domestic preparedness .com
T.I.P.S. Total Integrated Preparedness Solutions
$50 Per Year
Volume 1, Issue 17, August 24, 2005

This Issue:

Maritime FSOs: The New Breed of Homeland-Security Professionals

By Laurie Thomas
Maritime Security

Not quite two years ago – on 1 October 2003, to be specific – the U.S. government officially opened a new career field for a large number of people in the fast-growing ranks of homeland-security professionals. On that date, the final rules relating to the nation's maritime security were published, and many men and women who previously held such job titles as terminal manager, human-resource specialist, or owner/operator took on new responsibilities – namely, the duties they would have as facility security officers (FSOs) at port and maritime facilities throughout the United States.

The Maritime Transportation Security Act of 2002 (MTSA) raised the bar for security measures both at facilities on land and on vessels afloat. Prior to 9/11, it was no secret that port security – or the lack thereof – was a large and growing problem in the United States. In 1999, President Clinton authorized the creation of an Interagency Commission on Crime and Security in U.S. Seaports. Among its findings was that the vulnerability of America's ports to attack by terrorists was already high, and might be even higher in the future.

Continued on the Next Page

CBRNE Attacks at Sea: Time to Revisit The Maritime SAR International Convention?

By Ashley Moore
Standards

"The issue is how seriously … governments take the threat of maritime terrorism. … We cannot continue to hope for the best and ignore the lessons." Cited in a 4 February 2003 Straits Times editorial on "Security At Sea."

Security at sea is just one of many preparedness-and-response policy issues facing the international maritime community. It is widely recognized that, in today's maritime environment, a terrorist attack at sea involving chemical, biological, radiological, nuclear, and/or high-yield-explosion (CBRNE) weapons or devices would strike a devastating blow to global economic stability. What is often ignored, though, is that for at least the past several years Al Qaeda has been increasingly active in the maritime environment and is still enhancing its capabilities.

Continued on Page 5

Editorial and Circulation Office
517 Benfield Road, Suite 303
Severna Park, MD 21146
www.domesticpreparedness.com
(410) 518-6900

Editorial Staff

James D. Hessman
Editor in Chief
JamesD@domprep.com

Channel Masters

Rob Schnepp
Fire/HAZMAT
rschnepp@domprep.com

Joseph Cahill
Emergency Medicine
jcahill@domprep.com

Colonel (Ret.) Robert Fitton
Military Support
bfitton@domprep.com

Ashley Moore
Standards
amoore@domprep.com

Jay Kehoe
Law Enforcement
jkehoe@domprep.com

John Morton
Interviews
jmorton@domprep.com

Neil Livingstone
Global Options
nlivingstone@domprep.com

Adam McLaughlin
State Homeland News
amclaughlin@domprep.com

Laurie Thomas
Maritime Security
lthomas@domprep.com

Business Office

Susan Collins
Circulation Director
subscriber@domprep.com

Sharon Stovall
Copy Manager
sstovall@domprep.com

Martin Masiuk
Advertising & Sponsorships
mmasiuk@domprep.com

Subscriptions
$50.00 annually 26 issues for single user, delivered via web or email. To order, visit www.domprep.com and click on subscribe.

Published by IMR Inc.
Martin D. Masiuk, Executive Director and Publisher,
mmasiuk@domprep.com

In a statement before the U.S. Senate Committee on Commerce, Science, and Transportation on 24 July 2001 – less than two months prior to the 9/11 terrorist attacks, it is worth noting – Acting Deputy Maritime Administrator Bruce J. Carlton said that, "While U.S. airports and land border crossings have well-structured security measures, our ports do not enjoy the same level of security even though they offer unparalleled intermodal access to our nation's interior."

That unparalleled intermodal access caused Congress to consider the passage of new port and maritime legislation, but the legislation that resulted dealt mostly with waterfront crime and cargo theft. In the aftermath of the 9/11 attacks, the previously mentioned Maritime Transportation Security Act, a law focusing primarily on maritime security, was finally passed (in November 2002). The goal of the MTSA is to prevent a maritime TSI, or transportation security incident – which is defined as an incident resulting in a significant loss of life, environmental damage, transportation system disruption, and/or economic disruption affecting a particular area.

