

# Processes and Techniques for Providing Critical Data to First Responders to Maritime Security Incidents

K. J. Wydajewski, P.E., MTS Member  
Arion Systems, Inc  
15059 Conference Center Drive, Suite 200  
Chantilly, Virginia, 20151-3802, USA  
ken.wydajewski@arionsys.com

B.L. White, MTS Member  
Vice President, Arion Systems, Inc  
15059 Conference Center Drive, Suite 200  
Chantilly, Virginia 20151-3802, USA  
bwhite@arionsys.com

**Abstract** – First responders are those elements of law enforcement, fire and rescue, emergency medical services, and national security personnel including military units who respond to emergency calls of service. In this paper, the maritime terrorist threat is introduced and an updated status of the U.S. government’s response to the threat through organizational change is documented. Some of the more recent changes within the U.S. Coast Guard that affect the nation’s posture against maritime terrorism are presented. A list of some of the first responders and supporting organizations to a maritime security incident is provided. A plausible incident scenario is used to illustrate the resulting flow of information and the need to rapidly disseminate data to the first responders to help them be both safe and effective.

First responders for a maritime security incident include federal, state and local law enforcement, fire and rescue units; USCG and National Guard military personnel; hazardous materials response teams, emergency medical services and public health officials. National security personnel on specialized chemical and nuclear incident teams directly support the first responder community. We contrast first responders by virtue of their official function, as opposed to others who may be first on the scene but usually with less specialized emergency training such as certain marine facility personnel, vessel operators, dockworkers, private security personnel, marine waterway pilots, and recreational boaters.

## I. INTRODUCTION

Terrorism has forever altered the American way of life. The attacks on the World Trade Center and the Pentagon last September clearly reflect that our open society is at risk from terrorists seeking to disrupt our economic, social, political, and religious foundations. Future attacks on our homeland may include maritime targets and therefore affect our ports, waterfront facilities, commercial, government and recreational vessels, and offshore platforms. Highly vulnerable facilities such as oil refineries, chemical storage plants, offload terminals, bridges, and nuclear power plants also can be targets of terrorists. The maritime community must continue to take action to prevent and mitigate the consequences of such attacks to our marine transportation system. With 361 ports, more than 1,000 harbor channels, 25,000 miles of waterways and 95,000 miles of shoreline, we have a significant amount of maritime real estate and infrastructure to protect in the 21<sup>st</sup> century.

Recent statements issued by the U.S. Coast Guard (USCG) have warned of possible attacks on our ports and maritime facilities. The Bush administration also cautioned of possible terrorist activity by SCUBA divers or underwater swimmers with breathing regenerative devices, while the Director of Homeland Security reported that Al Qaeda has shown interest in training terrorist cells to attack ports and ships. In May 2002, three Saudis were arraigned in a Moroccan court, charged with plotting to sail a dinghy loaded with explosives from Morocco into the Straits of Gibraltar to attack U.S. and British warships. These reports echo back to the bombing of the USS Cole and clearly indicate that our vessels and marine transportation system are prime targets for terrorists.

First responders often need key information available in federal and state databases that track maritime infrastructure, personnel, and cargo. Disseminating “critical information” on potential consequences of a terrorist event to the lowest level within the first responder hierarchy assists in the planning and prevention of maritime terrorism incidents. Some of the critical information may be shared-intelligence on terrorist organizations and their operational patterns or threat characterization. Other information is critical to rapidly identify the suspect vessels as “high interest vessels”, or HIVs, classify the threat and determine appropriate disposition. This can be a very routine and tedious data gathering and analysis procedure. Examples of critical data on a vessel may include vessel identification number, ship’s current position, registry information, current voyage information, planned destination, vessel arrival/departure date and time, crew list, cargo manifest and any potential threat.

