, the Coast Guard undertook this challenge. Along with other efforts, the service initiated the Port Vulnerability Assessment program. Later, "vulnerability" was discarded in favor of "security"—which gave us the current title: Port Security Assessment (PSA) program. This

better reflects the program's broad objectives. Regardless of the name change, a look at the original mission statement leaves little doubt as to the program's direction and purpose.

"The mission of the Coast Guard PVA program is to make federal, state, and local governmental agencies and other appropriate port stakeholders aware of the susceptibility of maritime critical infrastructure and assets to negative consequences from intentional acts, accidents, and natural disasters, and to recommend mitigation strategies to protect the public, the environment, and U.S. economic interests as required for national security."

While simple in language, this statement allowed the Coast Guard to take the initial steps along a complex path that many envision will result in a measurable improvement in the security of the nation's maritime infrastructure.

An Overview of the Program

The PSA program rolled out as follows:

1. Developed a "Model Port" concept;
2. Selected a PSA contractor;
3. Built the Coast Guard PSA Oversight Team;
4. Conducted the assessments; and
5. Produced the final product.

Using expert input in the fields of physical security, vessel and facility operations, regulatory framework, crisis response and consequence management, a "model port" was developed and serves as the technical methodology to conduct in-depth assessment. As there are more than 360 ports operating in the United States, the ports were sorted by economic and strategic importance and a list of 55 ports to be assessed was developed. The second process, a streamlined and user-friendly version of a Port Security Self-Assessment Methodology, is under development and will be distributed to COTPs to assist them, and port stakeholders to assess, the roughly 300 remaining ports.

After both the detailed and self-assessment efforts, periodic reassessments of ports will be conducted as funding permits. These reassessments are tentatively planned for every three to five years.

Developing a "Model Port" Concept

Delivered in late July 2002, the final draft of "Security Attributes of a Model Port (SA/MP) was the first step in the PSA Program. Initiated in response to Recommendation 7 of the *Report of the*

Interagency Commission on Crime and Security in U.S. Seaports, this document will serve as a baseline from which other parts of the program can be judged and developed. It is intended to be a strategic document that incorporates security attributes to be used by members of the MTS community to balance the competing interests of improving security and maintaining economic viability, even in time of heightened security fears. Specifically, it provides a description of a port by mission, goals, objectives, and benchmarks. Where appropriate, it provides best practices to illustrate the kinds of practices captured by assessment teams.

The foundation of the SA/MP is a series of tables listing the overarching security-related mission and goals for a seaport, and security-related attributes of its associated systems. This information was compiled by a team of maritime transportation industry experts and various federal agency representatives, augmented by experts in physical security, information assurance, and counter-terrorism.

A dynamic document, the SA/MP will be updated periodically to take advantage of new information, practices, and procedures from a variety of sources. An important feature of future iterations will be an ever-expanding collection of best practices gleaned from PSA assessments and other sources. For the Coast Guard PSA program management team, the SA/MP will also serve as a basis for analysis of port security improvements and trends. By comparing the results of PSAs and other analysis over time, managers can take both a broad, holistic, look at ports and systems, or examine in more detail more specific performance areas.

Selecting a PSA Contractor

The Coast Guard did not have on-hand sufficient personnel with the specialized skills required to complete the security assessments. To augment their resources, a private contractor was hired to conduct the assessments for the nation's most commercially and militarily critical seaports. In April 2002, after a lengthy bidding process involving six strong candidates, TRW Inc. (now part of Northrup-Grumman Mission Systems) was selected to perform the assessments. Under the blanket purchase agreement, the contractor is:

- Developing "Model Port for Security" guidelines as recommended in the August 2000 *Report of the Interagency Commission on Crime and Security in U.S. Seaports*;



Coast Guard Port Security Unit members in New Jersey drill constantly around the country in Raider Boats in the event of being called to action. Photo by Public Affairs Officer Tom Gillespie, USCG.

- Developing methods for and conducting PSAs for up to 55 ports throughout the United States; and
- Developing a port security self-assessment methodology to help local COTPs and stakeholders evaluate security conditions and make improvements within their ports.

Building the Coast Guard PSA Oversight Team

To oversee this project in the field, the Coast Guard has established a Port Security Assessment Team (PSAT). Drawn from both the public and private sectors, and with a range of experience related to security, the marine industry, and other disciplines, this team is part of the Coast Guard's Directorate of Port Security and is located at the Coast Guard's offices in Arlington, Va.

Members of the PSAT will carry out a variety of functions. During the pre-assessment process, team personnel accompany the contractor's team leader to the ports to act as liaison with the local Coast Guard units and other port stakeholders to scope the port's various activities to frame the assessment effort. This single point of contact will facilitate assessment coordination and maximize local stakeholder participation. During the assessment activities team members provide a continuous line of communication with local Coast Guard units and

stakeholders and ensure the contractor teams are meeting the expectations of the contract. Once the contract team has compiled a port's PSA report, the PSAT is responsible for ensuring that the report is reviewed for completeness and for accuracy, and is then delivered to the entities that can benefit from the information it contains.

In addition to being assigned to oversee the contracted port assessments, members of the PSAT can also deploy as a full team to conduct assessments "in-house." Team members will also be working overseas conducting assessments at foreign passenger terminals, in support of OCONUS Combatant Commanders when requested, and in this country in support of other federal agencies with tasking in the maritime and critical infrastructure arenas.

Conducting the Assessment

Although the details in any given assessment must be adapted to address the specific characteristics of each port, all assessments will have the same basic parts, including:

- Port familiarization
- Pre-assessment
- Criticality assessment
- On-Site assessment
- PSA report

The first step in any assessment is a port familiarization, allowing the assessment team a basic understanding of the port and its activities. Additionally, this portion is used to allow officials in the port, including the COTP, local government, and industry to become familiar with the assessment process and the assessment team. Specifically, this involves gathering all available documents, conducting an overview of the physical and organizational layout of the port, establishing points of contact with stakeholders, and inviting their participation in the upcoming assessment activities.

During pre-assessment, a leadership team comprised of Coast Guard assessment team members and contract team members visits the port. Typically, this occurs four weeks before the on-site assessment. During this visit, the leadership team holds meetings with port stakeholders to provide an in-depth explanation of assessment process, schedule, and goals. Finally, arrangements are made to visit all selected facilities and infrastructure.



Identifying and prioritizing critical assets is completed using an advanced version of the Coast Guard's port security risk assessment tool. The COTP asks key stakeholders to provide assistance in identifying situations that could interfere with any of the following:

- The federal government's ability to perform essential national security missions and to ensure the general public health and safety.
- State and local government's ability to maintain order and to deliver minimum essential public services.
- The orderly functioning of the economy, commerce, and the delivery of essential telecommunications, energy, financial and transportation services.

Their input, combined with previously developed Coast Guard criticality data and any other locally conducted risk, vulnerability, security and safety assessments, is used to produce an overall picture of the port's critical infrastructure.

The major portion of the assessment process is carried out by a nine-member team comprised of Coast Guard liaison officers, the contractor team leader (usually a former Coast Guard COTP), and analysts in at least six disciplines including marine/port operations, operations readiness, physical security, structural/infrastructure security, anti-terrorism, and research/data capture.



The Coast Guard Port Security Assessment program focuses on a holistic approach to assessments when determining the susceptibility of the maritime critical infrastructure. Assessments of a port such as this one in San Diego help to recommend mitigation strategies to protect the public, environment and U.S. economic interest as required for national security.

During six to 14 days on-site, this team visits the assets identified earlier to determine possible vulnerabilities and the strategies to mitigate those vulnerabilities. This portion of the process also includes an evaluation of the security countermeasures in place. Local public service systems, such as water, electrical, communications, and other utilities, are also assessed. Finally, the federal, state, local, and private emergency preparedness and response capabilities (law enforcement, fire departments, emergency medical services, and hazardous materials response organizations) are quantified by evaluating manpower, training, and equipment levels. To accomplish all of these tasks, the team utilizes a mix of on-scene inspection and review of documents, maps and charts, and plans.

The final stage of the on-site assessment is the outbrief to the COTP and Harbor/Port Security Committee. The outbrief covers a list of the system elements assessed, infrastructure assessed, vulnerabilities found, and descriptions of any vulnerabilities that pose an immediate risk and should be corrected before the issuance of the final report.

Final Product

Once the field work is completed, the PSA Team returns home to organize, interpret, and process the data collected during the assessment into a comprehensive, integrated PSA report for distribution to

port stakeholders. At a minimum, the report contains:

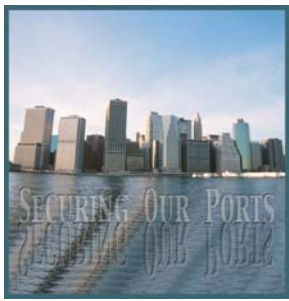
- An assessment of identified critical infrastructure vulnerabilities;
- An impact analysis of damage/loss to critical infrastructures and their supporting infrastructure;
- A description of interdependent critical infrastructures;
- Recommendations to reduce identified vulnerabilities; and
- Other information essential for the development of security contingency plans to mitigate the vulnerabilities.

Sensitive Security Information

Since portions of the report may be classified or are Sensitive Security Information (SSI), distribution of the full, unedited report is limited. It is also important to protect proprietary information. In an attempt to overcome these limitations, each PSA report has a standard format organized to facilitate easy separation of the report into classified and unclassified versions, and be easily customized to limit the information provided to the individual stakeholders. Therefore, as distributed, portions of these reports serve as a valuable tool to local port officials and an integral part of the Commandant's homeland security strategy.

Challenges Ahead

In some respects, dealing with ports as whole "ports" presents new regulatory and practical challenges for the Coast Guard. Regulations have traditionally been directed towards individual facilities, vessels, and operators based on public law and the Code of Federal Regulations. Yet the COTP has always had the job of maintaining the "big picture" of the port, while dealing with individual components as detailed in regulation. COTP Orders have dealt with issues both port-wide and facility/vessel-specific. Those traditional enforcement activities will continue, while new regulations will require many facilities and vessels to prepare their own security assessments, procedures, and response plans. Captains of the Port will be expected to deal with all their traditional duties, while maintaining a strategic and tactical situational awareness in the port—truly Maritime Domain Awareness in the first person—all under the watchful eye of citizens, industry, and a Congress with increased expectations of port security.



TSA Administers Grants for Port Security Improvements

by MARIANNA MERRITT

Director, Performance Standards & Management; Transportation Security Administration

Congress has appropriated special funds to implement many of the security measures that are necessary for the maritime industry under the Maritime Transportation Security Act. The Department of Defense Appropriations Act for fiscal year (FY)02 provided \$92.3 million in funding “for emergency expenses to respond to the September 11, 2001, terrorist attacks on the United States.”

In that legislation, Congress directed that the funds be dispersed for two grant categories: (1) security assessments and mitigation strategies, and (2) enhanced facility and operational security. It further stipulated that the funding is to be used for additional security activities not now being performed at the ports. Funds were provided to the undersecretary for transportation security. Since the Transportation Security Administration (TSA) was not yet fully staffed, the Maritime Administration (MARAD) and U.S. Coast Guard were designated to serve as agents of TSA for the award process. Department of Transportation guidance, under which TSA and the Coast Guard still operated at that time, stipulated that: (1) in addition to the assessment and enhancement improvement categories, 10 percent of the funds should be awarded to proof-of-concept projects; (2) preference should be given to ports/terminals that initiated security improvements after September 11; and (3) the awards would commence in June 2002.

Grant Team Guidance

The legislation imposed guidelines on eligible grant applicants and on each grant category. Eligible grant applicants were limited to critical national seaports, which included strategic ports, controlled ports, nationally significant economic ports (based on cargo flows) and ports or terminals responsible for movement of a high volume of passengers. Criteria for each category included the following:

- *Security Assessment category.* Awards were to be based on port or terminal assessments that identified vulnerabilities and proposed mitigation strategies.
- *Enhanced Facility and Operation Security category.* Ports were required to have a completed security assessment and offer security improvements in facility access control, physical security, cargo security or passenger security.
- *Proof-Of-Concept projects.* Projects were required to show how port security would be improved by implementation of the proposed changes.

The application period closed at midnight (EST) on March 28, 2002. More than 800 projects totaling nearly \$700 million were received. Five percent of the total funding was awarded for projects submitted under the Security Assessment category. Ten percent of the funding was awarded for proof-of-

concept projects and the remaining was awarded for enhancement of facility and operation security category projects.

Evaluation Process

The legislation provided for a three-level review process:

- A local/regional review by Coast Guard captains of the port (COTP) and MARAD regional directors to verify applicant eligibility and rank applications based on risk/mitigation.
- A national level review consisting of three teams (assessment, facility enhancements and proof-of-concept) of technical subject matter experts from the three agencies. In the assessment category, proposals from critical national security ports were evaluated for criticality of the security need addressed, and probability of high-risk reduction and cost effectiveness. In the enhanced facility category, preference was given to proposals that centered on prevention vs. response, infrastructure vs. operational/personnel improvement, port-wide benefits and new equipment vs. replacement or upgrades as well as Coast Guard COTP/MARAD regional director rankings. The proof of concept team gave preference to projects with potential for national application and concentrated on identifying a few promising projects in each of five categories: container tracking, cargo screening, maritime domain awareness, command and control, and access control.
- An executive team of agency representatives then examined the proposed grant awards from an overarching national perspective.

Awards Announcement/Oversight

Selection board members Rear Adm. (Ret.) Bennis, Associate Under Secretary for Maritime and Land Security; Rear Adm. Pluta, Assistant Commandant for Marine Safety, Security & Environmental Protection; and Capt. Schubert, Administrator of the Maritime Administration, reviewed the team recommendations and in mid-June provided a briefing on the awards and process to Coast Guard Commandant Adm. Thomas Collins, former Under Secretary of Transportation for Security John Magaw, and Transportation Secretary Norman Mineta. Secretary Mineta announced the awards on

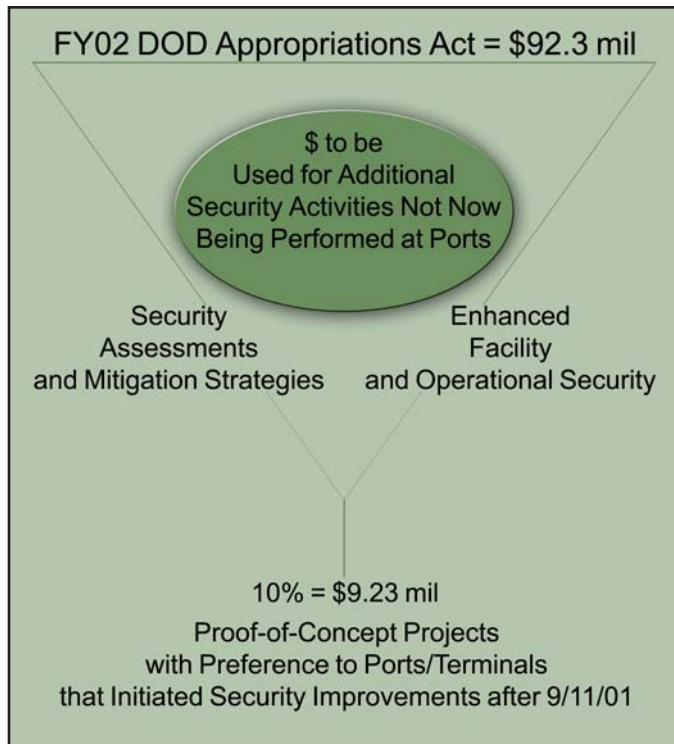
June 17. MARAD acquisition staff has begun negotiations (contracting process, line item funding) with the grantees and will administer the implementation of the projects. TSA personnel will provide oversight and review for projects that have particularly high potential for national application.

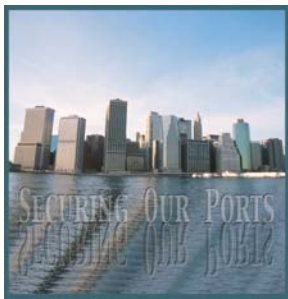
Another Round of Grants

The FY02 Supplemental Request signed by President Bush provided an additional \$104 million in funding for port security grants.

On Jan. 14, 2003, a Broad Agency Announcement (BAA) was released establishing the second round of port security grant funding. TSA, MARAD, and the Coast Guard continue to cooperate to manage the Port Security Grant program. The BAA and Port Security Grant application information are posted at <https://www.portsecuritygrants.dotts.net> (Note: https://). The application period closed on Feb. 27. More than 1,100 grant applications requesting more than \$1 billion in funds were submitted. Only \$245 million is available in grant money for this second round.

A similar review process, joint field review by Coast Guard COTPs and Maritime Administration regional directors and the national review by the Executive Board, used for the first round of port security grants is being followed. The review process is on track and TSA anticipates awarding the grants in the summer of 2003.





The Automatic Identification System & Port Security

by J.M. SOLLOSI
U.S. Coast Guard Office of Vessel Traffic Management

Seaports are engines of national and international economies. They are critical components of the world's economy and critical components of nations' infrastructures. As such, they are attractive targets to terrorists. And they are vulnerable. Seaports are intended to be accessible. For years, international organizations have strived to make seaports safer, more efficient and cleaner. Now, we are all faced with the possibility that this very openness and this drive to greater efficiency and capacity will render our ports and waterways welcome targets of opportunity for terrorism.

The world's maritime leaders have taken action to maintain all we have strived for, and at the same time, protect these assets from intentional damage. An important aspect of protecting ports and sea boundaries and enhancing maritime security is achieving and maintaining an acute level of maritime domain awareness (MDA). The operational intent of MDA is to determine and monitor the position, identity, cargo, course and speed of every vessel entering, departing, transiting or loitering in the maritime domain, including those in innocent passage. In the context of this issue, delivering the Automatic Identification System (AIS) is one very positive step that can be taken.

AIS Capability

It is well known what AIS will do. AIS-equipped vessels will transmit and receive navigation information such as vessel identification, position, dimensions, type, course, speed, navigational status, draft, cargo type and destination in near real time. AIS integrates a number of different technologies: the Global Navigation Satellite System, Differential Global Positioning System, frequency agile digital VHF transceivers, self-organizing communications protocols and an open system architecture which allows input from and output to other AIS receivers or external devices such as electronic chart displays or HF/SATCOM radios. AIS was originally designed and intended for use as a ship-to-ship collision avoidance tool and for monitoring traffic in Vessel Traffic Service areas. However, AIS capability can be readily extrapolated to serve as a tool for coastal and port states to achieve a level of MDA, and thereby add a needed level of protection.

AIS Applicability

The recent—and painstakingly developed—amendments to SOLAS, Chapter V, established an AIS carriage requirement for sea-going vessels over 300 gross tons on international voyages and all vessels over 500 gross tons on domestic voyages. Mandatory carriage under SOLAS V was scheduled for a phased implementation from 2002 through 2008, based on vessel type and tonnage. In addition

to SOLAS requirements, efforts are underway in many countries to mandate AIS carriage domestically for commercial non-SOLAS vessels.

The intent of this phased approach was to deliver AIS capability soonest to those vessels, either because of their size or employment, that posed the greatest risk to safety and the environment. However, what constitutes risk has changed since this well-intentioned schedule was developed. Risk of terrorist attack extends to all watercraft. AIS can be used to identify, track and monitor properly equipped vessels and to sort out those on routine voyages from those that depart from the norm or the expected.

An accelerated schedule has been adopted in the interests of improving security. This proposal requires outfitting the SOLAS fleet by July 1, 2004, essentially moving the categories of vessels less than 50,000 tons into the first two years of the schedule rather than having them spread over four additional years.

The Port Security Mission

Protecting the Marine Transportation System (MTS) is the primary element of maritime border security. The MTS includes waterways, ports, intermodal connections, vessels and vehicles. A port security mission includes protecting maritime borders by detecting, disrupting and deterring terrorist attacks against territory, population and infrastructure; halting the flow of illegal drugs, migrants and contraband through maritime routes; preventing illegal incursions of our exclusive economic zone (EEZ); suppressing violations of national and international laws in the maritime region; ensuring the free flow of legitimate commerce; and responding to events that occur.

Maritime borders are vulnerable. As an example, the United States maritime borders include 95,000 miles of shoreline, 361 ports, and an exclusive economic zone that spans 3.5 million square miles. Over 7,500 ships make more than 51,000 port calls annually. The passenger vessel industry carries more than 6.5 million people annually. Six million loaded containers, 156 million tons of hazardous material and nearly one billion tons of petroleum products enter our ports each year. The MTS moves 95 percent of the nation's overseas trade. The vulnerability of the MTS makes it an attractive conduit and target for terrorists intent on mass destruction or mass disruption. Our maritime security response to this threat must strike a

CURRENT SOLAS AIS IMPLEMENTATION SCHEDULE

Regulation 19 of SOLAS Chapter V—Carriage requirements for navigational systems and equipment—sets out navigational equipment to be carried onboard ships, according to ship type. The new regulation adds a requirement for carriage of automatic identification systems (AISs) capable of providing information about the ship to other ships and to coastal authorities automatically.

The regulation requires AIS to be fitted aboard all ships of 300 gross tons and upwards engaged on international voyages, cargo ships of 500 gross tons and upwards not engaged on international voyages and passenger ships built on or after July 1, 2002. It applies to ships engaged on international voyages constructed before July 1, 2002, according to the following timetable:

- Passenger ships, not later than July 1, 2003;
- Tankers, not later than the first survey for safety equipment on or after July 1, 2003;
- Ships, other than passenger ships and tankers, of 300 gross tons and upwards, not later than July 1, 2004;
- Ships not engaged on international voyages constructed before July 1, 2002, will have to fit AISs not later than July 1, 2008.

balance between the competing needs of economic globalization, which emphasize the rapid and efficient movement of cargo, and a restrictive security regime that minimizes the risk and consequences of a terrorist attack.

The elements of a plan to achieve this sometimes-contradictory goal include establishing a command and control infrastructure; building MDA; and

formulating a plan for interdiction, port control, asset protection and incident response.

Command and Control

To execute a security mission, the competent authority must establish a command and control structure with communications links to other organizations, agencies and services—a key capability when facing unconventional or unorthodox threats. Port authorities and law enforcement agencies should operate using shared information and connectivity along with a real-time common operational picture of ports and offshore approaches.

MDA

In order to achieve a maritime security environment that effectively differentiates between benign and threatening activities, a port or coastal state must have an awareness of all vessels—with their cargo and crew—that operate to and from their ports, or transit their coastal waters. The essence of this MDA is the timely possession of information and intelligence, and the ability to conduct surveillance and reconnaissance of all vessels, cargo, and people that operate in the maritime domain well before the potential threat enters the maritime boundaries. MDA is the linkage between offshore domestic security operations and inshore port-related missions. Effective MDA demands not only better collection of information and intelligence by multiple agencies but, more importantly, fusion of that information and intelligence so that it may be analyzed and transformed into actionable knowledge and tactical direction.