Costly, Far-Reaching, and Absolutely Necessary

Among its many provisions, the MTSA mandates that certain vessels and port/maritime facilities that are found to be at risk for a TSI must prepare and submit security plans, and those plans must include provisions for establishing and maintaining physical security, passenger and cargo security, and personnel security. Each vessel or facility plan also must identify a specific qualified individual who would have full authority to implement security actions.

The MTSA is far-reaching and costly legislation that affects approximately 5,000 facilities across the country. The ten-year cost of the security measures mandated by the MTSA for those facilities (vessels not included, in other words) has been estimated by the Coast Guard to be approximately $5.4 billion.

A parallel movement to codify the security requirements of all of the world's major trading nations was taking place at the United Nations. In December 2002, the International Maritime Organization (IMO) adopted the International Ship and Port Facility Security Code (ISPS). This code requires, among its numerous security provisions, that port facilities considered to be at risk for terrorist attack(s) must appoint their own port-facility security officers, and also prepare appropriate security plans. For the first time in history, there would be a consistent international framework of security requirements accepted by, and required of, the world's seafaring nations.

Continued on the Next Page

In the United States, regulations were passed to implement the MTSA requirements. In July 2003, the interim rules were published – in 33 Code of Federal Regulations (CFR); these were followed in October 2003 by publication of the final rules, which postulated a 1 July 2004 deadline for implementation.

Regrettably, a large number of facilities on or adjacent to U.S. waters have been found to be at a relatively high risk of a TSI and so came under the "umbrella" of the regulations. Among them, not surprisingly, are: facilities that handle certain dangerous cargoes and/or service vessels subject to the International Convention of the Safety of Life at Sea (SOLAS), and/or foreign-flag vessels. Also on the TSI-prone list are facilities that handle passenger vessels that carry more than 150 passengers; handle cargo vessels greater than 100 gross registered tons; or handle barges that carry certain types of hazardous cargoes.

The FSO position was established by the same rules, as were the requirements for FSO responsibilities and training. Generally speaking, the owner/operator of a maritime facility has the ultimate legal and financial responsibility for security, but the FSO also is assigned extensive security responsibilities – including certain duties that challenge FSOs, especially those employed by smaller facilities, who do not possess a strong security background.

A Long and Complex List of Responsibilities

The FSO must oversee the initial facility vulnerability assessments, the facility security plan development, the approval process, implementation of the plan, and the facility's annual audit. He or she also must ensure that security drills and exercises are conducted regularly and effectively, and that security records are stored for the proper period of time and with due regard to sensitive security considerations.

In addition, he or she must:

- Ensure that the security equipment called for by the security plan is tested, calibrated, and maintained;
- Similarly, ensure that his/her security personnel are adequately trained;
- Coordinate the facility's security measures with his/her counterparts on board vessels in the port, and maintain the security of the vessel-facility interface (a point of particularly high risk for terrorist attack);

Continued on the Next Page

Interview: Justin Thomas Russell, Director for Port Security, Center for Security Strategies & Operations, Anteon Corporation

Mr. Russell emphasizes the importance of balancing port and cargo security policy-making against the business requirement for the unfettered flow of commerce. Praising full stakeholder involvement in policy development, he notes the DHS progress in supporting outcome-oriented measures for information sharing and comments on how process and commercial off-the-shelf technology solutions (COTS) are streamlining business and security decision-making – a development that in his opinion holds promise for the implementation of non-invasive profiling and "fast lane" measures.

To get the complete audio download of the interview, please visit
www.DomesticPreparedness.com

- Establish and implement new security measures, when port-security – also known as MARSEC (maritime security) – levels change, and must report implementation both to the facility's owner/operator and to the Coast Guard.

Most important of all: He/she must ensure that the facility is at all times operating in accordance with the measures set out – in considerable detail – in the security plan. The punishment for non-compliance with the requirements of this rule may include criminal penalties, substantial monetary penalties, and/or suspension of facility operations.