Responding to terrorism requires both crisis management and consequence management. The FBI, as the lead federal agency for crisis management under Presidential Decision Document 63 (PDD63), identifies, acquires, and plans the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. While the FBI is “in charge” in matters of confirmed terrorism, initial responses and case development are functions usually performed by local and state police and emergency response public safety teams. Special federal and military forces may directly support the FBI and state and local crisis response authorities. Once opening a federal case, under PDD63 authority, the FBI investigates and prevents terrorist threats and apprehends those responsible for terrorism. As an element of the Justice Department, the FBI is augmented in prevention and preparedness through the services of the National

Infrastructure Protection Center. The Center directly assist states and local governments to prepare better by using counter-terrorism procedures more effectively and in a more coordinated inter-agency and inter-governmental approach to protect their critical infrastructure. Overall, crisis management is primarily a law enforcement function.

State and local governments, by contrast, exercise primary authority for consequence management (under the Federal Response Plan with Terrorism Annex). The function of consequence management is to protect public health and safety, restore essential services, and provide emergency relief to governments, businesses, and individuals affected by the aftermath of terrorism. FEMA is the lead agency for consequence management including federal maritime emergency response efforts; however, the USCG Captain of the Port (COTP), local emergency medical services and the local fire department are responsible for initiating a coordinated response effort for all major accidents including security incidents that lead to major disasters at a port or in the waters within their jurisdiction.

The maritime community requires timely information and coordination among the intelligence community and federal, state, and local responders. With existing communication techniques and processes, responders can rapidly assess a security incident and render assistance as an incident unfolds in real-time only if they have prepared well in advance and worked out their inter-agency processes and mutual supporting relationships.

## II. MARITIME TERRORISM THREAT

Consider the sequence of events, shown in Fig.1, for a hypothetical maritime security incident. A liquefied propane gas (LPG) tanker departs a foreign port on a trans-Atlantic voyage to the U.S. Loaded with over 126,000 cubic meters of super-cooled LPG, the foreign-flagged vessel transits the Atlantic Ocean without incident. As the vessel is within 96 hours of entering a major East Coast port in the US, the ship owner emails the Notice of Vessel Arrival, or NOVA, information to the USCG's National Vessel Movement Center (NVMC). The NVMC compiles the information, including vessel statistics, crew list, non-crew and passenger list, cargo list, current voyage information, safety management certificate, and intended ports of call. This information is disseminated to the USCG National Command Center (NCC), National Response Center (NRC), and the National Maritime Intelligence Center (NMIC). NMIC analyzes the information comparing the crew lists against lists of known terrorists and other criminals and disseminates their findings to the Office of Homeland Security and organizations within the police and intelligence community. The USCG Marine Safety Office (MSO) or COTP at each port in the United States also receives the NOVA information and a list designating certain HIVs with associated rationale for taking additional precautions and procedures. Once operational actions are

completed, combined agency follow-up actions and findings by the COTP directed boarding teams are disseminated in daily Situation Reports distributed among the homeland security and defense agencies. Interagency coordination occurs at the local port level through collaboration and relationships established in Port Safety and Security Committees.

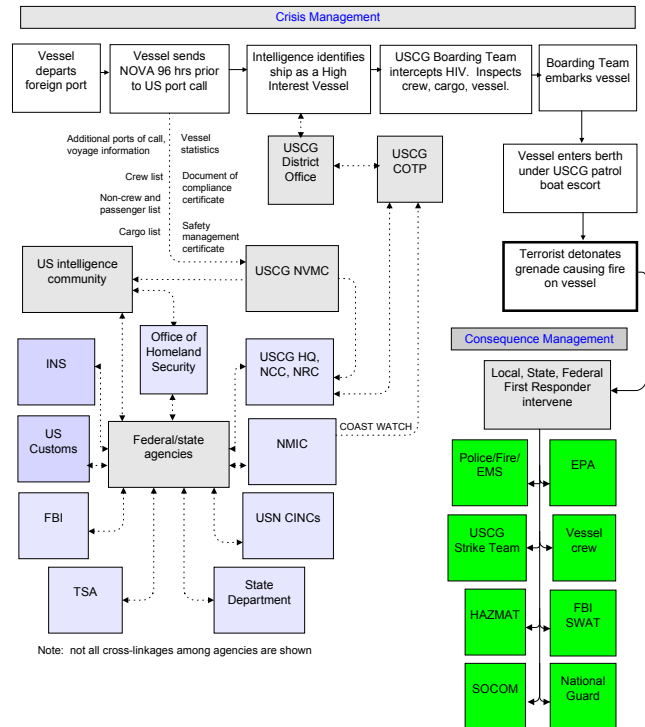


Fig 1. Sample maritime security incident.