The AIS can readily contribute to achieving MDA. AIS can provide the position and identity of every vessel within VHF-FM range to a coastal station. Even though AIS is presently limited to line-of-sight coverage and does not capture all vessels that could be considered a threat to national security, it provides a clear picture of the routine traffic so that movements out of the ordinary can be more readily detected. AIS also identifies hazardous material

movements so that they may be afforded special protection. And AIS information is in a readily exportable format. It may be exchanged among the various organizations, services or agencies with an interest in protecting a port's safety and enhancing its commerce.

Interdiction

Once a potential threat has been identified, a port or coastal state must have the capability to detect, intercept and interdict it using patrol boats or maritime patrol aircraft. Such action could disrupt planned criminal acts and prevent the eventuality of a catastrophe before it threatens the port.

“AIS-equipped vessels will transmit and receive navigation information such as vessel identification, position, dimensions, type, course, speed, navigational status, draft, cargo type and destination in near real time.”

The AIS would contribute to this mission by enabling the shore authority to track certain suspect vessels. It also assists a shore authority in distinguishing normal traffic from vessels moving contrary to a traffic scheme or prescribed route. AIS could also be used to track patrol craft assets. The precision navigation aspects of AIS would be used in intercept and interdiction operations.

Asset Protection and Incident Response

High-interest vessels that could be used as weapons or vessels carrying a large number of passengers should be identified, boarded and inspected offshore before they could do harm to our ports or population. Competent authorities need to ensure the security of high-interest vessels while underway, particularly when maneuvering adjacent to critical infrastructure. This is necessary to provide a visible, credible deterrent, and to maintain control of traffic. A vessel escort program could be employed to protect ships from external hostile attack. The individual escorts will entail a security zone enforced by patrol craft serving as perimeter control. The “moving” security zones will likely begin (or end) at the sea buoy.

The use of AIS in conjunction with a properly equipped Vessel Traffic Service (VTS) can serve as key elements of a traffic control and incident

response regime. Traffic control of all tracked vessels will enhance asset protection whether it be the vessel itself or critical assets ashore. Using a VTS as the command and control center in conjunction with highly accurate and timely AIS information can improve incident response and asset management during incidents. Transponder-based systems will enhance awareness of all waterborne activity and provide a greater capability to control vessel movement within the port.

A strategy for protecting maritime assets and marine infrastructure combines deterrence and a strong and active presence with the ability to preemptively respond to a bona fide threat. Surveillance provides some level of protection for critical vessel movements and coastal facilities, marine and otherwise (e.g. nuclear power plants, oil refineries). However, providing deterrent defenses will require patrol boats and aircraft. AIS can contribute to the surveillance aspect of deterrence. It can be used as a force multiplier by enabling more efficient command and control, and it can be used to manage the on-scene response craft.

Unity Of Effort

Proper execution of a surveillance, communications and response effort requires coordination among various and sometimes disparate national, international, local and private organizations. These organizations may already be conducting surveillance, creating useful databases, and collecting and sharing information. In addition to serving as sources of information, the port facility operator and the vessel operator will be involved in

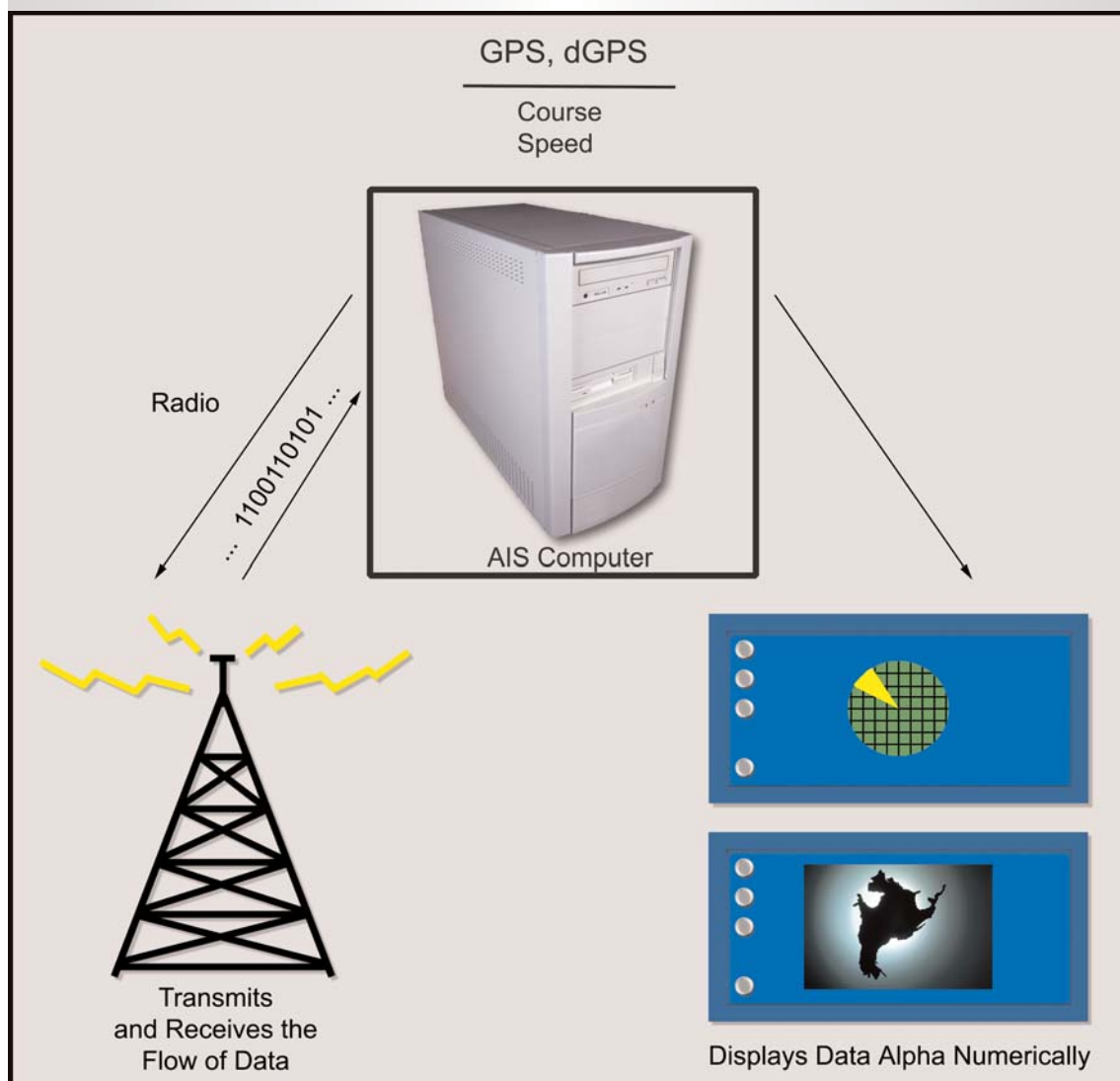
improving security at facilities and on vessels. Having primary responsibility for the security and safety of their facilities and/or vessels, they must be aware of what is occurring on and around their facility or vessel and they must have the procedures and personnel in place to prevent a criminal/terrorist act.

AIS can provide detailed vessel information to a wide variety of users ashore. AIS information is in a readily exportable format and it can be distributed along a network using a system of firewalls and access protection so that sensitive information is withheld or delayed.

Discussion

AIS will permit the identification and locating of any AIS-equipped ship from a properly configured

AIS Elements



USCG illustration. CPU and North America images copyright © 2003 USCG and its licensors.

shore station. However, the system has legal, technical and other limitations.

Legal Issues The concern from an international law perspective, particularly with respect to ships for which SOLAS provides an implementation schedule, is that Article 21(1)(2) of UNCLOS prevents coastal states from establishing equipment requirements on vessels in innocent passage, except in accordance with international standards. "International standards" in this context includes the SOLAS implementation schedule. Thus, to the extent we seek to apply AIS requirements to vessels subject to SOLAS in innocent passage, we need to amend the specified schedule.

Technical Issues AIS broadcasts are via VHF radio and thus limited to line-of-sight, usually not beyond 20-30 miles. AIS protocols and standards allow for interconnection to a long-range telecommunication system such as HF or SATCOM systems such as Inmarsat. However, existing HF and SATCOM systems onboard ships are not capable of receiving and retransmitting AIS information without modification.

The International Maritime Organization (IMO) performance standard for AIS requires that the equipment should function "as a means for littoral states to obtain information about a ship or its cargo" when a vessel is operating in that state's area of maritime responsibility. An AIS long-range reporting mode is required to satisfy this function and to assist administrations in meeting their responsibilities for wide area or offshore traffic monitoring. These responsibilities include safety of navigation, search and rescue (SAR), and environmental protection in offshore areas including the continental shelf and economic exclusion zones.

However, while further reference is made to a long-range mode in the International Telecommunication Union-Radiotelecommunications (ITU-R) technical characteristics and draft International

Electrotechnical Commission (IEC) test standards, neither document provides any detail other than to specify the required interface standard. The purpose of including the long-range mode or sub-system in the AIS transponder requirements is to provide a capability for wide area and extended range automatic reporting of basic ship data, such as a vessel's identity and position, using commercially available global communications infrastructure.

Economic Issues Other issues arise that are neither technical nor regulatory. These regard the ability of manufacturers to equip the world's fleet with AIS and the cost of various options.

Risk of terrorist attack extends to all watercraft. AIS can be used to identify, track and monitor properly equipped vessels and to sort out those on routine voyages from those that depart from the norm or the expected.

AIS manufacturers have not yet reached full production on the ship-board or the shoreside equipment needed to respond to the demand that would be created by an accelerated carriage requirement. The estimated population of affected SOLAS vessels is 40,000. Accelerating the implementation schedule as has been adopted will require that manufacturers respond to a demand for some 2000 AIS units per month over the next two years.

CIRM, the international body that represents marine electronics equipment manufacturers, confirmed at the special intersessional working group of the Marine Safety Committee in March 2002 that their members could meet this demand.

Mandatory ship reporting systems are supposed to be at no cost to the reporting party. This being the case, and if Inmarsat is selected as a reporting medium, it will be necessary to establish an account through which vessels report and the coastal state assumes responsibility for the charges. Implementing any offshore surveillance scheme will require a shoreside infrastructure to receive and process information. Receiver sites and a routing/data relay system will need to be acquired, and a traffic-monitoring center to which AIS information will be routed will have to be equipped and staffed with trained personnel.

Conclusion

In order to achieve a maritime security environment that effectively differentiates between lawful and unlawful activities, port and coastal states must have an awareness of all vessels operating to and from their ports, as well as those transiting their coastal waters. At the heart of this maritime domain awareness are information, intelligence, surveillance, and reconnaissance of all vessels, cargo, and people well outside the traditional maritime boundaries. Effective MDA demands not only better collection of information data by multiple agencies but, more importantly, fusion of that information into a center that can analyze the data and create actionable knowledge. This will be challenging due to the number of different agencies and services with an interest in vessel traffic, but it will also be very powerful because it will leverage the specialized and regional skills of various participants and enhance cooperation. MDA exists today, but only as a nascent capability. AIS can deliver maritime domain awareness faster and more reliably than any other means at our disposal.

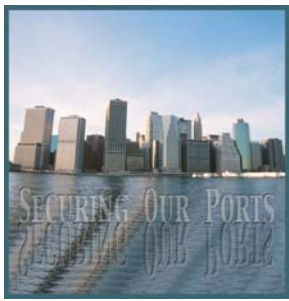
There are obstacles to full and immediate implementation of AIS. However, all can be overcome through cooperation and continued dedication to improving the safety and security of marine transportation worldwide.

The United States recommends that the world's maritime nations jointly pursue a combination of options to provide some level of coordinated MDA in all coastal and port states. This would be similar to the aviation tracking and monitoring processes that have been in place for decades.

The most readily available solution is to establish a surveillance system that relies on cooperative vessels, and the AIS meets that need. Although it is as yet untested, it is available now. We should jointly take full advantage of AIS's capability and its potential. Many visionary, talented and dedicated people in the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), IMO, ITU and IEC have worked long and hard to deliver AIS to the maritime world. We should ensure that the full potential of their efforts are realized.



“A vessel escort program could be employed to protect ships from external hostile attack. The individual escorts will entail a security zone enforced by patrol craft serving as perimeter control.” During a security overflight on the Cape Fear River, N.C., Coast Guard smallboats escort a Navy deployment ship. Photo by Public Affairs Officer Krystyna Hannum, USCG.



Houston–Galveston Area

On the Front Line

by Capt. KEVIN COOK
Captain of the Port; Houston–Galveston, and

Cmdr. PAUL THOMAS
Commanding Officer; MSU Galveston

It's 4:30 a.m. on Sunday. U.S. Coast Guard Cutter *Manta* checks in with the Task Unit Duty Officer (TUDO) working at the joint operations center on Group Galveston, Texas. *Manta* reports it has a rendezvous with the C/S *Rhapsody of the Sea*, and that the sea marshals have boarded *Rhapsody* from the Galveston pilot boat. The TUDO verifies that a team from Marine Safety Unit (MSU) Galveston has completed the security sweep of the Texas cruise ship terminal on Galveston Island, and that all security measures are in place. Shortly thereafter a Dauphin helicopter from Coast Guard Air Station Houston checks in; the overflight of the transit route has been completed and there are no suspicious vessels or activity. Vessel Traffic Service (VTS) Houston-Galveston verifies that all radar and visual contacts are checked into the system and have been cleared for entry to U.S. waters. Everything is ready; *Rhapsody* begins its inbound transit with 2,500 passengers under Coast Guard escort and protected by a moving security zone.

So begins another day in the Houston-Galveston-Port Arthur sector that will see *Manta* return to the waters offshore Galveston to deliver a law enforcement team to four ships awaiting security boardings prior to being cleared for entry. Meanwhile, USS *Whirlwind*, a U.S. Navy patrol craft 170 working as part of the Maritime Security Squadron (MSS) in the task unit, is stationed off the entrance to Lake Charles, La., where it will deliver a

Coast Guard boarding team to a liquefied natural gas (LNG) tanker. Once cleared for entry, members of MSU Lake Charles will sea marshal the cargo-laden tanker to the Trinkline LNG terminal. In the port area, teams from Marine Safety Office (MSO) Houston and MSO Port Arthur will conduct harbor patrols, facility security checks, and dock-side boardings of ships loading particularly hazardous cargoes. Coast Guard boats will enforce security

zones restricting access to highly industrialized waterways throughout the ports of Beaumont, Lake Charles, Houston, Galveston, Texas City and Freeport. Fixed wing aircraft from Coast Guard Air Station Corpus Christi will patrol the off-shore lightering areas and approaches while Coast Guard auxiliary aircraft from Houston overfly the Intercoastal Waterway. Throughout the day the Task Unit Fusion Center will coordinate this activity, target and track the resources, collate information coming in from dozens of sources, issue Captain of the Port orders, and respond to a myriad of inquiries from local, state, and federal agencies, and the maritime industry.

Introduction

Described above is Operation Neptune Shield in the task unit that protects the six major coastal ports in southwest Louisiana and southeast/central Texas (Captain of the Port [COTP] Port Arthur and COTP Houston-Galveston zones), a 200-mile stretch of coast along the Gulf of Mexico that includes the densest concentration of energy production, storage and refinery resources in the world.

Perhaps nowhere are the challenges associated with securing a big, busy, industrial port better illustrated than in the Galveston Bay port entrance where the Houston Ship Channel provides the gateway to the Ports of Houston, Texas City, and Galveston. This is the busiest port entrance in the nation and the second largest petrochemical port complex in the world. Virtually every sector of the maritime industry has a significant presence in Galveston Bay, including all aspects of the petrochemical industry (crude, product, chemical and gas carriers), container, roll-on/roll-off, bulk and break bulk trades (including the largest container terminal on the Gulf of Mexico), offshore exploration and production (offshore supply vessels, crew boats, survey vessels, mobile offshore drilling units, fixed platforms), a vibrant commercial fishing fleet, large and small passenger vessels, and the nation's third densest recreational boating population.

Each day more than 700 vessel transits are monitored by VTS Houston-Galveston and an average of 31 deep draft vessels enter the port. Each week there are more than 40 movements of liquid hazardous gas ships and barges, and an average of 43 arrivals for ships carrying particularly hazardous cargoes, of which at least 20 percent require at-sea high-risk vessel (HRV) boardings prior to port entry. The Houston Ship Channel, 53



U.S. Navy patrol coastals arrive at Group Galveston. Photo by NASA Photo Department at Johnson Space Center.

miles long and 400 feet wide, winds through heavily populated areas and leads to refineries in the Texas City and Houston areas that account for more than 50 percent of all the gasoline refined in the United States. More than 20 percent of U.S. oil imports enter the nation from the lightering areas offshore of Galveston, and about 30 percent of domestic LNG production comes from production platforms in the offshore area. In addition, the Port of Galveston is a thriving tourist and passenger port and is host to three major cruise ships with weekly and bi-weekly sailings.

This article describes how maritime homeland security (MHLS) has become operational and is integrated into the daily operations at one of our nation's busiest and most economically vital port complexes through a consistent focus on coordination of Coast Guard resources and partnering with the maritime community and local law enforcement. For security reasons, this article is intentionally vague with regard to specific tactics, resource laydowns, and activity levels.

Like all ports, the challenge in securing the Houston-Galveston port complex is in achieving the proper balance between the need for security and the necessary functions of the port, including flow of commerce, access to the waterway, requirements for safety, and ability to safeguard the environment. These tradeoffs are accentuated in a

port where the sheer volume and diversity of maritime activity strains the capacity of the port system even before security measures are overlaid on it. In the Port of Houston, for example, even a minor delay to a vessel can set off a chain reaction involving pilots, harbor tugs, stevedores, refineries and others that may cause a vessel to lose its place in the rotation and be forced to wait for a berth to come open. What may have been a two-hour delay (to complete a port security boarding, for example) at another port with excess capacity, potentially translates into a 36-hour delay in a port that has no slack in the system. The challenge is to ensure close coordination and cooperation so that security measures are integrated into the operations of the port and become part of the system.

Coordination of Coast Guard Resources

The challenge of coordinating the new MHLS missions was initially complicated by the fact that a single Coast Guard group (Group Galveston) serves two separate COTP zones, which include the equivalent of four medium or large marine safety offices (MSO Houston-Galveston, MSO Port Arthur, MSU Galveston, and MSU Lake Charles). One group commander was faced with the ominous task of prioritizing resource requests from two COTPs for missions spread out over 200 miles of coastline and 25,000 square miles of Exclusive Economic Zone off-shore.

**Houston-Galveston
Port Arthur
Task Unit**

**MSO Houston-Galveston
MSU Galveston
VTS Houston-Galveston**

**MSO Port Arthur
MSU Lake Charles**

**Group Galveston
Maritime Security Squadron
CGC Manta
CGC Manowar
CGC Heron
USN PC170
Air Station Houston**

In part to remedy this situation, the Commander of 8th Coast Guard District ordered the establishment of task units to carry out the MHLS missions within geographic sectors in the Gulf of Mexico, and all Coast Guard units within the COTP Houston-Galveston and Port Arthur zones were merged into one Task Unit for that purpose.

Task Unit Regional Fusion Center (RFC) With the task unit in place it was necessary to develop a system for command and control that would allow for seamless interaction and coordination of Coast Guard resources on a daily basis that was previously only present during the emergency phase of a major response to a maritime incident. The RFC was established to coordinate MHLS activity throughout the sector and to provide some resource savings by reducing redundant activity at Coast Guard commands in the task unit. The RFC provides support for MHLS operation in the in-shore zone throughout the sector, and directs most of the MHLS activity in the near- and off-shore zones. The RFC consists of three branches shown in the graph on page 45.

Task Unit Vessel Targeting Branch receives and screens such information from agents and shipping interests as the 96-hour advance notice of arrival, crew and cargo lists, and vessel histories. This branch works very closely with the National Vessel Movement Center to target vessels for security and

Port Security Challenge

Security vs. Access

Security measures may restrict access to waterways or to information.

Security vs. Commerce

Security measures may add direct and indirect costs. Measures may also impede commerce.

Security vs. Safety

Security duties may detract from safety duties. Duties may also add to crew fatigue.

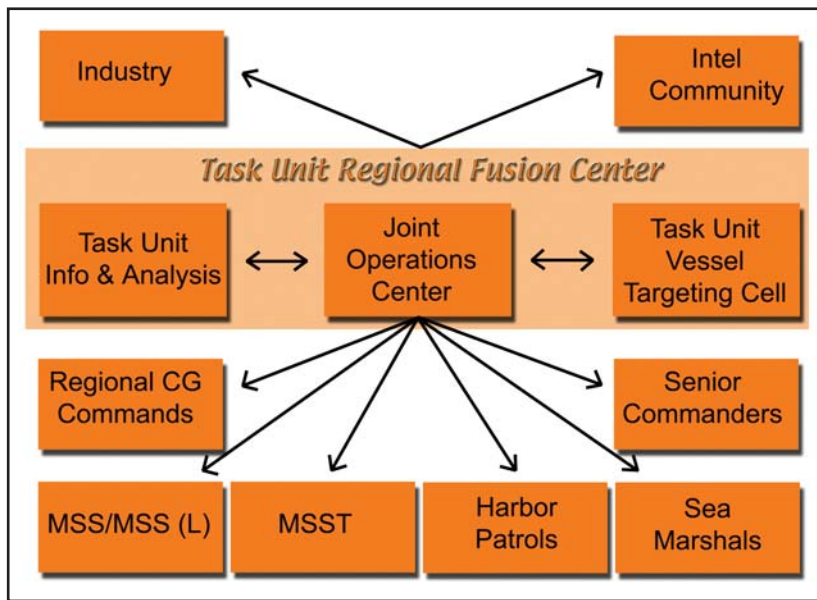
Security vs. Environment

Security efforts may divert resources from environmental protection, and may have an adverse impact on the environment. Measures may also hamper environmental response.

port state control boardings based on Coast Guard criteria, and coordinates extensively with the Immigration and Naturalization Service and U.S. Customs on a variety of other vessel, cargo and crew issues. It also produces the daily vessel approach list, cleared to enter list, and lightering zone activity list for use by all Coast Guard and U.S. Navy commands in the task unit.