The rules allow the FSO to perform other duties within the organization as long as he or she is able to perform the duties and responsibilities of FSO. In many of the 5,000 facilities, therefore, the title "FSO" indicates a collateral duty and is but one of many hats worn on that particular head. In smaller facilities, the FSO may be the owner, sole supervisor, and one of just a handful of employees. Lt. Kimberly Wheatley of the U.S. Coast Guard's Marine Safety Detachment Grand Haven (Mich.) comments that, "These types of companies have usually between two to five people working at the facility, so with two of the workers acting as FSO and alternate, the remaining crew become the security force. The additional workload may mean higher wages, less time for day-to-day business (when the MARSEC level changes), and more training requirements."

A Handy Acronym for an Unwelcome Mindset

The FSO also is in charge of the security "climate" of the facility – i.e., the overall security awareness and vigilance of the facility's personnel. In this capacity, he or she must deal with another familiar acronym, IWNHH – "It will never happen here," a mindset unfortunately common to far too many law-enforcement and security personnel (and to the general public as well).

James Bull, chief of the Facility Branch of the Office of Vessel and Facility Security of the Coast Guard's Port Security Directorate, commented as follows on the need for a new mindset: "Just as employees learned that worker safety was a joint responsibility of the company and the workers, they now must be reminded that facility security carries the same joint responsibility and that it may well offer protection beyond the work site to their families and fellow citizens." FSOs who are concerned about an attitude of complacency, Wheatley says, should "perform unannounced drills, conduct training – beyond the required quarterly training – and promote education."

The MTSA also mandated the development of standards and curricula for the education, training, and certification of maritime security personnel. Earlier this year, the U.S. Maritime Administration (MARAD) published formal (but voluntary) approval processes for certain categories of maritime security training – a basic FSO training course is one of those categories. Det Norske Veritas NA was selected as the contractor to assist MARAD in the approval process.

Much of the routine training required for FSOs may be carried out on the job, but many companies are opting for special training for their FSOs, and their other security personnel, to make them more proficient in carrying out their MTSA responsibilities.

Above and Beyond the Core Curriculum

The rules spell out the qualifications, knowledge, and training that the FSO must possess. The list of skills and knowledge needed for this important new job is an impressive one, and includes not only general security skills but also knowledge of: relevant international and national maritime codes and laws; current U.S. government rules and regulations; security assessment methodology; instructional techniques; current security threats; the recognition and detection of dangerous substances and devices; and the conduct of physical searches and non-intrusive screening – in short, numerous subjects that were definitely not on the core curriculum of someone aspiring to be a terminal manager or a human-relations specialist.

Continued on the Next Page

To meet this daunting challenge, Bull says, FSOs "are going to be required to become more active as educators and facilitators for the training of employees and others in their role in the Facility Security Plan approved by the Coast Guard Captain of the Port for the facility. Telling a security guard at a gated entrance, for example, that he or she must screen persons and vehicles entering the facility means that the FSOs themselves are going to require a certain level of training in how to conduct an effective screening and even what a screening, versus a search, entails."

The rapidly changing climate in the maritime threat environment requires that FSOs not only become qualified in their jobs but also remain as current as possible on any new homeland-security issues that might develop. "A great place to start," Bull suggests, "is the Area Maritime Security Committee established in each Coast Guard Captain of the Port Zone." (Some committees maintain open electronic mailing lists; the URL to sign up for these lists is http://cgls.uscg.mil/mailman/listinfo.) Attendance at seminars also is strongly recommended by Bull and other officials.

Help Is on the Web

Frequent Google searches under key terms also can be invaluable. For example, a recent search found the helpful site http://www.itspnet.com/itsp.htm. FSOs bedeviled and/or bewildered by record-keeping requirements will appreciate the fact that a record-keeping software program has been designed by an FSO for the use of other FSOs. The creator of the software – called FSO-IMA (Information Management Assistant – is Nickolas LaFleur of Innovative Tools for Security Professionals, who says that the program will, among other things, store all of the records required by MTSA regulations.

It also will show at a glance, he says, the last drill date; how long it will be until the next drill date; all of the vessel information needed for any vessels with which the facility interfaces; all facility information for any other facility with which the company does business; and a broad spectrum of personnel information for unlimited numbers of facility and contract personnel. The software also provides a number of required forms that can be tailored to the needs of individual facilities.