An important aspect of this scenario is the process of screening and intelligence analysis. This requires shared access to various highly secure databases. Analysis within the intelligence community revealed that one of the ship's crewmembers was on a Terrorism Watch List. A cross-check by the Immigration and Naturalization Service (INS) using the Interagency Border Inspection System (IBIS) verified that the suspect was a potential terrorist. The NMIC classified the ship as a HIV and relayed the information to the Coast Guard's NCC and COTP in the major east coast seaport via secure landline. The U.S. Customs Service (U.S. Customs), using its automated cargo database, confirmed that the vessel was transporting LPG exclusively.

The operational aspects of the scenario might occur as follows. The COTP at the East coast port readies a USCG boarding team to investigate the suspected crewmember. The team, perhaps transported onboard a 52-meter Navy patrol craft, intercepts the HIV approximately twelve nautical miles seaward of the coast. The 6-person team boards the HIV and divides its forces into three 2-person elements: two in the pilothouse, two in the engine room, and a roving security patrol topside. The team questions the suspected terrorist and

finds nothing unusual about his actions or responses. The individual produces a mariner's identification card and does not appear to have any contraband in his possession. The boarding team relays the information about the crewmember to the COTP at the east coast port. Subsequent liaison with INS, USCG intelligence, and other maritime agencies reveals that the crewmember's card is valid. Walk-around inspections by the boarding team do not reveal any suspected signs of planned terrorist activities to the vessel, LPG piping systems or vessel machinery. However, just to be sure, the INS and the COTP require the vessel master to restrict the crewmember to the ship during the port visit and post a private armed guard to ensure that the crewmember does not leave the ship.

The HIV takes on a commercial pilot near the sea buoy to guide the vessel up river. The boarding team remains on the vessel during the transit up the river. The boarding team closely watches the actions of all crewmembers during the journey. VHF radio communications between the HIV and the COTP are maintained. The patrol craft is joined by another USCG patrol craft and they establish a moving safety zone around the vessel, escorting the LPG tanker as it proceeds to the offload terminal. As the vessel approaches its intended berth, two commercially piloted tugboats assist the vessel into docking position.

After the vessel berths, and the private security guards are posted, the boarding team returns to the patrol craft and the pilot embarks on the pilot boat. Working with employees from the LPG terminal, the ship's crew begins to offload the LPG into large shore-based storage tanks. The vessel master of the HIV does not see any suspicious activity during offload operations.

Without warning, an explosion occurs within the vessel. The explosive, caused by an improvised explosive device detonated by the suspected terrorist, rapidly causes a large diesel fuel fire to develop in the engine room. The vessel master immediately notifies the COTP through the Coast Guard Group command center using VHF Channel 16. The Group, in turn, contacts the Port Authority and the port fire department as well as the NRC. First responders from the port city fire department, including a hazardous material team, arrive on scene and begin to assist the vessel crew in fighting the fire. The fire department establishes incident command (IC), while the COTP and the port authority maintain control, advise and direct vessel traffic and marine assets within the port. The fire department rapidly determines the total number of personnel on the vessel and the amount of LPG on the ship. They consider these aspects as part of their IC system:

- Rescue of endangered persons
- Initial actions to prevent incident from enlarging
- Obtain vessel data
- Determine life hazard and fire situation

- Determine status/condition/and control of vessel fire protection systems and equipment
- Status/condition/and control of other vessel systems
- Vessel dewatering and vessel stability.