Task Unit Operations Center is co-located with the Group Galveston Operations Center and staffed continuously by the TUDO. The TUDO maintains the regional situation and resource status including the locations and status of all Coast Guard vessels and aircraft, all partner agency resources, and all high-interest vessels. Tactical assignments for the Maritime Security Squadron, Marine Safety and Security Team (when attached), and other Coast Guard resources are made at the Operations Center. The Task Unit Operations Center is the nerve center of the regional MHLS efforts where real time information is translated into direction for Coast Guard and other agency action. The TUDO works very closely with VTS Houston-Galveston to ensure that all vessels entering Galveston Bay have been cleared for entry and is the information lifeline for Coast Guard and Navy vessels executing the MHLS mission in near- and off-shore zones.

Task Unit Information & Analysis Branch is the central point for gathering, analyzing and disseminating information from government and non-government sources, and maintaining liaison with local law enforcement, intelligence and industry partners. This branch produces the daily maritime domain awareness (MDA) brief for the task unit and provides threat alerts as appropriate to the local maritime industry and Coast Guard commands. The Information and Analysis Branch has established an extensive network of contacts and working groups designed to facilitate information sharing and raise awareness among maritime



and law enforcement stakeholders. Along with the port security committee, this network has been largely responsible for the exceptional degree of cooperation within the sector and the success of several joint agency/industry initiatives to enhance security while minimizing the impact on commerce.

The RFC has proven to be not only efficient, but extremely effective and absolutely essential to the smooth integration of U.S. Navy vessels and crews into the task unit. It provides “one stop shopping” for government and industry with the need to know the status of MHLS operations in the sector, and gives the task unit the ability to react rapidly to threat information or changes in tactical situations.



Coast Guard patrol boats and Navy patrol coastals rendezvous off the coast of Galveston to form Maritime Security Squadron Lite 861: CGC *Stingray* of Mobile, Al.; CGC *Manta* of Freeport, Texas; CGC *Manowar* of Galveston, Texas; USS *Chinook*, USS *Whirlwind*, and USS *Thunderbolt*, all of Little Creek, Va. Photo by NASA Photo Department at Johnson Space Center.

Extending Partnerships

The MHLS partnering effort has focused on vastly increasing the local network of and interaction among local, state, and federal law enforcement and intelligence agencies, and completely engaging the maritime community in planning and, to some extent, executing the security mission. The corporate security/law enforcement agency outreach program puts senior-level law enforcement and corporate security personnel together with Coast Guard security and intelligence personnel to discuss suspicious threat incidents, review newly implemented security requirements, and establish communications protocols.

The Houston-Galveston Port Intelligence Team was established to aid the timely exchange of threat information among government agencies having operational oversight in ports served by the Houston Ship Channel. Prior to this, exchanging port-related intelligence among federal, state and local government agencies was haphazard or non-existent. As this 20-plus agency group has matured organizationally, so have the quality and quantity of intelligence that has been disseminated (stow-aways, suspicious surveillance activities, diver threats, etc.). The group's successful response to, and vetting of, a terrorist threat against local refineries last summer underscored the effectiveness of the intelligence team. Current membership includes representatives from the Air National Guard, Customs, Department of Labor, DOD

Criminal Investigative Service, FBI, Immigration and Naturalization Service, Military Sealift Command, NASA, Office of Naval Intelligence, Port of Houston Authority Police, U.S. Attorney's Office, and local/county law enforcement agencies.

The maritime community in the Houston-Galveston area was quick to react to the call for heightened security in the wake of the September attacks, and capitalized on the very strong network in place for the coordination of safety and environmental protection issues. The Houston-Galveston Navigational Safety Advisory Council (HOGANSAC), a federally mandated advisory council in existence since 1991, quickly formed an ad hoc Port Security Subcommittee, and followed up with a formal charter for a standing Port Security Committee by February 2002. The PSC has been essential to the successful integration of MHLS requirements into the function of the port, and a large reason for the overwhelming cooperation from the entire maritime community. Some of the more notable initiatives of the PSC and the maritime community at large have been participation in a system that allows mariners to report suspicious activity to VTS Houston-Galveston, Port Authority of Houston dedicating their fireboats to conduct security patrols with Coast Guardsmen embarked, and the PSC publishing guidelines on credentialing and recommendations for the use of electronic surveillance. In June 2002, the PSC co-hosted a port security planning workshop. In November they

Maritime Homeland Security Milestones

2001

September

- (11) Port-wide safety zone requiring security upgrades at terminals and onboard ships;
- COTP and Industry Task Force on Offshore Lightering (ITOL) implemented voluntary security measures for lightering zones;
- Coast Guard WMEC deployed offshore Galveston

October

- 1st meeting of Port Security Committee;
- Multi-agency security operation for commissioning of USS *Howard* in Galveston

November

- Task unit formed and Fusion Center stood up;
- Navy PC 170s attached to Task Unit with Coast Guard as MSS Commander

December

- Security zones established in highly industrialized areas;
- Task Unit MDA Web page online to provide common resources and situation picture;
- Prototype MSS (Lite) Concept;
- Law Enforcement/Corporate Security program begun

2002

January

- Task Unit Operations Center stood up;
- Prototype MSST assigned to Task Unit;
- Memorandum of Understanding with Port of Houston for joint patrols

February

- VTS Global Command Communication System information exported to Task Unit Operations Center and MSS to provide real-time vessel position and operating info;
- Joined Energy Security Council

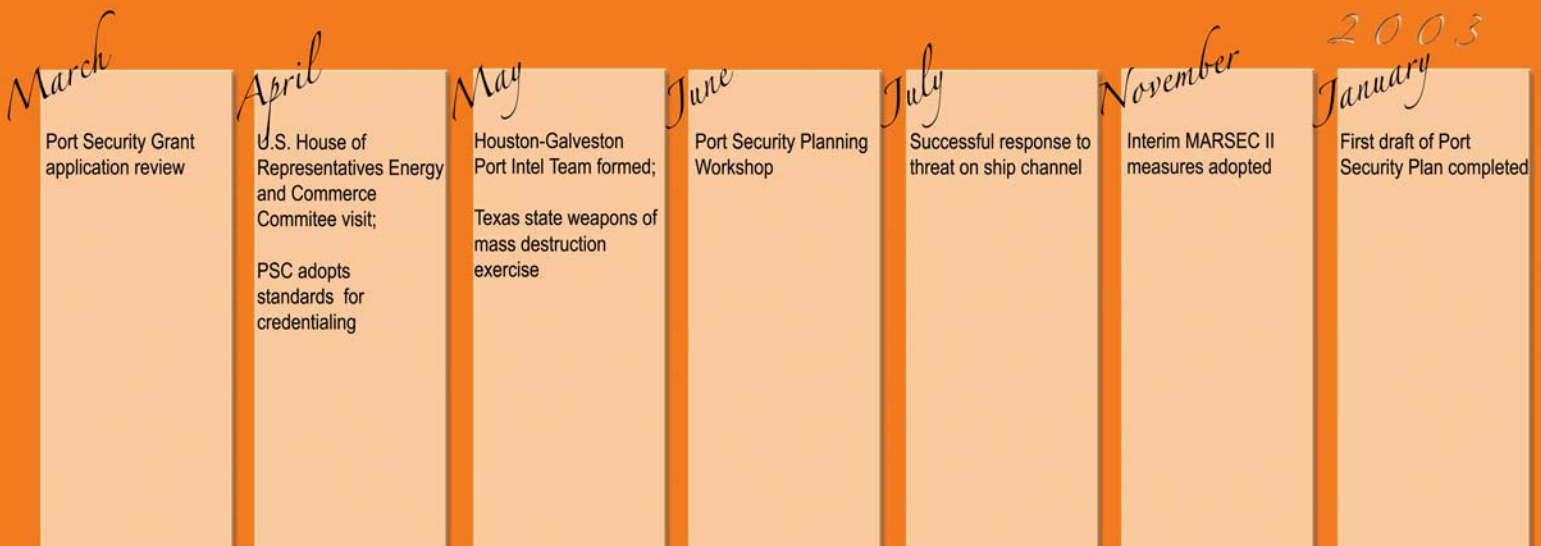
adopted Interim MARSEC II measures for ship and facilities, and in January 2003 the first draft of the Port Security Plan was published.

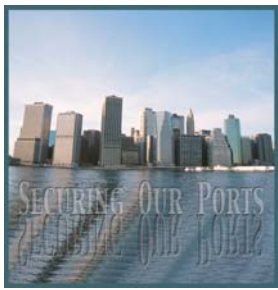
The Way Forward

It's 4:30 a.m. on Sunday. The Atlantic Area Fusion Center in Norfolk, Va., calls the Integrated Command Center in Galveston to verify the day's arrivals and departures, and passes active vessel contacts from the Area Vessel Monitoring Station to the Houston-Galveston VTS. VTS receives the Automatic Identification System (AIS) signals from the 30 ships in the Gulf of Mexico bound for Galveston Bay, and automatically cross references the information with the overseas cargo inspection database to verify that the cargo was cleared at the point of origin. Signals from the vessel indicated that cargo hatch or container seals have not been altered since inspection. The crew information is checked and a message is automatically generated to Coast Guard cutters offshore with names and boarding priorities of approaching ships. At the dispatch offices of the local pilots associations, agents and harbor tugs, a subset of the same data is available and they know which vessels are cleared to enter the port that day, the estimated time of arrival and any inspections or documentation required prior to cargo operations. Patrol aircraft detect a vessel 120 nautical miles out that is not checked into the traffic control system and is not transmitting AIS. CGC *Manta* is immediately

diverted to intercept and investigate the vessel while agents, owners, and operators are contacted ashore. In the port area, vessels are met by a single team of agents to clear crew, cargo, safety, security and environmental issues prior to operation. Containers are scanned as they are unloaded. Surveillance and intrusion detection systems monitor control spaces onboard ship, at marine terminals and at remote unattended infrastructure, and feed a centralized security station that dispatches vessel and shore patrols. The port is in MARSEC 1, operating with the everyday "normal" security measures in place ... and thriving.

This is Operation Neptune Shield in the not-so-distant future. Security measures are fully integrated into the function of the port, and all stakeholders are engaged in the joint security efforts. The way forward is built on the foundation of strong partnership and coordination of resources that we have laid, not just since September 11, but in the months and years prior. The challenge of securing our ports is a daunting one, but it is not unlike the challenge we faced in the wake of the *Exxon Valdez* incident and the resulting Oil Pollution Act of 1990. By building our capability, planning for coordinated action with shared resources, and maintaining open lines of communications we can meet this challenge, too. The Houston-Galveston maritime community is well on the way.





Establishing a Port Security Committee

by Lt. Cmdr. KEVIN KIEFER

Chief of Port Management Department; MSO Corpus Christi

To provide the maritime industry with new security guidance procedures related to the Maritime Transportation Security Act (MTSA), the U.S. Coast Guard has produced three informative Navigation and Vessel Inspection Circulars (NVICs). The first NVIC released, NVIC 9-02 (Guidelines for Port Security Committees, and Port Security Plans Required for U.S. Ports), was specifically created to establish a Port Security Committee for assessing and reducing security threats and vulnerabilities.

There are a number of ways available for establishing and maintaining these Port Security Committees, thereby allowing each Marine Safety Office (MSO)/Captain of the Port (COTP) to create a committee focused on the specific port's needs. This article describes the path taken by MSO Corpus Christi and shares its experiences and lessons learned.

Area of Responsibility

MSO Corpus Christi is located on the Texas Coastal Bend. Its area of responsibility is large, extending north to the Colorado River, south to the U.S.-Mexican border, and spreading more than 200 miles into the Gulf of Mexico. It covers approximately 340 miles of South Texas waterways, including the Gulf Intracoastal Waterway, the Corpus Christi Bay, and various ports along the Gulf Coast—essentially, the southern half of the Texas coast.

Affectionately referred to as the “Texas Riviera,” Corpus Christi is indeed a water lover’s haven with

tourists and commercial fishermen continually on the waterways. However, interspersed among these smaller vessels is the daily crossing of large cargo ships. In terms of tonnage, Corpus Christi is the seventh largest port in the United States, and the fourth largest in terms of movement of crude oil and petroleum products. With the recent military outload operation in the Port of Corpus Christi, the usually busy waterways have become even busier.

Strategic Port of Embarkation

Corpus Christi’s convenient location on the Coastal Bend and its numerous port and intermodal facilities offer a wide interface between the water and surface modes of transportation. For this reason, it is one of the Strategic Ports of Embarkation (SPOE) chosen by the Department of Defense. These strategic ports have the ability to quickly and safely support deployment of military personnel and cargo in defense contingencies to meet the mission requirements of overseas commanders.

To assure rapid execution and deployment for national defense, each SPOE is required to form a Port Readiness Committee (PRC). The PRC meets regularly, working with appropriate government agencies and port stakeholders. A PRC meeting usually addresses local intelligence issues, port security requirements, and processes to improve port security and operational efficiency through drills and exercises.

Creation of Port Security Committee (PSC)

NVIC 9-02 advises that Port Security Committee activities be coordinated with existing PRCs when-

ever possible. Because of the PRCs' proven success with recent exercises and actual military outload operations, MSO Corpus Christi determined that the PRC—as well as the local Harbor Safety Committee—should jointly form the basis for the new PSC for the Port of Corpus Christi. For advice on establishing PSCs, the MSO then turned to other MSOs that were in various PSC development stages. Lessons learned from other MSOs greatly assisted MSO Corpus Christi in their planning.

MSO Corpus Christi is planning to develop four PSCs because there are four main ports (Port of Corpus Christi, Port of Port Lavaca–Point Comfort, Port of Victoria, and Port of Brownsville) within the MSO's area of responsibility (AOR). The different port locations necessitate some different members and area concerns due to different physical characteristics and port uses. Each PSC will be considered separate and equal, and the COTP will remain actively involved in each one. Other MSOs with more than one major port have also used this approach.

PSC Membership

There are a number of ways to meet the requirements in comprising the PSC. NVIC 9-02 recommends involving a large number of organizations in the PSC. However, even if each organization only sends one representative, the resulting diverse group will potentially be large and difficult to manage. Some MSOs that have taken this approach have therefore divided the large committee into subcommittees or smaller groups based on the organization's functions (e.g., response organizations, container terminals, refinery terminals, etc.). Other MSOs have developed a smaller steering committee that helps direct and manage the larger, diverse PSC.

Another approach, and the approach that MSO Corpus Christi has decided to use, is a small PSC composed of representatives from existing larger, sector-specific groups. For example, about 30 law enforcement agencies were already meeting monthly through the Corpus Christi Intelligence Sharing Group prior to the PSC's creation; now they send one member to the PSC who then reports the information back to the entire group. The Coastal Bend

Business Roundtable Security Forum, a group of refinery terminal security managers, is also using this approach. In addition, the PSC reports to the larger and all-encompassing HSC, thereby ensuring that every Port of Corpus Christi organization is involved with the PSC's efforts to maintain security.

Corpus Christi PSC members include a representative from the following organizations (note that each PSC may be slightly different in its membership):

- Bureau of Customs and Border Protection
- Emergency Operations Center (of Corpus Christi)
- FBI's Joint Terrorism Task Force
- Federal Emergency Management Agency
- Gulf Intracoastal Canal Association
- Pilots Association
- Port of Corpus Christi Authority
- Transportation Security Administration
- U.S. Coast Guard
- U.S. Navy

Members also include a representative from local facilities, marine insurance brokers, railroad companies, shipping agencies, and shipyards. Other groups can be invited to discuss specific issues on an as-needed basis (as specific security situations arise).

Through groups such as the PSC...key stakeholders can be brought together to help determine and mitigate high-risk situations.

Meeting of the PSC

The COTP began the first meeting by providing members with an overview of Coast Guard activities in the port, and introducing the MTSA and NVIC 9-02. As required by the NVIC, each PSC has a list of requirements to

accomplish that will further ensure the safety and security of their port. Recognizing the intricacies of the NVIC's required Port Security Plan (PSP), the PSC decided to immediately begin drafting elements of it. Fortunately, the PSC had numerous security assessments regarding the Port of Corpus Christi already compiled (including the Coast Guard Port Security Assessment completed in September 2002). The PSC agreed to use the findings from these assessments as the main basis for developing the PSP.

The first element of the PSP that the PSC decided to address was identifying requirements they felt

An 87-foot Coast Guard patrol boat escorts the USNS *Cape Rise*, which is a Military Sealift Command Roll-on/Roll-off ship. Photo courtesy MSO Corpus Christi.



were necessary for the Port of Corpus Christi to meet Homeland Security Advisory System (HSAS)/Maritime Security (MARSEC) levels. Starting with existing MARSEC requirements from another MSO, they determined which of those ideas applied to Corpus Christi. The PSC will continue developing elements of the PSP at future meetings. (Note that although there will eventually be four PSCs headed by MSO Corpus Christi/COTP, only one PSP is required for the AOR.)

The PSC is also taking ideas and best practices from other groups, combining them into the future PSP. For example, one idea mentioned was originated by the Coastal Bend Business Roundtable Security Forum. Their notification system, essentially a Web-based digital paging system, can notify facilities, port authority, Coast Guard, and other agencies of an emergency situation within one minute. Another idea, originally discussed at the Intelligence Sharing Group Forum, concerns security guard procedures for vessels with Detain on Board crewmembers. Also discussed was the Declaration of Security (mentioned in NVIC 10-02, Security Guidelines for Vessels); the group decided it was a good template in addressing security concerns between vessels and facilities, and will begin implementing it as soon as needed.

The PSC meeting provided an open forum for past, present and future security-related issues. Overall, both the MSO and the various industry groups felt

that the new PSC and its purpose was a good idea and worthwhile for all involved.

Conclusion

To successfully meet the NVIC 9-02 requirements, the PSC developed both short-term and long-term objectives. Short-term objectives of the Port Security Committee include completing the HSAS/MARSEC requirements and drafting the committee's charter. Long-term objectives include finishing the PSP by the December 2003 deadline and aligning it with new domestic and international security requirements. While there are numerous security measures being conducted in the Port of Corpus Christi, the interweaving thread is the PSC. To allow maritime commerce to continue moving effectively while maintaining a high security level, it is imperative that all maritime stakeholders communicate their actions with each other. Through groups such as the PSC, these key stakeholders can be brought together to help determine and mitigate high-risk situations. This group and its members will play an active role in the continued security of the Port of Corpus Christi.

The success of MSO Corpus Christi's PSC is due in part to the cooperation of other MSOs who provided their own experiences and lessons learned regarding their PSC developments.

To learn more about Corpus Christi's PSC, contact Lt. Cmdr. Kiefer at (361) 888-3162 (ext 500) or kkiefer@msocorpuschristi.uscg.mil.

Barge Industry Develops First Coast Guard-Approved Security Plan



by AMY BRANDT
Manager—Government Affairs; The American Waterways Operators

The American Waterways Operators (AWO), the national trade association for the tugboat, towboat and barge industry, has developed a model vessel security plan to reduce the likelihood of a terrorist attack involving barges or towing vessels. The AWO Model Vessel Security Plan is the first industry standard security plan to be approved by the U.S. Coast Guard. In a recent letter, Rear Adm. Larry Hereth, Director of Port Security, informed AWO that U.S. tugboat, towboat and barge companies that implement the AWO Model Vessel Security Plan will be considered to be in compliance with the guidance provided in Navigation and Vessel Inspection Circular (NVIC) 10-02, Security Guidelines for Vessels. "I commend American Waterways Operators for its efforts in establishing a model security plan that raises the security standard for a significant portion of the maritime industry," the admiral wrote. "I look forward to further strengthening the U.S. Coast Guard's partnership with AWO in our fight against terrorism."

The goal of the AWO Model Vessel Security Plan is to protect people and property and prevent vessels from being used as weapons of mass destruction. The plan was developed after the September 11 terrorist attacks by a special AWO Security Working Group, including representatives from the Coast Guard and the U.S. Army Corps of Engineers.

Development of the Plan

AWO developed the Model Vessel Security Plan to assist member companies in improving the security of their operations. The process began in November 2001, less than two months after September 11 and more than a year before passage of the Maritime

Transportation Security Act of 2002, which makes vessel and facility security plans mandatory. AWO Vice Chairman of the Board Steve Scalzo, of Foss Maritime Company, led a high-level working group that met with Rear Adm. Paul Pluta, Coast Guard Assistant Commandant for Marine Safety, Security and Environmental Protection, and Maj. Gen. Robert Griffin, Director of Civil Works for the U.S. Army Corps of Engineers. The working group reviewed potential threats and vulnerabilities to the marine transportation system and recommended that AWO work with Coast Guard and Corps of Engineers officials to develop a model security plan.

From January to March 2002, representatives from 10 AWO member companies, the Coast Guard, and the Corps of Engineers met to develop and finalize the plan. The AWO board of directors unanimously voted to approve the plan in April 2002. In unveiling the new plan, AWO President and CEO Tom Allegretti said, "In developing this Model Vessel Security Plan, AWO continues its effort to be a constructive leader in the safety and security of the American tugboat, towboat and barge industry. We hope this plan provides AWO members with a template that they can use to develop and augment their own vessel security plans. In this way, our industry continues its role as 'the eyes and ears' on the waterways of this nation."

Last fall, the Coast Guard issued NVIC 10-02, which provides guidelines for the development of vessel security plans. The NVIC stated that the Coast Guard would consider accepting industry-developed standards as meeting the criteria



Crewmember Seaman April Dunlap, aboard a Station Curtis Bay, Md. utility boat, watches a barge get loaded during a Homeland Security patrol in Baltimore Harbor. Photo by Public Affairs Officer Zach Zubricki, USCG.

contained in the NVIC. After making minor modifications to the Model Vessel Security Plan to ensure consistency with the NVIC, AWO submitted the plan for Coast Guard approval. In March, the Coast Guard signaled its approval, making the AWO Model Vessel Security Plan the first industry standard plan to be submitted to and approved by the Coast Guard.

AWO members are now working to implement the plan throughout their operations. AWO has also asked the Coast Guard to recognize the plan as an equivalent standard to forthcoming vessel security plan regulations, which the agency will release this summer.

Elements of the Plan

The AWO Model Vessel Security Plan begins by identifying guiding principles for vessel security plans and terrorism prevention. The plan describes security policies and procedures that companies should have in place to assign responsibility for security, both onboard vessels and on shore. A company's security policies and procedures should include means to: (1) detect security threats early; (2) prevent or restrict access to the vessel; and (3) ensure communications between the vessel, the company, and appropriate authorities at all times. The plan specifies that a company's vessel security plan should include common-sense actions that can be implemented by companies and crewmembers in the event of a suspected or actual terrorist attack. The AWO plan requires companies to designate company and vessel security officers.