These responsibilities and training requirements point toward a need for a continuing conversation with the rest of the homeland-security profession, as well as the necessity for consistent and continuing cross training.

The need of current and future FSOs for emergency preparedness and response knowledge and capabilities requires them also to be familiar with the National Incident Management System (NIMS) and the Incident Command System (ICS). Passenger vessel facilities or facilities in special circumstances may foresee a situation in which crowd-control skills would assist the FSO in devising and carrying out security measures appropriate for the vessel-facility interface (in this situation, the local police academy would usually be a valuable source of training material). *The Lessons Learned Information Sharing Site* of the Department of Homeland Security (DHS) – which integrates many homeland-security disciplines, information databases, and communications capabilities – also will be a valuable resource for FSOs (see www.llis.dhs.gov).

The FSOs and DHS officials have worked closely together since the beginning of this difficult regulatory journey. "When all is said and done," LaFleur says about the FSO/DHS partnership, "it's not the regulations that will make us resistant to terrorism, but the teamwork involved in multi-agency and private-sector communication and involvement in doing what needs to be done to reach the desired end."

CBRNE Attacks at Sea: Time to Revisit The Maritime SAR International Convention?

Continued from Page 1

NATO's search for the Al Qaeda fleet, which includes a number of "phantom" vessels posing as legitimate ships and roaming the ocean freely, has been a difficult one. In the more than three years since the terrorist attacks of 11 September 2001,

Continued on the Next Page

NATO officials have boarded and searched only about 200 of the approximately 16,000 commercial vessels operating in international waters. Meanwhile, the front line of the war on terrorism has become ever more violent, unpredictable, and unwavering.

Following are a few examples, of many that might be cited, that illustrate Al Qaeda's flexible arming capabilities and determination to succeed as a maritime threat:

- **Yemen-Limburg, October 2002:** Twelve crew members were injured when an explosives-laden boat rammed the Limburg as it prepared to enter the port of Ash-Shir off Yemen's southeastern coast. A Bulgarian crewmember's dead body, covered in oil, washed ashore a few days later.

- **Rota, Spain, May 2005:** The Spanish newspaper ABC reported that a French Al Qaeda cell was "preparing to unleash an unspecified chemical agent" against a U.S. naval base in Rota. One of those said to be implicated in the plan was Algerian Said Arif – who, ABC reported, also was affiliated with Jordanian Abu Musab al-Zarqawi, one of the alleged masterminds behind the continuing insurgency in Iraq.

- **Jordan, June 2005:** Jordanian state television aired a video of four men admitting they were part of an Al Qaeda plot to attack the U.S. embassy, as well as Jordanian intelligence services and other targets, in Jordan. They planned, the report continued, to use a combination of conventional and chemical weapons powerful enough to kill 80,000 people and severely injure another 160,000. One of the alleged conspirators, Azmi Al-Jayousi, said that he was acting on the orders of Abu-Musab al-Zarqawi.

The obvious progression of al-Zarqawi's asymmetric warfare and toxic industrial chemicals/materials (TIC/TIM) weapons planning and operational capabilities is both understated and disturbing. If he and/or others were ordered to initiate attacks at or from the sea, the world's maritime stakeholders might well find themselves almost totally unprepared to protect themselves. Current international strategies, policies, and capabilities for mass-rescue operations (MROs) in the post-CBRNE maritime environment do not adequately address the harsh realities responders will undoubtedly face. A review of current national and international search-and-rescue (SAR) strategies and policies suggests that many if not all maritime nations, although acknowledging the risks involved, have reluctantly accepted the harsh reality that maritime CBRNE attacks may well result in the loss of perhaps thousands of lives.

From Halifax to LNGs and the IAMSAR

As the nations involved in the global war on terrorism become increasingly aware of the maritime threat environment, their citizens are becoming correspondingly concerned about piracy, Al Qaeda rogue ships, the waterborne shipments of hazardous materials, and other terrorism-related threats. In a 1978 book – "Time Bomb: LNG, The Truth About Our Newest And Most Dangerous Energy Source," by Peter van der Linde and Naomi A. Hintze – the co-authors stated that in certain situations the consequences of a single inadvertent rupture of a liquefied natural gas (LNG) tanker would create a catastrophic explosion. In certain circumstances, in fact, an LNG blast could match the physical destructive power of a nuclear detonation (but without the thermal pulse, neutrons, x- and gamma-rays, radiation, and other by-products of nuclear explosions).