Concurrently, the COTP notifies the USCG's National Strike Force Coordination Center (NSFCC), where a call is made to dispatch the USCG Atlantic Strike Team. The NRC notifies the FBI, who immediately relays the information to the Special Agent in Charge (SAC). The SAC initially sends an Advance Investigation Team to the scene to lead the investigation with state and local police forces and set up a federal incident command post. The USCG Strike Team collects information from the vessel master and the fire department about hazardous materials aboard the ship, including the LPG and petroleum, oil and lubrication products. The USCG Strike Team contacts the NRC for phone consultation with experts regarding the potential dangers of a combined LPG and fuel oil fire. The NRC also notifies the Office of Homeland Security (OHLS). The OHLS rapidly reanalyzes intelligence sources and uses its Homeland Security Advisory System to set the U.S. security threat condition to red in this East coast port with orange in other key seaports. Similarly, the NCC sends a message to all U.S. ports through their COTP – Port Safety and Security Committee network, warning of possible follow-on attacks at other ports.

As the vessel crew fights the fire, the FBI-led police tactical team takes the terrorist into custody. Conditions worsen and the fire rapidly spreads. The COTP, having joined up with the local and state public safety agencies, coordinates closely with the FBI incident command post through a unified command model which follows Incident Command System doctrine. The COTP establishes a waterborne security zone around the vessel and surrounding areas to reduce the risk of fire casualties on other vessels within the port. The COTP then issues an order preventing other commercial or recreational vessels from entering the port, thereby closing the port to all but emergency vessel traffic. In addition, first responders and USCG personnel in the unified command assess the situation and begin preparations to evacuate all non-essential personnel from the port, offload terminal and outlying areas.

As the fire intensifies, the entire ship becomes at risk. The vessel's crew is ordered to leave the vessel. A special boat on the scene sprays a steady wall of low velocity fog across the vessel to fight the fire. The situation worsens as the fire spreads throughout the vessel. The fire continues to burn for two days, causing round-the-clock first responder actions. After 48 hours of battling the fire, the first responders stop the fire. The fire produces no casualties. The vessel is a total loss and the environmental impact within the harbor requires cleanup and marine salvage operations. In addition, the incident causes a four-day stoppage of commercial vessel traffic into the port. This disrupts the flow of gas products to several locations along the eastern

seaboard, creating a serious, albeit temporary, economic disruption to certain locales.

The above hypothetical scenario illustrates how a terrorist can inflict damage to a commercial vessel bound for the US despite the best security precautions. The scenario shows that maritime first responders depend upon critical data on vessels and port facilities to safely and effectively take action during a security incident. Rapidly and effectively disseminating this critical data among members within the first responder community is critical to the overall success of the first responder actions.

### III. THE CRITICAL ROLE OF COMMUNICATIONS

Many communication systems, sprouting a myriad of acronyms, are presently in use throughout the maritime community. These systems include secure cellular phones and landlines, VHF, HF, UHF, digital selective calling on VHF/HF, INMARSAT, GMDSS, COSPAS-SARSAT, and AIS. These communication techniques allow mariners to send and receive information while at sea, and provide a means to alert USCG and US Navy units of security incidents.

The Global Maritime Distress and Safety System (GMDSS), initiated by the International Maritime Organization (IMO), is based on a combination of satellite and terrestrial radio services, and has changed international distress communications from being primarily ship-to-ship based to ship-to-shore (Rescue Coordination Center) based. GMDSS consists of several systems, some new and many of which have been in operation for quite some time. GMDSS will be used to perform the following functions:

- Alerting, including position determination for the unit in distress
- Search and rescue coordination
- Homing
- Maritime safety information broadcasts
- General communications
- Bridge-to-bridge communications.