The plan also provides guidance on areas that companies should address in developing vessel security plans specific to their operations, including awareness, training, personnel practices, planning, and emergency response. The plan uses the Coast Guard's Maritime Security (MARSEC) conditions to trigger the security level in place aboard the vessel. Companies may elect to move to a higher security level than that designated by the Coast Guard, but not to a lower one.

In addition, the AWO Model Vessel Security Plan contains a matrix that lists both required and recommended actions to be taken with regard to physical security of vessels and fleeting areas, en route or in transit security, communications, and cargo. These actions are geared to the Coast Guard's three MARSEC conditions, and vary based upon the type of cargo carried. An appendix to the plan categorizes nearly 100 commonly carried hazardous cargoes that could potentially be used as weapons of mass destruction. The cargo classification table determines what actions vessel operators should take when transporting those cargoes. Another appendix lists types of suspicious activity that vessel crewmembers should be aware of and report to the Coast Guard's 24-hour National Response Center.

Distribution of the Security Plan

Since the plan was finalized last year, AWO has shared it widely with government and industry organizations interested in maritime security. Recently, the plan was featured at the March 2003 Inland Waterways Conference sponsored by the 8th Coast Guard District and the Ohio Valley and Mississippi Valley Divisions of the Corps of Engineers. In March 2002, the Coast Guard's Marine Safety Office-St. Louis invited AWO to present the Model Vessel Security Plan to law enforcement personnel, including the FBI, National Guard, state police agencies, local Corps of Engineers officials, and other agencies. The Towing Safety Advisory Committee (TSAC) has also recognized the AWO plan as a practical and effective security-enhancement tool and urged the Coast Guard to approve similar industry-developed security standards for other segments of the maritime industry. Copies of the plan have been shared with the Navigation Safety Advisory Council (NAVSAC) and Harbor Safety Committees throughout the country. The AWO plan is also referenced in the American Bureau of Shipping's Guide for Ship Security.

The American Waterways Operators is the national trade association representing the U.S. tugboat, towboat, and barge industry. Headquartered in the Washington, D.C. area, the association is comprised of 375 member companies operating nearly 80 percent of the towing equipment in the United States. AWO has three primary missions: advocacy, safety, and industry image. The AWO Model Security Plan is available on the AWO Web site at www.americanwaterways.com under "Model Vessel Security Plan."

Building Security Guidance in the Domestic Passenger Vessel Industry



by GARY FROMMELT
PVA President & Project Manager; Hornblower Marine Services

September 11 challenged all our perceptions of protection of life and property. In the domestic environment, security was a concept that thwarted vandalism and theft. It secured property. Safety programs protected life.

As we were to learn in the days following the attacks, industry and government alike mobilized to secure waterborne passenger transportation. Those actions ranged from total port shutdown, to severely constrained vital operations, to confusion, to continued unrestricted operation.

The Passenger Vessel Association's (PVA) first interaction with the U.S. Coast Guard was a conference call on Sept. 12. That call brought many of our ferry operators and PVA officers and staff into direct contact with the rapidly forming port and waterway security cadre in Coast Guard Headquarters. It was obvious that many of the passenger vessel operators were taking steps to heighten security of their operations and not all were Coast Guard driven. As with the country as a whole, our members wanted to do something in response to our newly realized vulnerability.

Most of the major ports were quickly placed under Captain of the Port orders. All other ports experienced some sort of Coast Guard interaction, from recommended actions to queries asking, "What are

you doing to improve security?" Another concept that was gaining currency was "the new normalcy." The idea was that we must change—permanently. Even the most remote and smallest passenger vessel operation now had to think about what a new normalcy meant to that operation.

The PVA response was to publish a series of PVA Member Updates, transmitted regularly to members via email and fax. Those updates outlined security steps developed through the shared experience of our members, and guidance gleaned from the international-based regulations in Title 33, Code of Federal Regulations, Parts 120 and 128 and its interpretive U.S. Coast Guard Navigation and Vessel Inspection Circular (NVIC) 3-96, which were generally only applicable to large ocean-going cruise ships.

From the absence of existing plans that focused on domestic passenger vessel operations, it was clear that government and operators alike tended to default to those practices in which everyone had personal experience—airport check-in and screening procedures. While these early actions may have been a sincere effort to do something, it was not necessarily effective or sustainable for the domestic passenger vessel industry. Domestic passenger vessel operations are diverse. Our ferries and tour vessels are essentially mass transit and walk-up service operations. Dinner cruise vessels have more



DUKWs, or DUCKs, are amphibious tour vehicles that are able to travel on land and water. Photo by Ken Olsen, USCG.

in common with restaurants than transportation. Vessels that rely on charter business often dealt with groups who already had a family, business, or fraternal relationship.

To assist our members in their efforts to establish an effective and sustainable new normalcy, we embarked on creating the PVA's Passenger Vessel Security Guidelines. The process relied heavily on our members' experiences and innovations. This information was developed through round-table sessions at regional meetings, conference calls, meetings of our standing committees, and monitoring legislative and international activities.

To ensure that our efforts paralleled the Coast Guard's concept of new normalcy and that they would gain wide acceptance, we involved Coast Guard officials in our work. The interaction started with that initial conference call and continued through review draft.

PVA's Passenger Vessel Security Guidelines have gone a very long way towards establishing a common understanding between the domestic passenger vessel industry and our regulators.

They are a first step, although a giant one. Subsequent to their distribution we cooperated in a Coast Guard task group convened to develop

security screening on large passenger-carrying ferries. We also met with the Maritime and Land Security division within the Transportation Security Administration. Our 2003 annual convention featured presentations on security issues by Coast Guard and TSA experts.

In addition, PVA's internal focus continues to embrace the new normalcy. While several of our councils and committees—comprising member volunteers, PVA staff, and in some cases, Coast Guard personnel—have included security issues in their initiatives, the PVA Safety and Loss Control Committee changed its name to the Safety and Security Committee to better address this critical function. Without a doubt, this group of dedicated volunteers, many of whom spent countless hours toward the creation of the PVA Security Guidelines, will continue to emphasize the importance of security within the confines of the PVA membership and industry at large.

PVA's highest goal for the year 2003 is to refine the PVA Passenger Vessel Security Guidelines into a document to be submitted to the Coast Guard for approval as an "industry standard" for our sector. When this is accomplished, our domestic passenger vessels will have an alternative method of satisfying their legal responsibilities established by the Maritime Transportation Security Act of 2002.

One thing we know in this ever-changing statutory and regulatory arena is that security measures will evolve just as marine safety evolved—through a government and industry cooperative effort. That effort will continue to define and redefine our progress toward a new normalcy that can meet or exceed our success in passenger vessel safety.

The passenger vessel industry plays a vital role in the U.S. transportation system, carrying more than 200 million passengers each year. The Passenger Vessel Association is the national organization representing the interests of owners and operators of dinner cruise vessels, sightseeing and excursion vessels, whale watch and eco-tour vessels, gaming boats, car and passenger ferries, private charter boats, windjammers, DUKWs (amphibious vessels) and overnight cruise ships. Readers can obtain more PVA information on the association's Web site at www.passengervessel.com.



Perspectives on U.S. Security Initiatives Affecting International Liner Shipping

by CHRISTOPHER KOCH
President & CEO; World Shipping Council

As efforts to secure ourselves against the risk of terrorism continue, it is imperative for world trade that governments and industry continue to make meaningful progress in improving the safety and security of international maritime transportation systems. We are all faced with the tension between improving security and not unnecessarily damaging trade or the economy. Meaningful, sustained cooperation between industry and government is essential to develop effective multi-faceted strategies for mitigating those vulnerabilities, and to ensure that the implementation of security strategies does not unnecessarily disrupt the flow of commerce.

Containers and Liner Shipping

Shipping containers were developed as a more efficient, less expensive way to move goods. The intermodal movement of sealed containers not only reduced damage and pilferage of goods, it facilitated the development of intermodal supply chains, moving goods internationally from door to door with remarkable efficiency. More than 800 ocean-going liner vessels, mostly containerships and roll-on/roll-off vessels, now make more than 22,000 port calls to the United States each year. Last year, Americans purchased and imported goods from more than 178,000 foreign businesses. In serving

this flow of international trade, the liner shipping industry carried roughly six million containers of import cargo to the United States and carried approximately 3.3 million containers of export cargo being shipped from more than 202,000 American businesses. The value of that cargo was roughly \$500 billion, or more than \$1.3 billion per day. This remarkable system serves American importers, exporters and consumers by providing regularly scheduled services to and from virtually every country in the world. This access to an inexpensive, efficient and highly reliable transportation system not only strengthens the U.S. and world economies, but also has dramatically driven economic growth and globalization.

The principal issue and challenge facing the industry, its customers, and the governments of the international trading community is how to enhance the security of this commercial process in a way that both prevents terrorist attacks and enables trade to flow efficiently and reliably. This challenge is indeed substantial. But so have been the efforts of government and industry. At times, there have been differences that the industry has expressed regarding certain regulatory proposals. The liner shipping industry has, however, fully and consistently supported the core strategy of the U.S. government to:

- Develop a new international security regime at the International Maritime Organization covering ships and port facilities, and
- Build cooperative agreements with its trading partners that facilitate (1) pre-loading cargo manifest review, (2) notices not to load cargo that requires further review, and (3) the establishment of capabilities at ports of loading to allow security officials to inspect any high-risk container for security reasons.

Maritime security strategies must protect nations' abilities to maintain open trade even in the aftermath of a future terrorist attack. Potential responses to terrorist attacks, such as closing down all U.S. ports—or even certain vital ports—could cause severe economic damage to this country and our trading partners. Security systems must be designed to protect the flow of “safe” international commerce that has met increased security standards, while further scrutinizing the high-risk commerce that fails to meet those standards.

Organizing a Unified Government Strategy

Improving the security of international trade requires international standards, cooperation, and

implementation of new security practices. Within the U.S. government this requires a tightly integrated strategy with clearly delineated agency responsibilities, not only in detecting and preventing terrorist attacks against the international cargo transportation system and its ports, but also in adequate contingency and response planning. Such a system is logical to describe but is complicated to build. Maritime security is the responsibility of multiple government agencies with differing agendas relating to their perceived roles in the maritime security mission.

The formation of the Department of Homeland Security (DHS) has placed most of the government agencies with maritime security roles under one umbrella. These agencies include: the U.S. Coast Guard, which oversees many vital elements of the maritime security mission such as ship and port security, the Directorate of Border and Transportation Security, under which lies the Bureau of Customs and Border Protection (Customs), which oversees trade and has taken the lead role on container and cargo security, and the Transportation Security Administration (TSA), which has broad authority for transportation security in all modes, including maritime. Also in the mix are DHS's Bureau of Citizenship and



Gantry cranes load a container ship. Photo courtesy Maersk Sealand.

Immigration Services and the State Department, which have overlapping authority for foreign seafarers who enter the United States aboard international liner shipping vessels. Establishing the DHS will ultimately help resolve the organizational and jurisdictional confusion, but even with the formation of DHS, organizational protectionism, inefficient processes and redundant requirements must be subordinated by each agency to build a clear, unified maritime security system.



Hyundai containers are unloaded and transferred to a truck. Photo courtesy Hyundai Merchant Marine Company.

Once the U.S. government develops a clear vision of how security can be improved, it in many cases needs to then obtain international agreement in order to achieve effective implementation. This can be done in several ways, and it must be done, as there are obvious limitations on U.S. jurisdiction over international transportation. One example of significant progress in this regard is the Coast Guard's development of meaningful new ship and port security regulations, for which it obtained international agreement at the International Maritime Organization. Another example is the Customs Service entering into bilateral agreements with various nations as part of the Container Security Initiative—a logical approach to increasing the security of shipping in the absence of an internationally accepted program with international standards. Other security initiatives that will require international agreement include standards for seafarer credentialing documents and standards for container seals and sensors.

Cargo and Supply Chain Security

Container Security Initiative (CSI)

CSI is a program through which Customs is establishing government-to-government agreements with other nations' Customs organizations to (1) establish security criteria to identify and target high-risk containers, (2) develop and implement pre-screening processes to target and screen high-risk containers before they are loaded aboard a

vessel in the foreign port of departure, and (3) develop and deploy detection technologies to quickly screen and inspect identified containers prior to loading. CSI agreements are critical because they will help foster the continuation of trade if the industry is ever beset by a terrorist attack. Without such agreements and capabilities in place to inspect containers in foreign ports of loading, it could be difficult to provide sufficient security confidence to keep international trade flowing.

Considerable progress has been made in establishing CSI agreements,

and more progress is imminent. To date, CSI declarations have been signed covering 18 of the top 20 mega-ports for a total of 24 ports in 15 countries. These ports handle approximately 60 percent of the cargo that is transported to the United States. A possible CSI agreement with the European Union would expand the cooperative initiative and its security enhancements to even more European ports. These initiatives between Customs and its counterparts are an essential, logical core element of enhanced container security.

There are, however, several important challenges that CSI faces. First, the progress and establishment of these agreements has been, in diplomatic time frames, rapid and successful. It is important, however, for the governments involved to show that CSI agreements are more than paper documents, but are real initiatives with adequate staffing, container inspection levels and container inspection equipment, and at least some nonclassified indication that they are producing successful results. Unless this is done, questions about the adequacy of container security and CSI will continue unabated. The second challenge facing CSI is its expansion to smaller ports. Customs has appropriately focused on the largest volume ports to begin the program. But the program logically should be expanded to other ports.



A Maersk container ship enters the New York Harbor between Governor's Island and the Statue of Liberty. Photo courtesy Maersk Sealand.

Customs' 24-Hour Rule

An essential element of the CSI strategy is providing the government with cargo shipment information for screening before vessel loading. Since the rule was proposed last fall, the liner shipping industry and its customers have expended substantial time, energy and money in changing their systems and business processes to comply with the U.S. government's regulations requiring cargo information to be filed

electronically to Customs 24 hours before vessel loading. It has been expensive and difficult. But it is a clear and necessary piece of the government's strategy, and its early implementation has been generally handled with care and consideration by Customs.

Customs Trade Partnership Against Terrorism (C-TPAT)

C-TPAT is a voluntary program between Customs and industry members (importers, shippers, carriers, freight forwarders, etc.) to foster enhanced supply chain security. The principle is that if industry partners voluntarily undertake certain actions to improve their supply chain security, Customs will give their cargoes expedited treatment. C-TPAT importers, for example, are also expected to use only ocean carriers, brokers, freight-forwarders and non-vessel operating common carriers (NVOCCs) that are enrolled in C-TPAT. The World Shipping Council and its member lines have fully supported the ocean carrier portion of C-TPAT.

C-TPAT started by establishing a broad scope and ensuring all participants have security plans in place. C-TPAT now has more than 2,300 participants, including importers, carriers (all modes), brokers/consolidators/NVOCCs, and U.S. marine ports and terminals. The program includes 70 of the top 100 U.S. importers, 39 of the top 50 ocean carriers (including all World Shipping Council members), and 36 percent of U.S. imports by value. The development of "trusted shippers" under this

program appears to be moving ahead deliberately and purposefully.

Trade Act Implementation

The Trade Act of 2002 requires Customs to establish advance electronic documentation for all U.S. imports and exports in all transportation modes. While technically not part of the Trade Act requirements, Customs started with inbound ocean freight using the 24-hour rule. Customs is now examining how it will establish the cargo security rules for outbound ocean freight and for the other transportation modes.

Testing and Analysis of New Security Technologies

The government and industry recognize that new technologies may play a role in enhancing supply chain security. The most important technologies to date are the non-intrusive container inspection machines that U.S. and foreign Customs agencies are deploying to inspect the contents of shipping containers. The role and value of that technology is very clear, because it answers the most important question from a security perspective—what is in the sealed container? Non-intrusive inspection technology provides a highly efficient way to inspect containers about which security questions are raised, and, because it is the only technology that answers the above security question, its widespread deployment and enhanced use is both necessary and predictable.

It is not surprising that a host of different technology vendors are urging governments to consider their particular products as solutions to supply chain security concerns. The U.S. government is working to try to institute programs to identify supply chain gaps and assess some of these possibilities. One such program, Operation Safe Commerce, will provide funds to analyze and test supply chain security possibilities during the course of this year. While the picture in this regard is not entirely clear, initial indications suggest that the process being used to assess security technologies is becoming better informed and more analytical. There is a growing recognition that the government needs to work with industry to clearly identify and validate supply chain security requirements, because those requirements should drive technology, not vice versa.

Vessel and Port Security

The Maritime Transportation Security Act, which

became law last year, requires the Coast Guard to develop security plans and requirements for vessels and marine terminals. Prior to the passage of the MTSA, the Coast Guard had been strongly advocating that the International Maritime Organization (IMO) establish new rules in this regard, and the IMO quickly and successfully agreed to new international vessel and port facility security requirements in December 2002. The Coast Guard subsequently issued for comment an extensive set of proposals that would essentially implement the new U.S. legislation's mandate by requiring compliance with the new IMO ship and port facility security code. The Coast Guard is now developing regulations to implement various aspects of the legislation and the IMO rules, which will enter into force on July 1, 2004. The Coast Guard's effort to work with the IMO to develop this new security regime is a model of how to implement consistent international and domestic security requirements. The Council, along with many other industry representatives, supported the Coast Guard's objective to use internationally agreed IMO standards to meet the requirements of the new U.S. law.

The liner industry has been very supportive of the strategy and the leadership of the U.S. Coast Guard not only in its efforts at the IMO, but also in its domestic security efforts. Immediately after September 11, the Coast Guard implemented several measures to improve tracking of vessels destined for U.S. ports and the crews and passengers onboard those vessels. Advance Notices of Arrival (NOAs) are now required 96 hours prior to arrival in a U.S. port (except for voyages of shorter duration). Further, through its Sea Marshall program, establishment of safety and security zones, and escorts of high-risk vessels, the Coast Guard has taken steps to prevent vessels from becoming terrorist targets or weapon delivery devices.

The Coast Guard will remain a separate stand-alone agency within DHS, reporting directly to the Secretary. It will be important with this independent structure, however, that there not be duplication or inconsistent approaches with other branches of the new department. With that said, one question will be: what role, if any, does the TSA have with respect to ships and ports? Given the Coast Guard's successful record and that it is highly regarded by port and flag states around the world, it would seem logical that the Coast Guard should be given

the plenary role and full responsibility for these security matters.

With respect to containerized cargo security, however, it is and will continue to be very important that Customs be the agency responsible for cargo security. The Coast Guard should not duplicate that mission or act on container security independently of Customs. A clear Memoranda of Agreement between the Coast Guard and Customs is needed to define roles and missions in this area to avoid confusion.

Personnel Security

An estimated 200,000 foreign seafarers come to the United States each year. They are but a small percentage of the roughly 36 million foreigners who visit the United States each year for business or tourism. With that said, seafarers of all nations must be recognized as vital components of our maritime security system, and it is therefore essential that vessel operators and their crews be provided with a clear, fair and predictable set of rules.

The issues of checking and credentialing transport workers have been receiving considerable attention by the U.S. government, but viable solutions have not yet emerged. The liner shipping industry has expressed its support for the government to establish a national credentialing program, with uniform, minimum federal standards, institute a federal background check process, utilize "smart card" technology that incorporates biometric data in the credentialing of appropriate transportation workers, and negotiate an international agreement for a new international biometric seafarer identification document.

Transportation Worker Identification Cards

The TSA has been tasked with the development of a system of background checks and identification cards for U.S. transport workers. To date, TSA has not proposed implementation of any particular program or system, and appears to be struggling with the enormity and complexity of the



An APL vessel maneuvers close to shore. Photo courtesy APL.

task. There are millions of transportation workers in the United States, and different U.S. laws require different requirements for different classes of workers (e.g., truck drivers hauling explosives). The challenge of designing a system with a common set of biometric identifiers for maritime, truck, rail, transit and other workers is substantial.

International Seafarer Credentials

The United States has been supporting the development of a universal biometric seafarer identification card by the International Labor Organization (ILO). The Council has been working with U.S. officials to help formulate a position at the ILO talks that would enable a new biometric seafarer identification document to include or provide direct electronic access to the necessary data elements required for the processing of a U.S. visa. This credential is important because, given that the U.S. government is not likely to waive the visa requirement for foreign seafarers, it could conceivably enable a foreign seafarer to use his biometric seafarer identification credential to apply for and expedite visa issuance at any overseas consulate or embassy. The U.S. position at the ILO appears to support this basic objective, and hopefully the ILO negotiations will produce a clear and acceptable new set of standards and a new instrument for seafarer identification to be ready for approval during its 91st session in the summer of 2003.

Crew List Visas

The State Department has proposed the elimination of crew list visas because it has security concerns with its current crew list visa system. The Council has suggested that a final rule on this issue could be affected by the outcome of the ILO discussions on a universal biometric seafarer identification document, as discussed above. A positive decision by the ILO, which meets U.S. objectives, could, along with other international and domestic security initiatives regarding vessels and their crews, provide such new circumstances surrounding the crew list visa system that it would provide assurances against admitting undesirable persons to the United States.

If a determination were to be made, however, that abolition of the crew list visa would be warranted even after the introduction of a universal international biometric seafarer document, the State Department must address: the need for an expedited and privileged individuals visa application process for seafarers, including a significant reduction in the current visa processing time; the need for a

credible "signing off/on" visa waiver program; the need to keep costs for obtaining individual seafarer visas at a minimum; and, the possibility that other countries may impose reciprocal visa requirements on U.S. flagged and crewed vessels.

Electronic Filing of Crew Information

The Immigration and Naturalization Service (before its transfer to DHS) issued proposed rules to require the advance electronic filing of crewmember information with the U.S. government. The Council has supported the statutorily required advance electronic crew manifest submission. It will be consistent with the Coast Guard's Notice of Arrival (NOA) crewmember information requirements and will take the industry a significant step closer to what remains its ultimate goal—a single advance electronic crewmember submission per vessel to one central government repository. Until that system is created, however, we are concerned that the INS and Customs, which administers the government data system that will receive the electronic crew manifests, need to provide the industry sufficient flexibility in meeting the reporting requirements during this interim period without having to invest in new and expensive data systems.

Conclusion

Clearly there are many interlinking pieces to this maritime transportation security puzzle. The government is still in the early stages of developing procedures and rules to deal with the issues relevant to maritime cargo security. The bottom line is that carriers, shippers, ports, terminal operators, and government agencies are all in this together. Cooperative initiatives will be necessary to retain the benefits that all trading nations receive from the current efficiencies and predictable service that liner shipping provides the world's economy.