Probably the closest example of this type of catastrophe is the 6 December 1917 harbor explosion in Halifax, Nova Scotia, that devastated that Canadian port when two ships – one carrying 5,000 tons of high explosives – collided, creating the largest man-made explosion prior to the beginning of the atomic age.

Continued on the Next Page

The explosion that resulted virtually wiped out the suburb of Richmond, killing almost 2,000 people, injuring 9,000 more, and destroying 3,000 buildings. An additional 2,000 people were missing, and the short - and long-term economic damages were astronomical.

Although terrifying to contemplate, the low-probability/high-consequence effects of a CBRNE attack may not represent the most significant terrorist threats to some IMO (International Maritime Organization) states that are signatories to the International Aeronautical and Maritime Search and Rescue (IAMSAR) agreement. Judging from a review of updates and amendments to the agreement, terrorist attacks, including attacks using CBRNE weapons or devices on maritime targets, seem to have ranked low on the scale of probability. Nonetheless, even in today's post-9/11 world, the lack of maritime CBRNE preparedness poses potentially enormous consequences, both politically and economically, to the entire global economy.

A recent edition of the IAMSAR agreement, which is jointly published by the IMO and the International Civil Aviation Organization (ICAO), instructs participants on how to mount a large and rapid response – which would be critical in preventing a large-scale loss of lives at sea – in the event of a terrorist CBRNE attack against maritime targets. However, an effective response involves many factors that must be in place prior to the attack(s): advance planning, for example; viable alerting and communication systems; safety clothing and equipment – e.g., certified CBRNE personal protective equipment, detection systems, and decontamination facilities and equipment; and an effective transition plan.

Needed: Collective International Action

The timeliness of the response is particularly critical, because there almost surely will be only a small window of opportunity – known to first responders as the "Golden Hour" – to save lives after a physical trauma. Some experts believe, in fact, that a victim must receive assistance within two hours of his or her injury – but, according to some Government Accountability Office (GAO) reports, the reality is that simply responding to the scene may take as much as four hours. What this means, therefore, is that, by the time a first-responder team reaches the victims who were most critically injured in a CBRNE attack, they may well have succumbed to a combination of traumas, including miosis, salivation, lachrymation, muscular twitching and fasciculation, diarrhea, convulsions, coma, and/or respiratory failure. For practical purposes, any effective preparedness and response plan for dealing with terrorism incidents at sea – particularly incidents involving CBRNE attacks in international waters – must be based on the premise that collective international action will be required – and will be available when needed.

Fortunately, some mass-rescue operations are anticipated in a number of NATO Standardization Agreements (STANAGs), which encompass a set of processes, procedures, terms, and conditions on which the alliance's member countries have reached prior agreement. Unfortunately, however, current STANAGs do not specify the SAR capabilities and/or equipment required for either aviation or surface assets that might be called out to participate in a mass-rescue operation at sea.

Outdated Plans to Meet a Growing Threat

That is only the tip of the iceberg, though. The fact is that most if not all current maritime SAR plans and agreements: (1) are a decade or more outdated; (2) were originally developed to prevent and/or mitigate the consequences of maritime accidents or natural disasters; and (3) do not address the truly catastrophic effects of a CBRNE terrorist attack in or near a port or on the open sea.

Major Irvin Lim Fang Jau of the Singapore Armed Forces commented on this collective international problem three years ago in a prescient article he wrote for The Pointer (Journal of the Singapore Armed Forces, Vol. 28, No. 3): "The maritime terrorist threat is a hydra that continues to pose a clear, present danger to world commerce and, ultimately, the very well-being of nations.

Continued on the Next Page

"The war on global terrorism," he continued, "against newly regenerated Al-Qaeda elements and their shadowy associates is far from over, and we have not yet seen the turning of the tide."

Today, Al Qaeda insurgents are proving on an almost daily basis – both on the evening news and on the e-Qaeda online training website – that additional attacks are possible, almost anywhere in the world, at any time. As last week's missile attacks against U.S. Navy ships in Jordan demonstrated, those attacks could easily be carried out by Al Qaeda sleeper cells operating in or close to the maritime environment. For that and many other reasons it seems obvious that all international participants in current IAMSAR agreements must give much higher priority to the development, promulgation, and implementation of updated and more effective policies and plans for dealing with terrorist incidents involving CBRNE weapons or devices in the maritime environment.

The Coast Guard's Post-9/11 Deepwater Program: An Enduring Solution For U.S. Maritime Security

By Capt. Gordon Peterson, USN (Ret.)
Guest Commentary

During the past year, the Coast Guard has made significant progress in implementing a comprehensive port-security regime. Capabilities, capacity, communications, and collaboration – with a broad range of public and private stakeholders – all have improved during the execution of the Coast Guard's multi-layered defense-in-depth strategy to improve maritime security within U.S. ports and waterways.

Guided by the strategic DHS (Department of Homeland Security) goals encompassing awareness, prevention, protection, response, and recovery, the Coast Guard has both increased maritime domain awareness and created a security framework possessing both domestic and international dimensions. The new National Response Plan is being executed across all operations, and implementation of the Maritime Transportation Security Act of 2002 (MTSA) and the International Ship and Port Facility Security (ISPS) code has gone far to reduce vulnerabilities within the global maritime transportation system.

Despite this progress, however, a clear consensus exists that more must be done to reduce risk in a Marine Transportation System that Coast Guard Commandant Adm. Thomas H. Collins has described as at once the nation's "most valuable and vulnerable."

"We're not doing enough to protect our people in this second front," said Sen. Frank Lautenberg (D-N.J.) during a port security hearing this spring before the Senate Commerce, Science, and Transportation Committee. Rep. Jane Harman (D-Calif.), ranking member of the House Permanent Select Committee on Intelligence, described current port-security vulnerabilities as the nation's "Achilles heel" during a speech in Los Angeles earlier this month.

The Government Accountability Office (GAO) agrees. "More than three years after the terrorist attacks of September 11, 2001," the GAO reported in May, "concerns remain over the security of U.S. seaports and waterways. Seaports and waterways are vulnerable given their size, easy accessibility by water and land, large numbers of potential targets, and close proximity to urban areas."

The Coast Guard and other agencies in the maritime arena face numerous challenges in implementing a more effective port-security regime forged on the principle of mitigating risk through aggressive partnerships and improved capabilities. The age of the Coast Guard's active fleet (one cutter was commissioned in 1942) is clearly one impediment. "Continued risk reduction is contingent upon Coast Guard readiness and capacity," Collins testified before Congress in June. "It is no surprise, then, that readiness and capacity are the focus of my most pressing concerns in fulfilling maritime-security missions," he said.

Continued on the Next Page

Because most of the Coast Guard's current operational assets are projected to reach the end of their service lives by 2008, Collins sees the Integrated Deepwater System – a 25-year progressive modernization and recapitalization program – as the "enduring solution" to both the Coast Guard's declining legacy asset readiness and the service's, and nation's, need to improve security capabilities to reduce maritime risk in the post-9/11 world.

The Cornerstone of Future Capabilities

Testifying before the House Appropriations Subcommittee on Homeland Security in late July, Collins released new details on a single Deepwater post -9/11 implementation plan, which is now projected to require $24 billion in funding over 25 years. "It is the number one Coast Guard priority and the cornerstone of our maritime capabilities now and in the future," said Collins.

During earlier hearings, in June, congressional lawmakers asked that a single Deepwater funding stream be developed instead of a range of funding alternatives. Subsequently, with the full support of the Bush administration and DHS – the Coast Guard's parent agency – the Deepwater implementation plan was refined to provide a single long-range funding schedule for the Coast Guard's progressive sustainment, modernization, and recapitalization.

Collins told Congress that Deepwater's revised plan addresses the key issues of concern to Congress, including the sustainment of the service's air and surface legacy assets and the program's overall performance standards and measurements.