Government and industry are now engaged in an exceptionally difficult endeavor to institute safeguards against the risk of terrorism while protecting the benefits of a free society and free trade. Success is essential. It is incumbent on all the participants in this international transportation process to help the U.S. government and international community succeed. The members of the World Shipping Council are committed to helping the U.S. government succeed in these efforts, and commend those in public service and industry who are doing their best to address this new and complex set of challenges.

Cruising with Heightened Security Standards



by MICHAEL CRYE
President; International Council of Cruise Lines

In the hours immediately following the tragic events of September 11, no one could have predicted the effect it would have on the transportation industry. One of the most visible was the importance of security. The cruise industry, an industry with an enviable safety record, quickly implemented measures to ensure the highest level of security for their passengers and crew.

Through existing regulations, proactive planning, and a strong U.S. Coast Guard and industry partnership, the cruise industry was well

positioned to address the increased security demands of the post-September 11 terrorist threat. Upon hearing the news of the attacks, the International Council of Cruise Lines (ICCL) immediately became the liaison and crisis center for the cruise industry. With a goal to implement continuous communications with government agencies and a higher level of security awareness and vigilance aboard cruise ships, we initiated contact with government partners such as the Coast Guard, Immigration and Naturalization Service and the Department of Transportation.

Our first decision was to require all cruise ships to begin operating at security level III—the highest level—according to plans that were filed with the Coast Guard. Additional security measures that were not apparent to our passengers were also being implemented on the cruise ships while underway and in the port areas as well. Since the plans were already in place, the transition to security level III was accomplished swiftly and uniformly across the industry. Specific measures implemented at level III security included:

- 100 percent screening of cargo and baggage; and
- 100 percent positive identification (i.e., picture ID check) of personnel before they board the vessel.



A security guard checks the ID of passengers boarding the *Sea Princess* cruise ship. Cruise lines have increased their security checks, which are now very similar to what one would encounter at an airport. Photo by Public Affairs Officer Christopher Grisafe, USCG.



Petty Officer 1st Class O'Bry prepares to launch the CGC Pompano's smallboat to enforce a 100-yard security zone around the cruise ship *Seabourne Sun*. Photo by Lt. Dan C. Jones, USCG.

Since that day, the industry has expanded its communication efforts by continuing to work closely with the appropriate federal, state and local agencies while opening lines of communication with the FBI, Department of Defense, Department of State, and U.S. Customs to further enhance security partnerships. In addition, ICCL executives have testified on Capitol Hill in congressional hearings relating to maritime security and have done briefings for Homeland Security.

On the international front, we have been moving forward on security issues as well. ICCL supported the Coast Guard's efforts at the International Maritime Organization (IMO) to develop a resolution calling for the review, update and amendment of existing instruments related to maritime security and the development of any new conventions necessary to improve maritime security. ICCL attended the 75th session of the IMO Maritime Safety Committee. A working group was held

during these meetings to address various areas affecting the ICCL member cruise lines in matters of maritime security. Some of these areas include current security regulations; duties of ship, cruise line and port facility security officers, and the new Coast Guard Navigation and Vessel Inspection Circulars (NVICs) threat level system. The ICCL will continue to participate in meetings such as these to further address matters of maritime safety.

Many of the security requirements adopted by the IMO for all of maritime industry are measures that large passenger ships have been living with for a number of years. We are very fortunate that we had security plans in place and trained security staff that could immediately implement our security plans. A fundamental principle that I learned in the Coast Guard long ago—proper planning prevents poor performance—has proven itself once again. Our partnership and excellent communications with the Coast Guard have facilitated the planning

and execution of security measures without unduly hindering the travel vacation experience.

The cruise industry's highest priority has always been to ensure the safety and security of its passengers and crew. A cruise ship has certain inherent security advantages because of its controlled environment allowing limited access. We take every precaution to ensure everything that goes on and off the cruise ship is 100 percent secured and identified and determined to be what it has been represented to be. Because the safety and security of our passengers and crew is our highest priority, we continually embrace the newest technological innovations to enhance our safety posture and by reassuring our passengers that new security measures will not take away from the overall vacation experience.

Reassuring Americans that it is safe to travel has taken the time and talent of many people in the industry. In fact, according to a poll conducted by the Institute for Social Research at the University of Michigan, about half of all Americans feel no more safe and secure from terrorism today than they felt immediately after the September 11 attacks. The ICCL and the individual cruise lines have been actively communicating the safety and security procedures that are in place through media interviews, our respective Web sites, and direct

communications with travel agencies. The cruise industry is using every marketing and communication tool available to encourage travel and reestablish consumer confidence.

These efforts have produced excellent results. Passenger bookings are on an upward swing with many lines reporting reservation volume at record levels. In short, consumer confidence is returning and the industry is rebounding beyond anyone's expectations.

These are challenging times—not only from a security standpoint but also from a business point of view. We believe it is our responsibility as an industry to demand nothing less than the highest security for our passengers while providing them a memorable vacation experience. The Coast Guard has been an exemplary partner in our efforts.

Industry can act as the eyes and ears for government if we together develop the means to adequately share information. The Coast Guard will never have the assets to continuously protect our entire coastline. It is incumbent on us to develop effective methods to share information that can empower industry to effectively assist in this essential mission. We trust the Coast Guard, in its ever-increasing role in our national security structure, will leverage its assets by effectively utilizing industry.



A Coast Guard Station Miami Beach 41-foot patrol boat rides beside the cruise ship *Voyager of the Seas* as it transits inbound through the Port of Miami. Photo by Telfair Brown Sr., USCG.



The Pilot's Role in Maritime Security

by J. SCOTT RAINEY
Deputy Director; American Pilots' Association

The events of September 11 had a profound impact on members of the American Pilots' Association (APA), as Americans and as pilots. The day-to-day operations of pilots were impacted almost immediately by the terrorist attacks. Since September 11, our members throughout the country have been working closely with the U.S. Coast Guard helping to implement the security measures that were initially imposed as well as the measures that are currently in effect. In many places, this has required significant changes in pilotage operations.

Under normal circumstances, an APA-member pilot is the only U.S. citizen on a foreign ship moving in the fragile port and waterway system that is the lifeline of this country. The pilot comes aboard the ship while it is in U.S. waters to direct its navigation and to prevent it from engaging in unsafe operations. APA-member pilots play an important role in protecting our nation, in both normal and extraordinary circumstances.

In order to provide the nation with these critical services, pilots need to focus on their piloting tasks. Pilots are not combat personnel, security guards, law enforcement officials, or inspectors. As we consider ways to assist in enhancing port security, we need to be careful that we do not do anything that would detract from or jeopardize essential piloting functions. To do so would create a risk of an

accidental catastrophe that could have effects just as devastating as one occurring by terrorist design.

This is not to say, however, that pilots cannot provide important assistance in protecting against threats to maritime operations. Pilots are frequently referred to as the eyes and ears of a port. As the only U.S. citizens on the hundreds of foreign ships with foreign crews moving in our waters each day, state pilots know a great deal about what is happening not only on the ships but in the surrounding waters as well. They are in a unique position to detect suspicious or unusual activities.

**“THE PILOT COMES ABOARD THE SHIP
WHILE IT IS IN U.S. WATERS
TO DIRECT ITS NAVIGATION
AND TO PREVENT IT FROM ENGAGING IN
UNSAFE OPERATIONS.”**

Many of our APA member groups have already contributed greatly to our heightened maritime security posture. The United New York and New Jersey Sandy Hook

Pilots have received numerous citations for their leadership and initiative in response to the September 11 attacks on New York's World Trade Center. The Sandy Hook pilots provided their station boat, *New York*, as an on-scene command platform and assisted the Coast Guard in coordinating the maritime industry's heroic response. APA member groups have worked closely with the Coast Guard Sea Marshals. In some areas, the Coast Guard does not have adequate boats for boarding large commercial vessels offshore. In many cases, APA pilots have assisted Coast Guard personnel to board and disembark.



A pilot (on radio) talks to another vessel's pilot as the *Sealand Kodiak* transits Harro Straits through Puget Sound. Photo by John Bobb, USCG.

To further enhance maritime domain awareness (MDA), APA pilot groups share their vessel arrival and departure information with the Coast Guard and other appropriate commands, such as the Joint Harbor Operations Center in Norfolk. APA members assist in MDA in other ways as well. For example, the Charleston Bar Pilots helped establish a Volunteer Port Security Force (VPSF). The VPSF is

comprised of commercial mariners who operate routinely in the port.

In virtually every major commercial port, APA member pilots actively participate in local Harbor Safety and/or Port Security Committees. These bodies are comprised of maritime industry and government representatives who are familiar with their specific waterways and harbors. Pilots have provided needed operational input in the establishment and execution of new safety and security zones, tug and other vessel escort procedures, and other operational security measures.

Recognizing the important role state pilots play, the APA and the U.S. Coast Guard on Sept. 25, 2002 signed a memorandum of agreement regarding maritime security. A major part of our partnership project with the Coast Guard is an examination of ways to improve communications between pilots serving on ships and the Coast Guard. We are looking at communication procedures, methods, and protocols. The idea is to give quick and accurate notice to the Coast Guard of any suspicious activities, particularly onboard the pilot's ship, without compromising the pilot's duties or safety.

The APA is proud of its members' role in enhancing our nation's maritime security.

The American Pilots Association is the national trade association of professional maritime pilots. Its membership is made up of 56 groups of state-licensed pilots, comprising virtually all state pilots in the country, as well as the three groups of U.S.-registered pilots operating in the Great Lakes. APA members pilot more than 95 percent of all international trade vessels moving in U.S. waters.



A harbor pilot brings the inbound cruise ship *Voyager of the Seas* through the port of Miami while talking by walkie-talkie to tug operators. Law enforcement operators accompany the pilot onboard incoming cruise ships as part of the nation's heightened security measures. Photo by Telfair Brown Sr., USCG.



The Need for Vessel Security Officer Training

by LEN CROSS

Manager, Maritime Security Department; Han-Padron Associates

Bodies of water are carrying larger ships and transporting more passengers and greater quantities of high-value and hazardous cargo than decades ago. The shipping industry has witnessed innovative designs in ship construction and operation to handle this increased cargo/passenger load, and, as a result, training programs have been developed to prepare crews in the safe handling and operations of these ships. But, as these changes occur, we must also determine whether security training is being adjusted proportionately.

As the expansion continues, the industry's risk exposure has grown. The threats of previous years have given way to new, more lethal threats. Stowaways, narcotics smuggling, piracy and terrorism are some of the security issues facing the shipping industry. The nature of the threat varies according to the type of ship and the cargo/passengers it is carrying. Often, the individuals engaged in these activities are educated, well-trained, organized, and have an excellent knowledge of how the industry operates.

For example, many members of narcotics rings have college degrees; al Qaeda has a formalized training program with a 90+ page training manual that refers to targeting the maritime industry and recruiting resources within it for future operations. In light of this level of sophistication on the part of the enemy, the question must be asked, "Are Vessel

Security Officers (VSOs) sufficiently trained and do they comprehend the nature of the threats they face?"

Many vessels today do not have a designated, full-time VSO, and the International Maritime Organization (IMO) is currently considering whether this should be a full- or a part-time requirement for certain categories and sizes of ships. Regardless of the depth of the duty, a well-designed training program will prepare the VSO to protect the ship, to assess threats and vulnerability, understand and use protective technology, and learn to recognize and respond to a variety of emergency situations.

The VSO's role is similar to that of the Port Security Officer. VSOs continually watch for situations that could harm or adversely affect the ship, crew, passengers or cargo; they are also the first responders in an emergency. The ideal training curriculum for VSOs should be focused on four key areas: maritime, law enforcement, physical security and threat assessment.

The **maritime** section would provide the VSO with an overview of shipping operations, port operations, ship design and construction, and identification and location of critical areas of various types of ships. These subjects are important when conducting a port threat assessment and in developing a ship search plan.

The **law enforcement** element of the training would concentrate on maritime/criminal law, rules of evidence, report writing, use of force, weapons training, defensive tactics, crisis management, search techniques, crime scene management/evidence handling, communications, and identification of fraudulent documents. These courses prepare the VSO to assist the law enforcement officers in investigating events, and could help reduce the non-operating time of the ship due to legal requirements. In addition, the classes would ensure that the VSO thoroughly understands the information needed in an incident report and ensure that evidence was properly collected, preserved, and identified so that it would be acceptable as evidence in court.

The **physical security** portion of the training would include classes on planning, development and implementation of a ship security survey; access control; effective use of lighting and closed circuit television; hazardous materials incident response; alarm/intrusion detection systems; and identification of critical operation areas, such as the engine room, communication room, ventilation systems, etc. Training in physical security helps the VSO to understand the concept of *systems integration*—how all elements interact, resulting in a strong deterrent to potential adversaries.

Threat assessment is the final element to VSO training curriculum. It addresses cargo theft, piracy, narcotics smuggling, terrorism, organized crime, and stowaways/alien smuggling. The classes, taught by active law enforcement officers who have expertise in these matters, would provide VSOs



“Stowaways, narcotics smuggling, piracy and terrorism are some of the security issues facing the shipping industry.” A member of a Coast Guard boarding team arrests a man suspected of drug smuggling.

with the final tools needed to perform their tasks—knowledge of the nature of the threat and how it manifests itself.

By knowing a threat in all its forms, knowing their ships’ routines and ports of call, and knowing how to develop a strategy to combat threat, VSOs ensure the safe and secure operations of their ships and fellow crewmembers wherever they travel. In addition, a well-trained VSO reduces litigation exposure and enhances ship operations capability. A shipping line that invests in a formal training program for its VSO is adopting a *proactive* rather than a *reactive* approach to security, and is investing in ship operations, not court/legal costs.

The author is the manager of the Maritime Security Department of Han-Padron Associates, a marine engineering firm. He has 26 years of experience as a special agent with the FBI, and has worked on major terrorist and bombing cases, including the World Trade Center (1993), Oklahoma City and the SANG Building, Riyadh, Saudi Arabia.



CGC Alex Haley underway in Cook Inlet near Nikiski, Alaska while conducting a maritime homeland security patrol. The Haley will provide security for Cook Inlet oil platforms, the Nikiski liquified natural gas terminal, and the pipeline terminal in Valdez. Photo by Mark Farmer, USCG.



Coast Guard Remains Ready with Mobile Units

by Cmdr. MIKE GIGLIO

Assistant Chief, U.S. Coast Guard Office of Defense Operations

Always ready for the call. This maxim has guided Coast Guard operations for more than 200 years, and, since the tragic events of September 11, it has become more significant—and more challenging. We are all now painfully aware that “the call” can occur at any time, at any place, and be caused by a faceless enemy whose actions can impose far-reaching damage and devastation. Now more than ever, the Coast Guard must be ready to combat new and emerging threats, with little or no warning.

One way the Coast Guard has risen to meet today’s unique challenges is the establishment of new Maritime Safety and Security Teams (MSST). These domestic, highly mobile units, comprised of both active-duty and reserve personnel, provide specialized law enforcement and force protection capabilities to meet heightened port security requirements. Modeled after existing Coast Guard programs—the Port Security Unit (PSU) and the Law Enforcement Detachment (LEDET)—the MSSTs provide specialized skills and capabilities to detect, deter and prevent terrorism. MSSTs were specifically designed to protect vital commercial and military shipping and critical infrastructure against maritime threats. Possessing multi-mission adaptability, MSSTs will surge to support security requirements for major marine events, such as the Olympics and Operation Sail, and will support Coast Guard and other interagency forces performing more traditional missions, including search and rescue, counter-drug operations, and alien migrant interdiction operations.

Maritime safety and security, environmental protection, and homeland defense have always been core Coast Guard mission areas. However, significant service downsizing in the early 90’s resulted in a fundamental shift in organizational focus away from some maritime security functions. September 11 revealed an urgent need for rebuilding Coast Guard security capabilities and resulted in the rapid development of special tools and new skills to counter emerging asymmetric threats. MSSTs are just one of the tools the Coast Guard is developing to adapt to this new threat environment.

Equipped with six armed fast boats and a mix of lethal and non-lethal weapons, MSSTs provide defense-in-depth, pushing out the defensive perimeter from the ship or facility being protected. Unit personnel are trained in advanced boat tactics and weapons skills designed to prevent terrorists from reaching their objective. The Coast Guard is also leveraging advanced technology to improve the MSST’s ability to interdict chemical, biological, radiological and nuclear (CBRN) agents and high explosives concealed in merchant shipping.

A key factor in the MSSTs’ success is their ability to coordinate and operate with other Coast Guard, government and private sector groups. The coordination function will be performed by the MSSTs’ planning branch. The planning branch provides expertise in marine safety and regulatory responsibilities and will interface with Port Security Committees, which are composed of government and private sector stakeholders. Planning staffs will ensure that MSSTs are familiar with port activities,

port security and other contingency plans, port vulnerabilities, and risk mitigation strategies.

As a military service and branch of the armed forces, the Coast Guard maintains a state of readiness to support the Navy during times of war and other contingencies. Coast Guard platforms and personnel provide unique, non-redundant capabilities to augment Naval forces at home and abroad. To ensure interoperability with the Navy, MSST personnel are trained in joint tactics, techniques and procedures at the Coast Guard's Special Missions Training Center located at Marine Corps Base Camp Lejeune, N.C. There they receive training in advanced boat tactics, use of lethal and non-lethal weapons, and advanced law enforcement tactics. The Navy and Coast Guard are expanding opportunities to integrate training, which will provide the synergy needed for the services to work together. This ultimately enhances performance in the field and ensures standardization of doctrine and tactics. Four teams have now received this specialized training.

Structured for quick response, the MSSTs will be ready to go anywhere at any time—boats and crews will be able to load and deploy via ground or air transportation to any domestic port in the United States and its territories within hours of notification. They will perform 24x7 day and night operations, and will be capable of remaining on-scene for weeks at a time. These new and unique teams fill a vital role in our nation's response to terrorism, and they provide the Commandant with a highly effective tool to combat maritime related threats to national security. Out in front once again, these teams prove the Coast Guard's centuries old commitment to answer "the call"—whenever it happens and in whatever form it takes.

Organizationally, the MSSTs fall under the operational control of the two Area Commanders who are responsible for Coast Guard operations nationwide. Once deployed and depending on the nature of the mission, tactical control may be assigned to a Group Commander, Captain of the Port, or other appropriate unit commander. Each MSST is commanded by an active duty officer, and is comprised of 104 Coast Guard men and women (71



active-duty augmented by 33 reservists). The MSST can be deployed as a single unit or in flexible force packages tailored to meet mission requirements. This operational flexibility is a key attribute of the MSST that allows for unit employment in a wide range of maritime security missions.

The first four MSSTs were commissioned in Seattle, Wa., Chesapeake, Va., Galveston, Texas, and San Pedro, Calif. Two more teams are included in the President's 2003 budget and additional teams are being considered as part of the Coast Guard's multi-year resource plan. As the lead federal agency for Maritime Homeland Security, the Coast Guard has set a clear course for enhancing the Nation's security and MSSTs are a vital component of the service's strategic plan.



TOP: Petty Officer 3rd Class Robert J. Dellavalle practices his defense tactics on his partner, Petty Officer 3rd Class Bradley M. Krise, while instructor Petty Officer Ryan T. Fry supervises. All are members of MSST 91103. Photo by Petty Officer 4th Class Lance Jones, USCG. **BOTTOM:** MSST members and Petty Officers Thomas Duffy (left), Jason Miele (center) and Nicholas McConnell patrol near the Statue of Liberty. Photo by Petty Officer Tom Sperduto, USCG.



Increased Coast Guard Assets for Homeland Security

by Cmdr. CHRIS CARTER
Chief, U.S. Coast Guard Migrant Interdiction Division

Since the tragic events of September 11, the U.S. Coast Guard has placed an increased emphasis on the port security mission under the broad legal and regulatory authorities of our captains of the port (COPTs). In the popular press, this activity is typically described as being carried out by "Coast Guard Sea Marshals." This is because the first visible response to the terrorist attacks was to place small teams of armed Coast Guard personnel aboard vessels entering or departing ports to secure access to the bridge of the vessel, protecting it from terrorists or hijackers, especially in the Pacific area. Since then, a more complete set of capabilities has been developed. As we shall see, Operation Sea Marshal now refers to one of several compatible law enforcement capabilities and is not simply a job title.

The National Strategy for Homeland Security aligns and focuses homeland security functions into six critical mission areas: intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response. The Coast Guard has responsibilities in all of these areas.

The Coast Guard's maritime homeland security (MHLS) mission is to prevent a terrorist event from occurring in or via the maritime domain of the United States. To achieve this mission, the Coast Guard will:

- Achieve and maintain maritime domain awareness;
- Detect, deter and defend against any attack;
- Monitor and control the movement of high-interest vessels;
- Defend maritime borders, ports, waterways and coastal approaches;
- Safeguard the U.S. maritime transportation system and protect critical infrastructure; and
- Reduce America's vulnerability to terrorism.

MHLS starts with Risk-Based Resource Management. A risk analysis conducted shortly after Sept. 11, 2001 concluded that the 55 largest ports in America handle more than 90 percent of all traffic and cargo. Of these, the top 18 are considered to be militarily or economically strategic "tier one" ports. To fight the war against terrorism, the Coast Guard will initially concentrate its efforts on these ports, and other heavily trafficked or critical sea lanes and waterways while expending a reasonable effort to surveil all other maritime areas. To accomplish these duties without significant negative impact on traditional missions such as fisheries enforcement and migrant and drug interdiction, we are adding a number of assets and personnel to Team Coast Guard:

Small Boat Allowances: These resources, and the necessary support personnel, are being added to "plus-up" selected Marine Safety Offices (MSO) and Groups with additional patrol and escort capability. This will provide an enhanced capability to

conduct shore-side and waterside harbor patrols, to enforce security zones established by the COTP, to conduct security boardings and escorts of high-interest vessels and to provide increased presence within and surveillance of U.S. ports and waterways.

Maritime Safety and Security Teams (MSSTs): The Coast Guard is also in the process of deploying these mobile, multi-mission law enforcement/force protection assets primarily focused toward improving port security and harbor defense capabilities in our nation's strategic seaports. MSSTs are equipped with armed fast boats, specialized detection systems and personnel trained in the tactics and techniques for enforcing Department of Defense Restricted Areas, Naval Vessel Protective Zones, security zones established by the COTP to protect naval vessels, Military Sealift Command (MSC), Ready Reserve Force (RRF), or commercial vessels carrying critical military cargoes, other high-value assets (e.g., cruise ships and liquid and natural gas [LNG] tankships), and other critical port infrastructure. MSSTs will enhance the Coast Guard's MARSEC 1 security posture and will be able to deploy nationwide. MSSTs will be staffed with qualified Coast Guard boarding officers and boarding team members possessing specialized skills for performing anti-terrorism/force protection missions.