The Deepwater program's long-range plan now sets forth in specific detail the deployment schedule and delivery timeline for each air and surface asset over 25 years. Some increases in the number of aviation assets – notably, the Coast Guard's C-130 long-range maritime patrol aircraft – are projected under the refined plan to improve the Coast Guard's aerial surveillance and long-range transport capabilities.

Initially, the Integrated Deepwater System was designed to perform at the level that the Coast Guard's legacy Deepwater fleet performed at in 1998. "The tragic events of 9/11 and the stand-up of the Department of Homeland Security changed the performance requirements of the Coast Guard," Collins said. Revisions to the original baseline began almost immediately after the contract was signed (in June 2002, with Integrated Coast Guard Systems, a joint venture between Lockheed Martin and Northrop Grumman) to reflect post-9/11 requirements and ensure that the new assets being funded would have the capabilities to meet the system requirements projected.

In response to this need for change, the Coast Guard engaged in a series of internal and external third-party reviews of the Deepwater acquisition. In 2003, the Center for Naval Analyses completed a three-part study, and the Coast Guard's carried out its own Performance Gap Analysis (PGA). These and other studies influenced the final force structure selected for inclusion in the $24 billion, 25-year plan.

Under the revised plan, Deepwater cutters and aircraft will be equipped with the systems and enhanced capabilities needed to operate successfully in the post -9/11 threat environment. Deepwater's interoperable, network-centric system for C4ISR (command, control, communications, computers, intelligence, surveillance, reconnaissance), for example, will serve as a valuable force multiplier by providing a common operating picture and facilitating an increase in maritime domain awareness.

Continued on the Next Page

Similarly, improved asset capabilities for the detection of and defense against chemical-biological-radiological (CBR) threats are essential to survival and continued operations during an attack involving a weapon of mass destruction. "These and other Deepwater capability enhancements are absolutely critical to ensuring the Coast Guard's future ability to maintain the maritime security of America and to protect the nation's $450 billion marine transportation system," program officials say.

Some Security Gaps Remain

Deepwater's three classes of new cutters and associated small boats, new or converted manned and unmanned aircraft, and improved systems for command, control, surveillance, intelligence, and reconnaissance all will play an important role in enabling the Coast Guard to close the gaps that still exist in the Marine Transportation System's vulnerable ports and waterways.

Senate and House appropriators are scheduled to confer in early September, following the summer congressional recess, to reach consensus on the funding level that they will endorse for the Deepwater budget for fiscal year 2006. Senate appropriators strongly support a level approximating the administration's $966 million request – a budget described by Coast Guard officials as a critical "first installment" on the revised Deepwater implementation plan.

Deepwater's program executive officer, Rear Adm. Patrick M. Stillman, makes a strong case that implementation of the revised Deepwater Program will do much to reduce the maritime risks associated with a possible terrorist attack. "The Coast Guard has made significant progress since 9/11 to secure our homeland," he said, "but maritime safety and security gaps remain.

Admiral Collins has said many times that these gaps present risks that must be reduced. In this sense, the Deepwater Program is very much focused on *reducing risk* in the maritime domain.

Stillman also said that this year's revisions to the Deepwater program's Mission Need Statement and post -9/11 implementation plan were guided as well by the Coast Guard's strategy for improving maritime homeland security and the DHS's strategic goals and priorities. "Continued risk reduction is contingent upon improving the Coast Guard's capability, capacity, and readiness," he said. "Without these basic building blocks, successful implementation of maritime security strategies will not be sustainable."

Capt. Gordon I. Peterson, USN (Ret.), a senior technical director with the Anteon Corporation's Center for Security Strategies and Operations, is assigned to the Integrated Deepwater System's program office.

States of Preparedness

By Adam McLaughlin

State Homeland News

Maryland

Approves $5.5 Million for Port of Baltimore Security

The Maryland Board of Public Works approved a $5.5 million contract earlier this month to enhance security at the Port of Baltimore. The contract – approved unanimously by the three-member panel (which included Gov. Robert Ehrlich) – was awarded to Adesta LLC, a security and communications company based out of Omaha, Neb. Under the contract, Adesta will install surveillance and perimeter detection technology throughout the terminals of the Port of Baltimore.