Operation Sea Marshal: We are adding law enforcement personnel in military or economically strategic ports for Vessel Security Team (i.e., "Sea Marshaling") duty. These teams are designed to provide positive control of high-interest vessels (HIV) by protecting them from internal threats (terrorist hijacking) to ensure that the vessel remains under the control of the Master and the direction of the Pilot, and to provide valuable on-scene situational awareness. HIVs are commercial vessels that may pose a relatively high security risk to the United States.

A security boarding of an HIV is a risk management tactic that provides the operational commander with valuable information to optimize the evaluation and mitigation of risks. Because the Coast Guard will employ its organic law enforcement authority to board, search and inspect as necessary, and specific COTP authorities to control the movement of vessels in the U.S. territorial sea,



A Coast Guard law enforcement officer stands watch on the bridge of a merchant vessel during transit of the San Francisco Bay.

Vessel Security Teams will be led by a qualified boarding officer as defined in the Coast Guard Maritime Law Enforcement Manual.

To safely operate in a fluid threat environment, Vessel Security Teams [boarding officers] will perform initial safety inspections, ensure space accountability (when appropriate), and be able to locate stowaways, chemical, biological, radiological, nuclear (CBRNE), and other contraband. To accomplish these tasks, teams must possess some

limited marine safety expertise. Because law enforcement personnel may encounter terrorist activity, the program must include the necessary interagency relationships to ensure the availability of prompt and appropriate federal, state or local law enforcement response for this contingency.

We are also capitalizing on enhanced counter-terrorism intelligence and vessel movement information to assess and respond to MHLS risks. This will be done by assigning intelligence teams in various ports, improving secure communications capabilities at groups, MSOs, and stations, and adding personnel for maritime domain awareness operations center watches.

Finally, Automatic Identification System (AIS) receivers will be installed in various locations. AIS can provide information such as identification,

position, heading, ship length, beam type, draft and hazardous cargo information from any AIS-equipped vessel. This information will be captured and displayed to improve maritime domain awareness.

The combination of improved information, enhanced intelligence, secure communications, and additional vessels and personnel dedicated to MHLS in the most critical militarily or economically strategic ports

will facilitate the groups' and stations' ability to support the COTP/MSO in successfully carrying out their port security mandate and achieve the objectives of the MHLS mission.

These initiatives will make our ports and waterways safer for both the maritime industry and recreational boaters.

Mission Areas of the National Strategy for Homeland Security

- Intelligence and Warning,
- Border and Transportation Security,
- Domestic Counter-terrorism,
- Protecting Critical Infrastructure,
- Defending Against Catastrophic Terrorism,
- Emergency Preparedness and Response



A Coast Guard law enforcement officer communicates with other Coast Guard assets to ensure that security is maintained around a merchant vessel.



Homeland Security

Foreign Passenger Vessel Security Program

by Cmdr. ALAN MARSILIO,
Lt. BUDDY REAMS, and
Lt. MATT EDWARDS
U.S. Coast Guard Marine Safety Center

The effects of the September 11 terrorist attacks have been felt throughout the U.S. Coast Guard in numerous ways, forever changing the way the Coast Guard does business. Marine safety personnel, already tasked with ensuring safety on commercial vessels, have become key in the Coast Guard's role as sea guardians for homeland security. One specific area that has been dramatically impacted is the foreign passenger vessel and passenger terminal security program. The Marine Safety Center (MSC), charged with the review of vessel construction plans, has helped lead the way to improved security on passenger vessels, both foreign and domestic, that call on U.S. ports. The MSC was one of the first units to identify necessary changes and to see that they were captured in implementing guidance, the new Navigation and Vessel Inspection Circular (NVIC) 4-02, "Security for Passenger Vessels and Passenger Terminals."

What is the Foreign Passenger Vessel/Terminal Security Program?

The Foreign Passenger Vessel/Terminal Security Program had its inception as a result of the murder of a U.S. citizen, Leon Klinghoffer, during the hijacking of the passenger vessel *Achille Lauro* in 1985. While this incident did not occur in U.S. waters, it became apparent that proactive steps

would be necessary to avoid such future atrocities. The requirements for the Foreign Passenger Vessel/Terminal Security Program are codified in 33 CFR 120 and amplified by NVIC 3-96 (superceded by NVIC 4-02). This program requires a vessel security plan for each foreign passenger vessel over 100 gross tons, carrying more than 12 passengers for hire, and making voyages more than 24 hours (any part of which is on the high seas) that embarks or disembarks passengers in a U.S. port. Likewise, a terminal security plan is necessary for any terminal receiving one of the aforementioned vessels. This requires the operators of vessels, predominately cruise ships, and passenger terminals to examine and document the assets, procedures, and policies necessary to ensure a minimum level of security.

This program originally called for the National Maritime Center (NMC) to review vessel security plans and for the captain of the port (COTP) to review the Terminal Security Plans in their zone. In 1999, the responsibility for the vessel security reviews was transferred to the MSC.

There are some similarities between the applicability requirements of the Coast Guard's Control Verification Examination (CVE) Program and the Vessel Security Program (VSP), as it relates to cruise

ships. The CVE program applies only to those foreign vessels "embarking or disembarking" passengers at U.S. ports, which essentially means at least one passenger is beginning or ending their voyage in the U.S. The VSP program applies to all of these vessels but extends coverage to any foreign vessel that discharges passengers in U.S. (or its territories) ports, even if those passengers came from foreign ports, are only sightseeing in the U.S., and will return overseas on the same vessel during the same voyage.

NVIC 4-02 implemented sweeping changes in the type of security measures expected and also placed a deadline on submitting revised plans, a step to accelerate the implementation of the new measures. A primary goal of NVIC 4-02 is to mesh the Vessel Security Plans with the Terminal Security Plans to create a family of robust, comprehensive plans to deter a terrorist threat on a vessel at any of its U.S. ports. NVIC 4-02 requires the operators of all affected vessels (approximately 190) to incorporate new guidance and resubmit their security plans to the MSC for Coast Guard approval.

How did we do it?

Vessels that do not comply with the NVIC 4-02 standards, i.e., possess a security plan approved by the MSC, will soon be prohibited from entering a U.S. port. It was therefore necessary to identify those vessels that visit or will be visiting U.S. ports and alert their operators of this new guidance. An initial list of passenger vessels involved in the Coast Guard Port State Control program was generated and their owners were quickly notified. Finalizing the list of those vessels not currently in the Port State Control program required a complete search of all previous records to obtain a list of vessels

historically calling on U.S. ports. This entailed searching through nearly five years of correspondence regarding security plan review. The next task involved determining which of the vessels had changed names or owners. Finally, we found addresses for all the owners/operators and sent them letters explaining the changes and the accelerated timeline for submitting the changes. While we recognized that this list of affected vessels would not be all-inclusive, our goal was to initially receive security plans from 90 percent of all vessels identified in our document search.

The new Vessel Security Plans have to be received and reviewed, and correspondence needs to be generated in an expedited manner. As such, it was essential that a process be developed to carry out these tasks. The status of all vessel plans is tracked in a database. At any given time, it is easy to determine what plans have arrived and are in the review process, what plans have been returned for revision, and what plans have been approved. It was equally important to formulate plan review guidance and create standard comments for plan review letters. A work instruction was developed for staff engineers to identify key areas of the security plan and to determine what is acceptable based on the new standards. Concurrently, standard comments were written to expedite the staff engineers' review as well as to promote consistency.

Where are we now?

Vessel owners and operators and the MSC staff are in the final stages of this process of updates. In an effort to reduce the number of times a plan is resubmitted for review, we hosted industry meetings to detail our concerns and expectations for each section of the NVIC. This coupled with the meticulous comments presented in our plan review correspondence will help the operators of cruise vessels calling on U.S. ports to quickly meet the country's new security expectations. In addition to providing the highest level of security reasonably possible onboard foreign passenger vessels, this process has been invaluable in laying the groundwork for the Coast Guard's efforts to implement and integrate the requirements of the recently enacted domestic Maritime Transportation Security Act and the International Ship and Port Facility Security Code. These comprehensive standards will eventually encompass virtually every class of vessel operating in U.S. waters and all are based on a robust, flexible, and consistent set of security plan expectations.



Petty Officer 2nd Class Travis Sanders, a boarding officer with MSO Mobile, looks for foreign vessels due to arrive in the Port of Mobile using the Ship Arrival Notification System (SANS). Photo by Public Affairs Officer Chad Saylor, USCG.



Operation Safe Commerce—Northeast

Container Security Through Partnerships

by Public Affairs Officer AMY THOMAS
U.S. Coast Guard 1st District

Cargo container security and documentation, specifically for cargo entering the United States from foreign countries, is the focus of a public-private sector partnership in the 1st Coast Guard District. Although standards have existed since the 1940s for cargo container size and weight limits, there was no standard for verifying the containers' contents before they were loaded onto ships, trains and trucks and routed through global distribution channels.

The U.S. Attorneys for the Districts of New Hampshire and Vermont, along with the Governor of New Hampshire, the U.S. Marshal for the Districts of New Hampshire and Vermont, the 1st Coast Guard District Commander, and others, formed Operation Safe Commerce (OSC)—Northeast to respond to the potential threat to homeland security from the 1.2 million cargo containers entering the United States through the ports of Montreal and Halifax each year. The challenge for OSC Northeast was to safeguard containers entering the country without impeding the flow of commerce.

"This is a new world for us in terms of figuring out who our partners are, and trying to define what the

processes are of the whole supply chain," said Rear Adm. Vivien Crea, commander of the 1st Coast Guard District in Boston.

Using theories developed by Stephen Flynn, a retired Coast Guard commander and now Senior Fellow on the Council on Foreign Relations in New York City, OSC—Northeast's goal is to "push back the borders" by validating legitimate cargoes at their points of origin. This, Flynn theorized, would keep potentially dangerous weapons or components as far from American shores as possible.

Rear Adm. George Naccara, Adm. Crea's predecessor, and Capt. Peter Boynton on the 1st Coast Guard District staff, joined in OSC—Northeast. Through their leadership, they sought to involve the Coast Guard and use its maritime safety and port security role in helping to prototype safeguards for the container supply chain.

With Flynn's theories in its back pocket, the OSC—Northeast steering committee set out to determine just how vulnerable cargo containers, borders and global supply chains were. The objective was threefold. Committee members sought first to define the end-to-end supply chain relationship;



Coast Guard Petty Officers Leah Ingram and Chris Bolin conduct a security round on the liquefied natural gas tanker *Polar Eagle* at a transfer facility in Nikiski, Alaska. The two Coastguardsmen are part of a four-person Sea Marshal's security team dispatched from MSO Anchorage to assess the vessel's security and provide additional protection during its transit through Cook Inlet. Photo by Public Affairs Officer Keith Alholm, USCG.

second, to survey low-cost seal, intrusion and tracking systems; and third, to conduct a demonstration of an instrumented cargo container belonging to volunteer private manufacturer Osram Sylvania.

"Nobody had actually tracked and documented each step of the process of manufacturing and importing goods, much less what gates they had to go through," Crea said.

Officials with the Volpe National Transportation Systems Center, in Cambridge, Mass., installed sensors, intrusion alarms and tracking devices on the Osram Sylvania container in order to monitor the container's progress on its journey from Slovakia to Hillsborough, N.H.

At the conclusion of the test run from Slovakia, future recommendations for successful OSC programs were made. First, OSC programs should be conducted in conjunction with similar govern-

ment and industry initiatives to ensure the best results. Second, all participants should agree on the supply chain evaluation criteria. Last, all future OSC initiatives should be designed to optimize security, mobility and economic influence.

Concurrent with OSC-Northeast, a similar project was developed in Boston. Its focus is to secure U.S. seaports and to enhance security practices already in place. Boston-A Model Port completed its first phase in June 2002 with the signing of a charter by the members of the steering committee. Its membership includes Coast Guard Captain of the Port of Boston, Coast Guard Group Boston, the FBI, U.S. Customs Service, state of Massachusetts, city of Boston, MASSPORT, and other local governments and private sector participants.

Charter members of Boston-A Model Port examined the knowledge learned from the successful coordination of high-visibility transits, such as

liquefied natural gas (LNG) tankers through Boston Harbor, and are applying that knowledge across different types of port activities.

“Seaports are critical in the safe and secure movement of goods and commodities, the cornerstone of global economy. Thus the whole environment of the seaport is the focus of Boston’s efforts,” said Lt. Cmdr. Robert Crane of the Coast Guard’s Maritime Homeland Security division in Boston. Consequently, Boston–A Model Port created work groups composed of numerous stakeholders to analyze the safety and security of bulk cargoes, passenger vessels, consequence management, intelligence networking and other security measures within the seaport.

Similar to OSC–Northeast and Boston–A Model Port, the New York/New Jersey Mega Port project will address the security of the millions of containers carrying vastly diverse cargoes into that port. With the Port Authority of NY/NJ taking the lead, the Mega Port project focuses on more complex international supply chains, specifically those between megaports. The project will provide more detailed descriptions of global supply chains and prototype technology and methods to secure those supply chains. Additionally, the project will capture and share best practices among government and private sector entities.

Plans are to analyze gaps in the security of the supply chains of several volunteer shippers who routinely move goods originating in Europe and Southeast Asia.

Additional projects under the auspices of OSC are emerging elsewhere across the country. Congress, through the 2002 Supplemental Appropriations Act for Further Recovery From and Response to Terrorist Attacks on the United States (Public Law 107-206), provided grant funds for OSC to improve the security of international and domestic supply chains through discreet pilot projects involving the three largest container load centers. As a result, the Port of Los Angeles/Long Beach, Port of Seattle/Tacoma, and the Port Authority of New York and New Jersey have submitted proposals for funding under this initiative. These grants are scheduled to be announced by TSA during the summer of 2003.

To be successful, Crea said she thinks that engaging the private sector is the most important step. “If they know where their goods are, and have some predictability of when they’re going to arrive, they can reduce their costs significantly,” Crea said. “There’s definitely an incentive.”

Inspecting the millions of containers that enter the United States every year is a task that is next to impossible and could bring trade to a virtual standstill. Through the partnering of government and industry, limited resources can be put to more efficient use to keep commerce flowing smoothly. According to Crea, if 95 percent of the containers coming in have been packed and shipped by trusted partners, more focus can be placed on the other 5 percent that were not.

“We don’t have any choice,” said Crea. “We are a maritime trading nation. Clearly, it’s preferable to keep [the threat] as far off our shores as possible. If we can push back to the source port and start the chain of custody there, it’s less of a threat to us.”



Petty Officer 2nd Class James Benton checks to see if the seal on a container has been tampered with. Photo by Public Affairs Officer Dana Warr, USCG.



Smart Card Technology in the Maritime Transportation Industry

by JIM ZOK

Associate Administrator, Financial Approvals & Cargo Preference; MARAD

In the post-September 11 world, there is a continuing need to assess potential national security vulnerabilities. The transportation system is working diligently to identify any security gaps and propose technical and procedural solutions that would seal those breaches. Because the marine transportation system moves the majority of the products and goods into and out of the country, there is an especially urgent need to address problem spots and head off potential threats. Technology provides a number of effective methods for addressing immediate and long-term vulnerabilities—and interoperable “smart card” technology offers great promise in this area.

According to *Government Smart Card Interoperability Specification*¹, published by the National Institute of Standards and Technology (NIST), “A...smart card system consists of a host computer with one or more smart card readers attached to hardware communications ports. Smart cards can be inserted into the readers and software running on the host computer communicates with these cards....” In addition to the core data used to identify the cardholder, a smart card could be enhanced with biometric data such as fingerprints, facial geometry, and iris scan. Smart cards become “interoperable” when they are created in such a way that different vendor cards can function with other vendor software and smart card readers. (The NIST specification named above outlines how this can be achieved.)

Currently working groups within the International Organization for Standardization (ISO) are using the NIST Interoperability Specification as a draft work item for the development of an ISO Interoperability Smart Card Standard. In addition, many other standards defining biometrics and data formatting are being developed at ISO and other standards bodies to support credentialing efforts and promote interoperability. International organizations such as the International Maritime Organization (IMO) and International Labor Organization (ILO) are working on how to implement these technologies to benefit the safety and efficiency of the global maritime industry.

Potential applications within the marine transportation industry for interoperable smart cards are numerous. For example, the Merchant Mariner Document (MMD) card issued by the U.S. Coast Guard could incorporate a computer chip into the card enabling it to contain data on licenses and certifications, as well as other pertinent information such as lifeboat and tankerman endorsements. Data that the mariner is required to carry at all times could be stored on the card, as could training and assessment information used by unions, shipboard officers, training schools, the Coast Guard, and the mariners themselves. Having such an electronic system for the MMD, the Coast Guard could find it easier to automate Regional Examination Centers (RECs) and mariners could keep better track of their competency and verify course completion more easily. Information on the card can be protected to allow only persons with

the proper authority the right to access, read and write to appropriate data elements as defined by the business rule.

Smart card technology could make controlling access to ports much easier and make ports significantly more secure. When a mariner wants to enter a port, the controlling facility would use the information provided on the card to determine whether access can be granted. The number of options for the card to interface with facility security systems is many, and affects the degree of security at a given facility. The facility's security plan and business processes would define the degree of security required, and ultimately the most effective and efficient way to implement the technology. The smart card of a foreign mariner could contain passport, VISA and Immigration and Naturalization Service (INS) information verifiable through a secure connection to the issuing organization. Biometric data can positively match the person holding the card to the identity carried on the card. The biometrically verified identity could then be checked against any globally distributed "watch list."

It is possible port administrators, unions, or port operators could issue cards to port workers that, in addition to the usual identification and biometric data, could also contain notes regarding key skill or training areas or specific access limitations. Using the smart card technology to control port access

could also be applied to truckers who transport goods to and from the ports via land routes.

What benefits can be realized by integrating the smart card technology into the marine transportation system? The movement of people and goods through the system would be greatly enhanced,



Copyright © 2003 USCG and its licensors.

while providing an optimal level of security not easily achieved today. A secure integrated network of information would allow various organizations to limit access to their facilities as their policy dictates. These same sources could be queried as needed to provide a variety of security-related information, and intelligence entities would be able to broadcast alert messages as needed.

Even with the possibility of so many benefits, though, objections have been raised to this technology. An important hurdle to be overcome is the issue of individual privacy. An advanced technology card that contains personal information could draw opposition. Balancing one's privacy rights against national security is an issue that is drawing debate, and one

that would have to be resolved before a comprehensive form of smart card technology could be implemented for the marine transportation industry. In addition, trust levels for specific data ownership and security must be established before data exchange agreements can be reached.

What is needed before we can move forward with a comprehensive program of smart card interoper-

ability for the industry? At a minimum, there are several goals that come to mind. Some would have to be successfully completed for the program to work effectively, while others need only to be started for the maritime community to realize benefits.

1. Increase and promote standardization of tokens (smart cards) and the interoperability of the required databases. A number of standards need to be in place to guarantee success. Fortunately, a number of initiatives are already underway. In addition to the NIST smart card specification mentioned earlier, the U.S. General Services Administration (GSA) and NIST are working with several agencies and organizations to develop standards for structured security and data protection. Further, GSA and NIST are working with private industry to create international standards. Through the ISO there exist working groups that are developing biometric, smart card and database standards to address interoperability issues. Ongoing efforts at the International Civil Aviation Organization (ICAO), the IMO and the ILO are also assisting to drive standards to the international level.

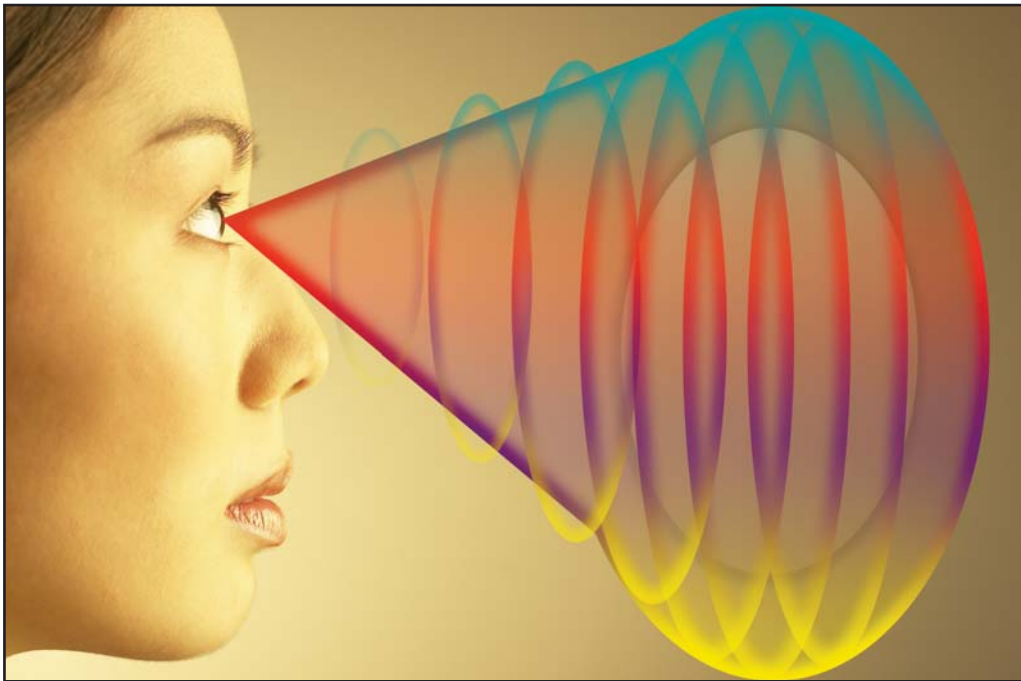
2. Coordination of federal government efforts for smart card and database interoperability. In order to implement smart card technology

and share security information, federal agencies need to work in concert to create a coordinated plan for smart card interoperability. The informal interagency advisory board created by GSA has proven an effective forum to exchange ideas and improve practices. The efforts led by the Office of Management and Budget have also aided the federal government's progress towards accomplishment of this goal. Procurements must be handled through a single contracting vehicle, the GSA "Smart Access Common ID Contract." Finally, numerous agencies must identify their existing identification card projects or requirements that are candidates for system integration efforts or which could be upgraded and consolidated, using interoperable smart cards.

3. Coordination between government agencies (including state and local governments), as well as corporations, unions, and other entities. The federal government will need to provide strong, visible leadership to promote the development, implementation, and continued use of standards for smart cards, biometrics, and vendor interoperability. For the maritime industry, the federal government will have to promote and encourage the use of smart card technology with regulators, ports, unions, ship operators, and owners. In addition, the federal

government will have to assume leadership and coordinate a whole host of related policy issues such as privacy, liability, process and work flow standards, risk assessment methods, systems interfaces, security standards, audit processes, appeals practices, etc.

4. Investigate funding requirements for full implementation of federally mandated smart card technology. Decisions must be made on how such a program would be cost shared or funded and how fees will be determined and collected. State and local governments will need to determine their funding requirements as well, and indicate whether assistance



"In addition to the core data used to identify the card holder, a smart card could be enhanced with biometric data such as fingerprints, facial geometry, and iris scan." USCG illustration. Face image and fingerprint on page 81 are copyright © 2003 USCG and its licensors.

(in the form of grants, cost sharing, etc.) would be needed for implementation. The maritime industry must identify its fiscal needs, securing whatever loan guarantees or other financing mechanisms may be required.

5. Develop test beds to evaluate technologies and determine best practices for the maritime environment. During his congressional testimony on April 9, 2003, Secretary Tom Ridge of the Department of Homeland Security (DHS) highlighted the Transportation Security Administration (TSA) Transportation Worker Identification Credential (TWIC) project as a prime example of the use of technology to improve security and facilitate trade across all the transportation sectors. The TWIC is currently initiating two regional pilot programs in the greater Philadelphia-Wilmington and Los Angeles-Long Beach areas, which will evaluate a range of advanced identification and information technologies at six to 10 facilities in each region. The TWIC program supports the requirements of the Maritime Transportation Security Act, which requires an increase in transportation worker security, by enhancing access control for individuals requiring unescorted physical access to secure areas of the national transportation system (maritime, aviation, transit, rail, and other surface modes). As another specific example, the Ship Operations Cooperative Program's (SOCP) Smart Card Project is investigating the development of a mechanism to facilitate mariner tracking, training, and certifications; expediting shipboard mariner sign on/sign off; and the need to improve security for both ships and port facilities. With the support from other interested organizations, SOCP is working with its maritime industry partners to evaluate smart card technologies and consider potential applications that would add value to the maritime industry. Inherent in the design and implementation of a Mariner Administrative Smart Card for the industry, SOCP has recognized the need for an open and expandable system architecture to accommodate future maritime industry business requirements and desires. With that key goal in mind, SOCP is working closely with its members and industry



partners to ensure that technology fielded in a SOCP Mariner Administrative Smart Card Demonstration satisfy this requirement.

Smart card technology offers many security benefits to the marine transportation industry. Proper implementation of this technology would provide expandability and could be built upon in the future to enhance system operation and effectiveness. Though many issues need to be worked through, it is a technology that will allow us to enhance the movement of goods and people through the system while at the same time providing an improved level of security.

¹ National Institute of Standards and Technology (NIST) Interagency Report 6887, Version 2.0, dated July 8, 2002. Available in PDF format on the NIST Web site: <http://smartcard.nist.gov/gscis.html>.



Technology for Port Security

by RIC WALKER

U.S. Coast Guard Research & Development Center; CATs-I Information Center

The terrorist attacks of September 11 moved a lot of cheese. The 1998 best seller, *“Who Moved My Cheese?”* by Spencer Johnson, M.D., is a simple parable that reveals some profound truths about change, and how we deal with it. Our world has changed, our lives have changed, and security is foremost on everyone’s mind these days.

The U.S. Coast Guard is no exception. The nation’s ports are critical to our economic vitality. They are among the most valuable and most vulnerable assets of the country, and the Coast Guard is on the frontlines of the port security challenge.

Port security is not a new mission for the Coast Guard, but it has obviously taken on a new urgency and a higher priority since September 11. Terms like maritime domain awareness, high-interest vessels, and threat assessment are common as we search out the new location of the *cheese*.

The Coast Guard Research & Development Center has also responded to the shift in priorities swiftly and decisively. For example, numerous R&D Center technical staff deployed to several ports to assist in response activities. An additional goal was to document areas where improved technology might enhance Coast Guard mission effectiveness in securing our ports against terrorist attacks and other threats in the future.

The insight gained during this time was key in formulating how we might best help the Coast Guard to fulfill their missions. The result was a new R&D Center program—the Captain of the Port (COTP) Advanced Technologies Integration

program, known as CATs-I. The purpose of this program is to evaluate advanced technologies to enhance the Coast Guard’s port security capabilities and to improve COTP and Group-level command centers. The technologies and concepts being evaluated will provide an integrated toolset of capabilities to establish local domain awareness and to prevent and respond to incidents in the port environment.

Working with the area commanders, Miami/Port Everglades and the port of San Francisco were identified as key partners. They serve as “operational laboratories” for the test and evaluation of technologies for improved security. The R&D Center has partnered with COTP, group, and local stakeholders in the two ports to identify the most critical port security performance needs. Several technologies were identified for test and evaluation that will address these performance needs.

The purpose of CATs-I is not merely to test equipment, but to evaluate technologies and provide information that will assist the Coast Guard in the acquisition of new systems for improved port security. Characterizing the cost and performance tradeoffs of new technologies is one of the key elements being provided for informed decision making. In addition, the R&D Center is working with operational staff in the ports to develop a concept of operations for each technology to ensure the most effective integration into Coast Guard operations.

CATs-I Technologies

The R&D Center is investigating the following CATs-I technologies:

Common Situation Display System (CSDS)

CSDS is a Web-based information display and distribution system for establishing, maintaining, and communicating situational awareness in near real time to Coast Guard and non-Coast Guard decision-makers. It was developed utilizing the National Interagency Incident Management-Incident Command System (NIIMS ICS) protocols to support daily operations and to provide all pertinent incident response data, forms, geographic displays, and response asset tracking to members of a Unified Command via the Internet. CSDS provides access to Coast Guard incident response information from outside the Coast Guard Intranet firewall, which allows for the expeditious flow of information between the Coast Guard and non-Coast Guard Unified Command partner agencies.

Protected Voice Comms

The Protected Voice Communications system consists of hard-mounted and portable satellite phones. It is designed to provide communications when port or land infrastructure is destroyed or overloaded, or vessels are operating in known communication dead zones. Satellite phones allow communications between interested parties without resorting to radio broadcasts, thereby providing some protection to the flow of information. These commercial off-the-shelf (COTS) satellite phones are intended to supplement current and soon-to-be-procured Coast Guard voice systems. They should provide another alternative for critical communications with other agencies, such as police and firefighters, the Drug Enforcement Administration, FBI, and Immigration and Naturalization Service, connecting units both on shore and afloat.

Blue Force Tracking

This system is designed to acquire and display the position of Coast Guard and other friendly assets (blue force) while underway in the port. This information may be provided to the appropriate command centers via the CSDS. The graphical display of the location of blue force assets is a key

element for situational awareness and should lead to improved command and control and incident response. Automatic Identification System (AIS) technology will be assessed for the operational benefits it may provide for blue force tracking. The AIS gathers and distributes live vessel movement information, including a vessel's identification, position, course, and speed. CSDS has the capability to present this information using icons on a chart for a CATS-I view of the asset distribution throughout the port.

Exclusion Zone Barriers

In recent months numerous security zones have been established to help protect critical port assets and infrastructure. The Coast Guard is also much more serious about enforcing these and other secure zones that may have existed before September 11. To aid in this process, exclusion barriers are being designed to keep intruders out of secure areas or away from vulnerable vessels or facilities. They can range from simple floats that mark a line of a security zone to sophisticated systems that can stop a moving vessel.

Trip Wires

One of the capabilities that is essential to port security is the rapid response to suspect activities. Trip wires are designed to decrease response time by providing an alert when an intruder approaches a security zone. A variety of technologies are used in land-based systems to protect homes and businesses but have not been evaluated in a marine environment. Trip wire sensors may be combined with exclusion barriers and surveillance systems for an integrated approach to protecting critical assets.

Day/Night Surveillance

One of the main goals for improving port security is enhanced local domain awareness. Surveillance systems are capable of providing a continuous view of the activity in a port. The Day/Night Surveillance system being investigated under this program consists of a long-range, infrared camera

Coast Guard officers posing as terrorists are quickly apprehended during a port security exercise in Port Everglades, Fla.





Capt. James Watson, COTP Miami, discusses improvements in port security as a result of new technologies, like the Port Security System being tested under the Research & Development Center's CATs-I project.

automatic detection and tracking processor, and it will display geographic target tracks and vectors, as well as real-time video images.

Several of the systems mentioned above have been installed in Miami or San Francisco. Technical evaluation of these systems is ongoing. Operational evaluations were conducted in both partner ports during the first half of FY03. Operational experience to date has result-

ed in several recommendations for improvements, and these will be addressed over the next several months. Based on the accomplishments to date, the Coast Guard has recently committed to operational deployment of several of these enhanced systems for port security in the south Florida area.

RADNET

This system uses COTS radar to provide radar surveillance capability to Coast Guard Groups and COTPs. RADNET uses a networkable radar and wireless technology to provide radar surveillance coverage of a port/coastal area. Display and control of the radar is provided to the Coast Guard command center via the Internet or through wireless modems. The system can support up to four remote locations. If necessary, the radar unit is rapidly deployable to other locations and available commercially at relatively low cost. Working in concert with the Day/Night Surveillance system, it may provide increased range of target detection, and the ability to provide target range and location. Operators in the command center may select targets of interest, and pass appropriate intercept information to vessels on patrol, significantly increasing the effectiveness of their time on the water.

Port Security System (PSS)

The PSS is designed to provide an integrated command and control system for port security sensors at Coast Guard groups, stations, and Marine Safety Offices. It can integrate the control and output of multiple sensors into one console. Such resources as the day/night surveillance cameras, RADNET radar, and trip wires could be managed via the PSS. The system is designed for collateral or unattended operation by relying on an

In addition, the Unified Command for CATs-I has approved several more technologies for investigation, and these will be pursued during the remainder of this fiscal year. In particular, the R&D Center will work with the COTPs and groups to:

In a related effort the R&D Center will also investigate technologies for improved underwater port security, including anti-swimmer systems, and sensors and platforms for inspecting ship hulls and pier structures.

- Improve the integration of sensors with command and control systems,
- Investigate systems for detecting chemical, biological, radiological and nuclear threats,
- Develop improved port security planning tools,
- Evaluate systems for inspecting and detecting underwater threats,
- Evaluate ways to improve the identification of friendly forces, and
- Assess means to improve the data communications with vessels underway.

The U.S. Coast Guard Research & Development Center is working with the Coast Guard, with particular focus on the COTPs and groups to live in this new world, to help all to achieve their missions, and to learn to manage in a new world where the cheese is constantly moving.



Improving Our Future Capabilities with the Integrated Deepwater System

by Lt. Cmdr. ANDREA PALERMO

Communications Director; U.S. Coast Guard Integrated Deepwater System

The U.S. coastline presents an array of attractive targets to terrorists who may exploit our relatively open borders and waterways to infiltrate weapons and operatives into the United States. These targets are a complex, interdependent system of critical infrastructure located within the marine transportation system. This system encompasses a network of navigable waters, publicly and privately owned vessels, port terminals, intermodal connections, shipyards, vessel repair facilities, and a trained labor pool operating and maintaining this infrastructure. Attacks on these targets could damage critical military facilities, shut down vital economic hubs and cause economic and environmental disasters.

As a result of the September 11 attacks, the U.S. Coast Guard was designated the lead agency for maritime homeland security (MHLS). The MHLS mission requires the United States to strike a vital balance between facilitating the free flow of goods and services and protecting national security. This presents a formidable task. Thousands of watercraft in an enormous area make it extraordinarily difficult to sort out illicit traffic—the United States has more than 95,000 miles of coast and an Exclusive Economic Zone covering more than 3.5 million square miles. The Coast Guard must also operate in a wide variety of environments, from Arctic waters to the Caribbean and Pacific. The amount of traffic involved is also daunting. More

than 7,500 foreign-flag ships visit the United States every year, many with multinational crews and cargo. Some experts believe that maritime trade could triple by 2020.

The potential for terrorist attacks in this maritime domain and the responsibility of protecting American lives, property, and interests in the nation's inland waterways, in nearby coastal waters, and on the high seas are two reasons why the Coast Guard's current Deepwater assets must be upgraded and progressively recapitalized. Current Deepwater assets are reaching the end of their useful service lives. They are technologically and operationally obsolete. There is a compelling need to modernize and enhance the operational capabilities of these assets to ensure that national maritime security and safety requirements can be met as well as supporting our additional mission areas.

To address these shortfalls, the Coast Guard established the Integrated Deepwater System (IDS) Program. IDS is an acquisition project to renovate, modernize and/or replace the Coast Guard's Deepwater assets with an integrated system of surface and air platforms, along with command, control, communications, computers, intelligence, surveillance, reconnaissance (C4ISR) and logistics systems. Rather than focusing on a specific class of cutter or aircraft, the Coast Guard has focused on the capability to perform all of its 14 federally mandated missions in the Deepwater region,

including countering terrorist threats, rescuing mariners in distress, catching drug smugglers, stopping illegal migrants, and protecting the marine environment. The new IDS assets will possess common systems and technologies, common operational concepts, and a common logistics base. When fully implemented, the Deepwater system will give the Coast Guard a significantly improved ability to perform each of its missions, along the U.S. coast or in its harbors and ports or far from U.S. borders. This will include the ability to detect and identify all activities in the maritime arena—known as maritime domain awareness (MDA)—as well as the improved ability to intercept and engage those activities that pose a direct threat to U.S. sovereignty and security.

The Coast Guard's ability to respond so rapidly to the attacks on the World Trade Center and the Pentagon validated its reputation as an effective, multi-mission force. Coast Guard forces previously assigned to law-enforcement operations—including 55 cutters, 42 aircraft, and thousands of Coast Guard men and women—were immediately reassigned to homeland security tasks. Cutters patrolled offshore and in U.S. harbors to maintain a deterrent presence and escort cruise ships, tankers, and other high-value units into and out of American ports. Coast Guard Port Security Units, normally staged overseas, were deployed in several U.S. ports. Coast Guard personnel also were employed as Sky Marshals on commercial airliners

and as Sea Marshals onboard commercial shipping. As always, the Coast Guard responded with speed and agility to the threat at hand.

The Coast Guard has always played a critical role in securing the American homeland. The Deepwater Program provides an unprecedented opportunity to strengthen our fleet, providing the men and women of the Coast Guard the capabilities needed to perform these missions as well as future missions well into the 21st century. On June 25, 2002, the Coast Guard awarded the Deepwater contract to Integrated Coast Guard Systems (ICGS), a joint venture between Lockheed Martin and Northrop Grumman. This long-term relationship between the Coast Guard and the system integrator (SI), ICGS, promises to deliver to the men and women of the Coast Guard an integrated system of ships, aircraft, unmanned aerial vehicles, improved C4ISR and supporting logistics infrastructure.

While many people believe that homeland security missions only take place close to shore (such as port security missions), the truth is that a successful MHLS strategy must push out U.S. borders to sea if threats are to be detected and eliminated well before they reach the shore. Interdicting threats to homeland security as far from shore as possible has become more vital as potential adversaries have lengthened their reach. Any other strategy takes unnecessary risks with our national security. IDS assets will be designed with the speed and weapon-



ry needed to interdict and eliminate identified threats.

Deepwater assets require the flexibility to confront a wide range of challenges. The multi-mission design of Deepwater assets will enable the Coast Guard to respond to an array of threats, protecting critical infrastructure in U.S. ports and harbors as well as far out to sea. Deepwater assets will be designed to maintain an extended on-scene presence and provide an optimal command and control capability. Finally, the IDS solution provides an affordable means for our allies to participate in a common effort to improve interoperability in our respective naval forces. Each of these capabilities contributes to the Coast Guard's homeland security strategy and is an essential element of American safety and security on our maritime front lines.

The Coast Guard's MHLS strategy complements the president's national strategy for homeland security. In this national strategy, there are three broad objectives to be accomplished:

1. Prevent terrorist attacks within the United States;
2. Reduce America's vulnerability to terrorism; and
3. Minimize the damage and recover from attacks that do occur.

The national homeland security strategy is a sound strategy that depends primarily on sharing infor-

mation, securing U.S. borders, protecting vital infrastructure, partnering with others at home and abroad, and preparing to respond quickly to future events. The modernization of the Coast Guard's cutters and aircraft, complemented with modern C4ISR capability through the IDS Program, is essential to the Coast Guard's ability to execute this strategy effectively.

Deepwater assets will contribute important capabilities to each of the Coast Guard's six elements of homeland security strategy, as well as meeting the president's strategy for homeland security:

1. Increase MDA—build and leverage MDA to create a comprehensive knowledge base for maritime security operations;
2. Conduct enhanced maritime security operations—establish and maintain a new threshold level of maritime security readiness, including layered maritime security operations for selective area control and denial, heightened levels of emergency preparedness, and a targeted response to the threat of terrorism;
3. Close port security gaps—strengthen the port security posture and reduce the vulnerability of strategic economic and military ports;
4. Build critical security capabilities—develop required capabilities, improve core competencies, and recapitalize the Coast Guard

INTEROPERABILITY SCENARIO

1 HAE-UAV WIDE-AREA SURVEILLANCE

Florida coast is surveyed for drug activity; HAE-UAV then flies to northeast to patrol fisheries and continues north to locate iceberg position; real-time data sent ashore and integrated into common operating picture.

2 MPA PROSECUTION

MPA flies from Cape Cod; detects, classifies and identifies fishery violator; prosecution completed by imaging the boat in closed area.

3 NSC INTEROPERABILITY WITH DOD

NSC deployed with DOD and participates in NATO exercise in North Sea.

4 MULTI-ASSET OPERATIONS

FRC receives TOI data from an OPC (including VUAV data) and a VRS; supports rescue mission.

5 OVER-THE-HORIZON OPERATIONS

OTH prosecution conducted by LRI; data from VUAV and HAE-UAV allows OPC to perform simultaneous prosecutions.

6 SHORE-BASED COMMAND CENTER

HAE-UAV relays surveillance information via SATCOM to shore command center; center relays information and Drug Enforcement Administration intelligence reports into the command operating picture and cues OPC and FRC via SATCOM.

HAE-UAV = High Altitude Endurance Unmanned Aerial Vehicle

MPA = Maritime Patrol Aircraft

NSC = National Security Cutter

FRC = Fast Response Cutter

TOI = Target of Interest

VUAV = VETOL (Vertical Take-off and Landing) Unmanned Aerial Vehicle

OTH = Over The Horizon

VRS = VETOL Recovery and Surveillance Aircraft

OPC = Offshore Patrol Cutter

LRI = Long Range Interceptor





Dr. Vance D. Coffman, CEO of Lockheed Martin (front); Rear Adm. Thomas H. Collins, Commandant of the Coast Guard (center); and Dr. Ronald D. Sugar, President of Northrop Grumman, sign contracts which award Lockheed Martin and Northrop Grumman with the Coast Guard's Deepwater contract. Photo by Telfair H. Brown, USCG.

5. Leverage partnerships to mitigate security risks—organize and sustain a public-private sector partnership, while increasing international cooperation; and
6. Ensure readiness for homeland defense operations—prepare, equip, and train forces to conduct both homeland security and homeland defense operations and to transition smoothly between them.

Achieving MDA—the comprehensive information, intelligence, and knowledge of all relevant entities within the U.S. maritime domain and their respective activities that could affect America's security, safety, economy, or environment—allows the Coast Guard to anticipate and respond to potential threats in a timely fashion, as well as optimize the deployment of valuable assets. Deepwater will improve the Coast Guard's existing C4ISR capabilities, enabling a common operational picture (targets of interest, ships, geospatial data, cargoes, port facilities, trade routes, personnel manifests, etc.), thereby improving risk assessments of terrorist and criminal activity in the maritime domain. In addition, Deepwater's improved C4ISR system will be interoperable with the Navy and other federal agency systems to provide MDA and improve domestic interagency communication and coordination.

An explanation of the Deepwater task sequence—surveil, detect, classify, identify, and prosecute (SDCIP)—is important to understanding how Deepwater's design contributes to MHLS. The Coast Guard's missions performed in the

Deepwater environment follow the SDCIP task sequence. This mission execution sequence was derived from a review of operational tactics past and present, across all missions and across all maritime services. The process starts with surveilling vast areas of the seas. Surveillance detects objects. These objects are then classified as either a target of interest (TOI) or as friendly. The object is then identified, for example, as a vessel, debris, etc. Those objects classified as TOIs mandate some form of prosecution. Prosecution can entail saving someone in the water, sending an armed boarding party onto the TOI for law-enforcement action, or delivering ordnance on target. A combination of air and surface assets can be employed to conduct these missions. The SI's system concepts, developed in accordance with IDS minimum performance requirements, are designed to provide the Coast Guard with a system of assets to execute this task sequence better.

Consequence management is another important aspect of MHLS. It is quite possible that another attack will occur despite our best efforts at prevention. The Deepwater Program's investments in command and control infrastructure, as well as cutter and aircraft capabilities, will enable faster, better-coordinated responses to terrorist incidents. These capabilities will be essential for the Service to build on its impressive track record of consequence management.

Cooperation between the Navy and Coast Guard is another essential component of safeguarding MHLS. Deepwater will enhance this cooperation, enabling the Coast Guard to meet its obligations under the National Fleet agreement, which addresses the operational integration of our units, as well as synchronized planning, training, and procurement between the two services. Homeland security and defense are key elements of the national fleet policy, and the Navy and Coast Guard are working to ensure that scarce resources—our people, our ships, and aircraft, and the taxpayers' dollars—are allocated to meet the most critical needs confronting the nation. Last April, the Deepwater Program Executive Officer signed a Memorandum of Understanding (MOU) with Rear Adm. Charles Hamilton, the Navy's Deputy Program Executive Officer for Ships. This MOU will ensure the Deepwater Program is totally interoperable and compatible with Navy platforms. It provides the mechanism for the Coast Guard and the Navy to explore areas of technical commonality such as C4ISR systems, combat

systems, modularity, human systems integration and automation, air and surface interfaces, and total ship computer environments. Modernizing the Coast Guard fleet will enhance joint missions, including enforcement of economic sanctions and force protection.

The ICGS' proposed implementation plan is based on the Coast Guard's 1998 mission profile and notional funding levels. The actual implementation schedule, asset types, and numbers of assets may vary, based on updated mission requirements and actual funding provided. However, ICGS proposed three new classes of cutters and their associated small boats, a new fixed-wing manned aircraft fleet, a combination of new and upgraded helicopters, and both cutter-based and land-based unmanned air vehicles (UAVs). All of these highly capable assets are linked with state-of-the-art C4ISR systems and supported by an integrated logistics system.