A significant share of the funding will be allocated to the purchase and installation of a video-surveillance system consisting of over 85 cameras, many with thermal and low-light capabilities. Other purchases will be used to help strengthen the physical barriers at various gates throughout the Port (to prohibit entry by unauthorized vehicles), and over $400,000 is earmarked for the purchase of a variety of hand-held sensors capable of detecting explosives, chemical agents, and narcotics.

Continued on the Next Page

The Port of Baltimore is one of America's busiest container terminals, facilitating the movement of over seven million tons of general cargo annually. The port is also a significant economic engine for the region, generating approximately $1.5 billion in revenues annually, and directly employing over 16,000 Marylanders.

The contract with Adesta funds the latest in a series of upgrades the Maryland Port Administration has undertaken, in response to post-9/11 federal government mandates, to improve security at the Port of Baltimore – which according to state officials has now received more than $14 million in port-security grants since 2002.

California

Hosts Kickoff of Port Security Training Exercise Program

The Port of San Francisco, previously selected by the U.S. Department of Homeland Security (DHS) to initiate the department's Port Security Training Exercise Program (PortSTEP), finished the exercise in impressive style last week, validating the Port's selection to serve as test vehicle for a three-year series of exercises directed by the U.S. Coast Guard and the Transportation Security Administration (TSA).

The primary focus of the PortSTEP program is the building of links within the area maritime security (AMS) committees of various ports. The AMS committee assists the captain of the port in writing, reviewing, and updating an AMS plan, and supports other transportation entities that depend upon the port being secure. "PortSTEP is designed to benefit maritime and transportation security communities throughout the United States via a suite of exercises and evaluations," said Noreen Brown, TSA's PortSTEP project officer.

A typical PortSTEP exercise will involve the entire port community – including various private-sector entities as well as state, federal, and local agencies with port-and/or maritime-security responsibilities. The scenarios projected for the program range from how officials react to discovering a suspect cargo container to the handling of an explosion at a rail yard in the seaport. The communications and coordination capabilities – both of the government and of U.S. maritime industries – will be tested at each of the 40 seaports throughout the nation that are scheduled to participate in the PortSTEP program over the next three years.

North Carolina

Prepares for Rescue Drill in Offshore Waters

Emergency-readiness officials from two North Carolina counties are working with the U.S. Coast Guard and other public agencies, and the private sector, to develop plans and preparations for a full-scale mass-rescue exercise scheduled to take place in January 2006. The exercise scenario will simulate the sinking of a casino boat off the North Carolina coast and the rescue of up to 600 passengers.

Unlike previous emergency drills of a similar nature, the 2006 exercise calls for the participation of private boat owners and other transportation entities as well as such nonprofit emergency organizations as the American Red Cross and Salvation Army.

Kenneth Beans, Horry County's assistant fire-rescue chief, said that next year's exercise is expected to give emergency responders an opportunity to hone their operational skills while also enhancing their ability to integrate and operate with other agencies. The exercise will place these and other responders in situations with which they may be unfamiliar, such as a requirement to carry out triage processes on the water to determine the extent and seriousness of victims' injuries before transporting them to land facilities for appropriate medical treatment.

Do you have the best response tools?

MultiRAE Plus

PID plus multi-gas equals protection from the unexpected

- Toxic Industrial Chemical (TIC) vapors
- Flammable gases and vapors
- Oxygen concentrations

HazRAE

Chem/Bio/WMD Decision Support

- A 6-foot stack of HazMat references in your hand
- Identifies unknowns using signs and symptoms
- Speeds the transition from detection to decision

PlumeRAE

Plume Measurement and Prediction

- Down-range wireless monitors tell you where the plume is located
- Easy-to-use complete system
- Quick toxic threat evaluation

GammaRAE II

Personal Radiation Detector

- Prominent visible, audible and vibration alarms
- Water-resistant for easy decon
- Fast response to radiological threats

RDK Gamma

Toxic Gas/Radiation Perimeter Monitoring

- Rapid Deployment Kit with wireless monitoring
- Remotely monitor threats up to 2 miles away
- Includes 4 down-range monitors for quick, adaptable response

www.raesystems.com

Hazardous Environment Detection Solutions

RAE SYSTEMS