President Bush has acknowledged the critical importance of modernizing the Coast Guard. In February he stated, ". . . I hold in high esteem the United States Coast Guard. We've got a plan to beef up the Coast Guard, to modernize her ships, to make sure the Coast Guard is available around all the coasts of the country to protect the homeland." The president was referring to the Deepwater Program. To demonstrate his support of the Coast Guard and the Deepwater Program, the budget for fiscal year (FY)03 requested the largest increase in the history of the Coast Guard. This trend continued with the President's proposed budget for FY 2004. In the President's national strategy for homeland security, it is noted that the President is committed to building a strong and effective Coast Guard. His proposal calls for providing the necessary resources to acquire the sensors, command-and-control systems, shore-side facilities, boats and cutters, aircraft, and people the Coast Guard requires to perform all of its missions.

The Coast Guard has demonstrated time and time again its devotion to duty and its devotion to the safety and security of the American people. The Integrated Deepwater System, supported by our partners in industry, promises to bring to the men and the women of the Coast Guard the necessary tools to maintain operational excellence at an affordable cost well into the 21st century.

INTEGRATED DEEPWATER SYSTEM: A SYSTEM OF SYSTEMS



Bell Eagle Eye Vertical Unmanned Aerial Vehicle



Global Hawk High Altitude Endurance Unmanned Aerial Vehicle



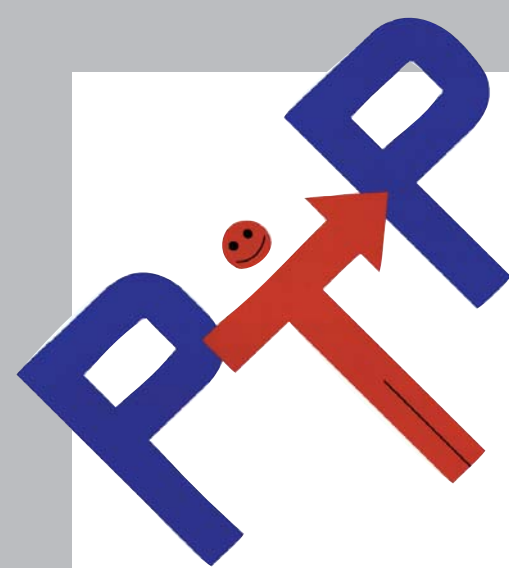
Long-Range Interceptor



AB-139 VRA, Recovery and Surveillance Aircraft



National Security Cutter



Beyond Traditional Application

by NAOMI CHANG¹

Whether preventing safety or security mishaps, one concept remains true: one of the best preventive elements is the *human* element. Prevention Through People (PTP) is traditionally thought of as a strategic approach to increase safety and environmental protection. Preventing accidents and spills through risk analysis, mariner education and best practice review is not a new concept. What is new, however, is our expanded focus on issues related to homeland security and tools used to wage war against terror. The following will highlight how the PTP mindset, which was traditionally used to prevent safety and environmental mishaps, is also an avenue in preventing maritime terror attacks via strategies and specific practices.

What makes an approach a “Prevention Through People” strategy?

The PTP philosophy states that a focus on people is the most effective and efficient way to solve most problems related to safety and environmental protection. Effectiveness is based on studies that cite human factors as the root cause of more than 80 percent of marine casualties and accidents. In the case of terrorism, it is the people on vessels and in ports that prevent acts of terror. While the “nuts and bolts” of technology play a role in prevention, it is the people behind the technology using their awareness, inquisitiveness, training and communications that constitute a “PTP” strategy.

Evolving from the PTP philosophy, concrete practices were developed to further safety and environmental protection initiatives. Those, too, can apply to security issues. Commonalities between preventing safety and security mishaps using person-centered practice include the following:

- Solutions are non-regulatory in nature;
- Prevention, rather than reaction, is the mindset;
- All port and vessel stakeholders are part of the solution;

- Education and training are paramount;
- Sharing best practices is key; and
- Stakeholder motivations are high

Prevention Through People in Practice

Although U.S. Coast Guard units and maritime industries may not be using the term “PTP” to characterize their security initiatives, human factor elements run deep within their plans of action. Currently, Coast Guard ports across the country are looking at human factors in their homeland security initiatives. Although not exhaustive, the following is a list of Coast Guard security programs that may be considered “PTP” in nature:

- Coast Guard Group and Marine Safety Office (MSO) Boston initiated Coast Watch Boston. They are available 24 hours a day to take reports of any unusual maritime-related activities, such as unusual business in the port or unusual activities by vessels in the harbor. Most of these examples of “unusual” activity relate to the human element.
- The Homeland Security Harbor Watch Program, administered through the U.S. Coast Guard’s 9th District, and the Bay and Delta Guardian Watch Program, administered through the 11th District, are like neighborhood watch programs for the water. These programs are meant to inform, educate, and enlist the assistance of all persons who witness suspicious activities.
- Capt. Ronald W. Branch, Captain of the Port, MSO for New Orleans, developed a person-centered practice to prevent security mishaps. He wrote in the June 2002 Marine Safety Bulletin (Volume II, Issue IV), “All masters, mates, pilots, deckhands and agents can serve as our ‘eyes and ears’ in the field as they go about the normal business of the port.” His request for assistance was directed to everyone in the maritime industry community in combating terror.

¹Naomi Chang is a Potomac Management Group, Inc. technical writer for the U.S. Coast Guard’s Human Element and Ship Design Division (G-MSE-1) in Washington, DC.

In addition to the Coast Guard, merchant mariners also use approaches to security that are person-centered in nature.

- The April 2002 American Bureau of Shipping publication *Activities* discussed the application of risk management techniques to maritime security. Risk-Based Decision Making is a classic PTP initiative.
- The Maritime Institute for Technology and Graduate Studies (MITAGS) offers a security awareness workshop. This course discusses understanding and coping with potential terrorist attacks.
- American Waterways Operators (AWO) has developed guidelines for ensuring security on boats for crews and for the surrounding areas.

Specific Practices for Prevention

Coast Guard and merchant mariner guidelines alike provide specific examples of prevention tactics, such as gathering intelligence and conducting drills to test a crew's readiness in response to security threats. Other person-centered tactics include using positive identification badges for personnel, vendors, and visitors. Guidelines such as these suggest awareness of suspicious situations that may include vehicles or small boats loitering in restricted areas, or unknown persons trying to gain specific information about a vessel's security, personnel, or standard operating procedures by questioning personnel or their families.

The important role mariners perform in the war against terrorism include being more mindful of surrounding events and unfamiliar persons, and then informing crewmembers and other area ships of the suspicious activity. Such basic tenets of the human element—including awareness, inquisitiveness, training and communication—enhance port security.

Awareness of Suspicious Behavior

With both the Coast Guard and maritime industry telling mariners to look out for "suspicious" behaviors, an important question is raised: "What makes an activity or a person suspect enough to cause alarm?" What one person believes to be "suspicious" may not be suspicious to another. Or the observer may feel that there is insufficient cause for urgency and, therefore, take no action. For example, a stranger photographing a vessel may be part of a tour group with an interest in ships, but that same person photographing specifically located vessel facilities, such as the placement of loading arms and cargo cranes on the dock or looking for areas that could be potential bomb spots, could be cause for alarm.

Any occurrence that seems unusual should be questioned.

Inquisitiveness

An inquisitive attitude can be one of the best deterrents to terrorist attacks. If an unfamiliar person's activity looks out of the ordinary, don't be shy—ask. Approach the individual and ask detailed questions in a civil manner. Routine questions, such as requesting a work order number or asking for the name of the job supervisor, should be provided in a direct manner. If the person has nothing to hide, he or she will probably give a detailed response in an equally civil manner. Vague, inaccurate, or confusing answers are red flags that should be reported. But even double-checking with a supervisor about the questioned activity is a good follow-up to the situation and should not be discouraged.

Training

The addition of security awareness training for mariners is a crucial part of a prevention plan. Conducting drills to test crew readiness and educating staff about security policies are necessary parts of security training, and both fall under the umbrella of PTP. Preparation for what may come is more desirable than having to realize the weaknesses after an attack.

Communication

Increasing communication is another non-regulatory practice. Communication with ships in the vicinity keeps everyone apprised of current situations. Reports of suspicious activities or vessels can easily be transmitted via radio to other ships as well as to local law enforcement departments, thereby ensuring that everyone is alerted to a situation. Just as truckers use citizen band (CB) radios to report erratic and dangerous drivers to other truckers and law enforcement officers, so, too, can mariners report suspicious behavior to each other.

On a recent visit to Anchorage, Alaska, Coast Guard Commandant Thomas Collins stated, "Safety and security are not oil and water." Preventing safety and security mishaps is something that we can all do throughout our daily business. By using non-regulatory strategies, having a prevention mindset, involving all stakeholders, offering appropriate training and sharing best practices, both safety and security are within reach. Prevention can be achieved by using one of the best preventive elements: the *human* element.

The Coast Guard National Response Center (NRC), at (800) 424-8802, can be reached 24 hours a day. It is a national clearinghouse for information for all suspected or actual terrorists attacks in the U.S. domestic marine industry.

What Can PREP Do for You?

by Lt. Cmdr. MICHAEL HEISLER
NSFCC Preparedness Department

The National Strike Force Coordination Center (NSFCC) Preparedness Department has been improving the preparedness of response communities for more than a decade by developing, executing, and evaluating national Preparedness for Response Exercise Program (PREP) government-led area exercises. Through the years we have continuously revised and improved our exercise processes to meet or exceed the needs of our customers—the “response community.”

History

The Preparedness Department was established in 1991 as part of the NSFCC to lead the design and evaluation of government-led PREP area exercises. Our department is billeted for 18 members with a blend of six civilians and 12 U.S. Coast Guard active duty personnel. We recently welcomed the addition of two new valuable resources when we received two new planner billets, a mass rescue operation planner and a port security planner. The department is tasked with developing six government-led PREP area exercises annually and one Spill of National Significance (SONS) exercise biennially.

PREP was developed after the *Exxon Valdez* and other major oil pollution incidents to establish a workable exercise program, which meets the intent of section 4202(a) of the Oil Pollution Act of 1990 (OPA 90). PREP supports preparedness within the National Response System (NRS) through the routine exercise of Area Contingency Plans and required industry facility and vessel response plans. The NRS is the mechanism for coordinating response actions by all levels of government in response to an oil spill or hazardous materials release. At the national level, the National Oil and Hazardous Substance Contingency Plan (NCP) provides response

guidance for the NRS and is supplemented by the Regional Contingency Plans at the regional level and the Area Contingency Plans (and industry facility and vessel response plans) at the local level. The focus of the NCP is to achieve the best response through an efficient, coordinated and effective response by the entire response community—federal, state, local government and the industry responsible party.

The goal of PREP is to conduct 20 area exercises per year nationwide, with six of the 20 annual exercises being government-led and the remainder being industry-led. The primary difference in the two types of exercises is in who is responsible for leading the design effort. For government-led exercises, either the Coast Guard or the Environmental Protection Agency (EPA) lead the design effort, and for industry-led exercises, the industry participant in the area exercise leads the design effort. Commandant (G-MOR) tasked the Preparedness Department with being the lead design agent for all Coast Guard government-led PREP area exercises. We also provide support to EPA federal on-scene coordinators tasked with government-led area exercises when requested.

PREP exercises differ from other types of exercises in that per the PREP guidelines, the focus of the exercises is “on the interaction between the responsible party and the federal, state, and local government” in the exercise of both the Area Contingency Plan and the industry response plan. Therefore, the focus of PREP exercises is aligned with the focus of the NCP. The guidelines also require the formation of an exercise design team with representatives from industry, federal, state, and local and state governments.

In the late 1990s, we were asked to adapt our processes to support the exercise of non-oil spill contingency plans which also require a coordinated federal, state, and local government (and often industry, as well) response effort. Our first such effort was the 1996 Key West Cruise Ship (now called Mass Rescue Operations or MRO) Exercise. Every year since then, we have done at least one non-oil spill response exercise (MRO, HAZMAT or Mass Care Exercise). Participation in these other types of exercises required us to develop expertise in the emergency management processes and procedures used by state and local governments in responding to major incidents and in the use of the National Interagency Incident Management System (NIIMS) based Incident Command System (ICS) to support responses to “all hazards and all risks.”



Participants attend a planning meeting during a PREP exercise in Juneau, Alaska.

Present

Since September 11, we have used our expertise gained in designing “all hazards and all risks” exercises to assist response organizations within a geographic area to become better prepared for what the future may bring. We are much more flexible in our exercise scheduling and design process and work closely with the response community to develop the type of exercise that meets both their Homeland Security and NRS preparedness needs and objectives. Our new and improved exercise scheduling system allows FOSCs to schedule PREP exercises when it best meets their needs within a designated calendar year.

Today, we readily accept the challenge of designing exercises that address “all hazards and all risks,” including Homeland Security-type scenarios. Most recently, we conducted a highly successful PREP exercise in northwest Florida—Comprehensive HAZMAT Emergency Response Capability Assessment/PREP (CHER-CAP/PREP)—which had a scenario consisting of an oil spill and HAZMAT release resulting from an act of terrorism. The After Action Report and Lessons Learned from this exercise, and all PREP exercises, are captured in the Coast Guard Standard After Action Information & Lessons Learned System (CG SAILS).

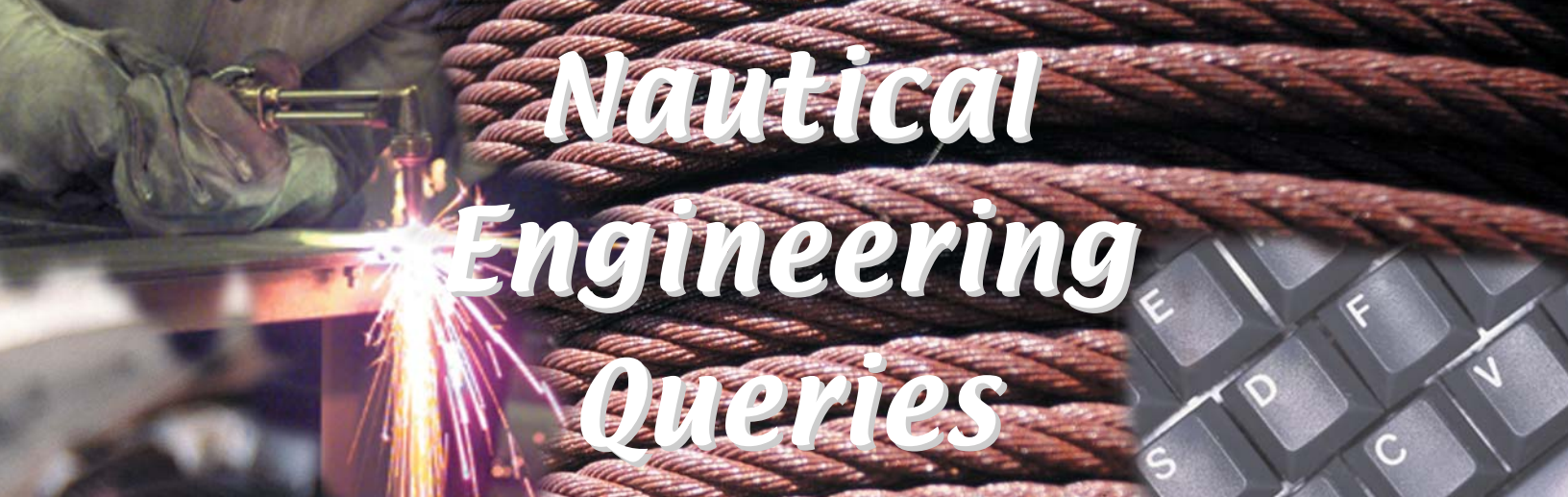
With our current staffing and approval of our program manager (G-MOR), we are capable of supporting up to eight exercises annually—six PREP and two additional

exercises. However, funding for non-PREP exercises must continue to come from the unit requesting the exercise. We also offer the following services: facilitate Incident Reviews in lieu of conducting an exercise, provide incident response management command post support for actual responses, and assist in a full range of contingency plan assessments.

Future

Our role in providing preparedness support will evolve as the government and industry continue to meet the challenge of protecting the environment, public health and welfare. Recent significant events, such as the Coast Guard transferring to the Department of Homeland Security and the release of Homeland Security Presidential Directive (HSPD-5) are bound to have an impact on the way we do business. For example, HSPD-5 calls for the creation of a new National Incident Management System and a National Response Plan, which will obviously have some effect on the current response management system (NIIMS ICS) and the NCP. Whatever changes come our way we will remain steadfast in our belief: “Preparedness Perfects Response.”

More information about PREP can be found on the NSFCC Web site: www.uscg.mil/hq/nsfweb/index.html.



Nautical Engineering Queries

1. The mechanical efficiency of a particular centrifugal bilge pump is 92.5 percent. What is the smallest motor listed that can effectively operate this pump at a capacity of 100 gpm and a discharge head of 15 feet?
 - A. 1/4 horsepower motor
 - B. 1/2 horsepower motor
 - C. 3/4 horsepower motor
 - D. 1 horsepower motor
2. It is desired to operate an air compressor with a 12-inch flywheel at a speed of 510 RPM. If the motor runs at 1,750 RPM, what size motor pulley should be used?
 - A. 2.5 inches
 - B. 3.5 inches
 - C. 4.5 inches
 - D. 5.5 inches
3. If your vessel burns 2.9 tons of fuel per hour operating at a speed of 20 knots, how many tons per hour will it burn at a speed of 15 knots?
 - A. 1.2 tons
 - B. 1.6 tons
 - C. 2 tons
 - D. 2.4 tons
4. A boiler forced draft pressure gauge indicates nine inches of water. This corresponds to a pressure of _____.
 - A. 0.216 psi
 - B. 0.228 psi
 - C. 0.325 psi
 - D. 0.433 psi
5. A machine capable of producing 1,650 foot-pounds of work per second is considered to produce how much horsepower?
 - A. 1 horsepower
 - B. 2 horsepower
 - C. 3 horsepower
 - D. 4 horsepower
6. The capacity of a particular ballast pump is 200 gallons per minute. Approximately how long will it take to ballast a tank with 68.5 long tons of seawater?
 - A. 1.5 hours
 - B. 2 hours
 - C. 2.5 hours
 - D. 3 hours
7. An oil fog lubrication system is recommended for _____.
 - A. gear shaft bearings
 - B. high-speed continuous operation of roller bearings
 - C. low and moderate speed ball bearings
 - D. heavily loaded and high-speed ball bearings
8. The heat required to change a substance from a solid to a liquid while at its freezing temperature, is known as the latent heat of _____.
 - A. fusion
 - B. vaporization
 - C. condensation
 - D. sublimation
9. A distinguishing feature of an eductor, when compared to other pumps, is the _____.
 - A. discharge end being smaller than the suction end
 - B. small size of impeller
 - C. lack of moving parts
 - D. ease at which the wearing rings may be changed
10. The average salinity of normal seawater, when expressed as brine density, is equivalent to _____.
 - A. 1/32nds
 - B. 1.5/32nds
 - C. 2/32nds
 - D. 3/32nds

Answers: 1-B, 2-B, 3-A, 4-C, 5-C, 6-A, 7-B, 8-A, 9-C, 10-A

Nautical Deck Queries

1. You are signing on a crew. A prospective crewman presents a Merchant Mariner's Document that you suspect has been tampered with when he reports to sign the Shipping Articles. Which action should you take?
 - A. Confiscate the document and deliver it to the Coast Guard.
 - B. Sign the man on and notify the Coast Guard at the first U.S. port of call.
 - C. Refuse to sign the man on articles until authorized by the Coast Guard.
 - D. Refuse to sign the man on and notify the FBI of unauthorized use of a federal document.
2. Uncleared crew curios remaining onboard during a domestic coastwise voyage after returning from foreign should be _____.
 - A. listed in the Official Logbook
 - B. cleared prior to the next foreign voyage
 - C. noted in the Traveling Curio Manifest
 - D. retained under locked security by the owner
3. An alien crewmember with a D-1 permit leaves the vessel in a U.S. port and fails to return. The first report you make should be to the _____.
 - A. Customs Service
 - B. Immigration Service
 - C. local police
 - D. OCMI
4. A document which has a list of names, birthplaces and residences of persons employed on a merchant vessel bound from a U.S. port on a foreign voyage and is required at every port is called the _____.
 - A. Certified Crew List
 - B. Crew Manifest
 - C. Shipping Articles
 - D. Station Bill
5. You are coming to anchor in eight fathoms of water. In this case, the _____.
 - A. anchor may be dropped from the hawsepipe
 - B. anchor should be lowered to within two fathoms of the bottom before being dropped
 - C. anchor should be lowered to the bottom, then the ship backed, and the remainder of the cable veered
 - D. scope should be less than three times the depth of the water
6. How should the lifeboat sea painter be rigged?
 - A. Spliced into the ring on the stem post
 - B. Secured by a toggle around the outboard side of a forward thwart
 - C. Secured to the inboard side of a forward thwart and led inboard of the falls
 - D. Secured by a toggle to the stem post and led outboard of the falls
7. While on watch, you notice that the air temperature is dropping and is approaching the dew point. Which type of weather should be forecasted?
 - A. Hail
 - B. Heavy rain
 - C. Sleet
 - D. Fog
8. The major factor that causes the color difference between a red star (Betelgeuse) and a blue star (Rigel) is _____.
 - A. its surface temperature
 - B. the elevation above the horizon
 - C. the mass of the star
 - D. the contrast to nearby stars
9. BOTH INTERNATIONAL & INLAND: You see a red sidelight bearing NW (315°). That vessel may be heading _____.
 - A. NW (315°)
 - B. East (090°)
 - C. SW (225°)
 - D. West (270°)
10. BOTH INTERNATIONAL & INLAND: In fog, you hear apparently forward of your beam a fog signal of two prolonged blasts in succession every two minutes. This signal indicates a _____.
 - A. power-driven vessel making way through the water
 - B. vessel being pushed ahead
 - C. vessel restricted in her ability to maneuver
 - D. power-driven vessel underway, but stopped and making no way through the water

Answers: 1-C, 2-C, 3-B, 4-A, 5-A, 6-C, 7-D, 8-A, 9-C, 10-D

U.S. Department of Homeland Security

United States Coast Guard

National Maritime Center
4200 Wilson Blvd., Suite 630
Arlington, VA 22203-1804

Official Business
Penalty for Private Use \$300



U.S. Coast Guard Commandant Adm. Thomas H. Collins shakes hands with Norman Y. Mineta, Secretary of Transportation, during the Change of Watch Ceremony Feb. 25, 2003. The ceremony commemorates the transfer of the U.S. Coast Guard from the Department of Transportation to the Department of Homeland Security. Photo by Public Affairs Officer Harry C. Craft III, USCG.