VHF/HF are used within ports for ship-to-shore and ship-to-ship communications. Limited to line-of-sight, the USCG uses VHF primarily to communicate with vessels transiting ports. GMDSS and COSPAS-SARSAT are primarily used for search and rescue operations. Ship-to-ship communications via Tactical HF and Navy HICOM are additional techniques that commercial vessels use to request U.S. Navy assistance in emergency situations. However, Fleet CINC command center approval is needed prior to establishing extended ship-to-ship communications between merchant ships and USN afloat vessels.

The Automated Identification System (AIS), a line-of-sight continuous broadcast signal used to transmit ship-to-

ship and ship-to-shore data up to 20 nautical miles, allows commercial ships and coastal authorities to obtain digital ship information, including position and identity. AIS is predominantly an aid to navigation system that is especially useful to vessels in situations where physical obstructions prevent radar detection. AIS also provides a method for ships to identify other ships. The IMO is in the process of accelerating the implementation for the mandatory fitting of AIS on all ships 300 gross tonnage and above on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages, and all passenger ships. The AIS applies to all ships constructed after 1 July, 2002, with a phase-in scheduled requirement of 1 July, 2008.

In a maritime security incident, these communication techniques will be used to transmit critical data to USCG and other Navy units. The location of the incident and availability of shipboard communication equipment will determine which technique will be the most effective method of sending and receiving data to USCG and other Navy units. Close to shore or within port regions, VHF will most likely convey the information to the USCG COTP. For maritime security incidences occurring further offshore, communication systems such as INMARSAT, GMDSS, and other satellite-based systems will prove to be the most reliable and expeditious method of communication to report security incidents. In any case, critical information on the incident must be rapidly relayed to the first responders in order to make their actions effective. Landline and cellular communications are a common method to activate first responders and establish interagency communications.

### IV. GOVERNMENT ORGANIZATIONAL CHANGE

Many U.S. organizations have made changes in response to the events of September 11<sup>th</sup> and the recent terrorist threats. Large organizational changes have occurred and are continuing to evolve within the government hierarchy.

Last December, Congress amended the Merchant Marine Act of 1936 by passing the Port and Maritime Security Act of 2001. The amendment ensured greater security for U.S. seaports. Key areas in the legislation included the requirement for conducting initial security evaluations and port vulnerability assessments, establishing local port security committees, and maritime facility security plans at all U.S. ports. Others requirements mandated that ports improve security infrastructure, such as security monitoring and recording equipment, concealed video systems, and remote surveillance systems [1].

Bipartisan legislation to establish a comprehensive national system to increase anti-terrorism security at U.S. ports and waterways is pending. Two bills, one in the House and one in the Senate, will expand the role and authority of the USCG in countering maritime terrorism. A key provision of both bills requires that the USCG conduct vulnerability assessments of U.S. ports. The results will be used to

implement a 3-part national maritime transportation planning system, consisting of a comprehensive national plan, specific area plans, and local vessel and marine facility plans. These tailored plans are intended to deter a catastrophic marine event to the maximum extent possible. A final bill, expected to pass later this year, is expected to require the USCG to assess the effectiveness of security systems in foreign ports, and to deny entry to vessels from ports that do not maintain effective security [2].

The USCG NRC is an important first responder organization. The NRC is available 24 hrs a day to take reports of oil, hazardous materials (hazmat), biological, and chemical spills and/or suspicious activity on/or near the water. The NRC's extensive reference materials, advanced telecommunications and operation of automated chemical identification and chemical dispersion information systems are invaluable tools for the maritime first responder community. The NRC and the USCG NCC work closely with the Office of Homeland Security and the NMIC. Collectively, these organizations share and disseminate important intelligence information related to maritime security response and anti-terrorism efforts.

#### *A. Department of Homeland Security*

In June of this year, President Bush announced a major initiative to reorganize parts of the federal government. The reorganization, slated for completion later this year, will create a Department of Homeland Security. This Department is expected to consist of four divisions [3]:

- Border Transportation and Security
- Emergency Preparedness
- Chemical, Biological, Radiological, and Nuclear Countermeasures
- Information Analysis and Infrastructure Protection

The Department of Homeland Security will help remove barriers to efficient border security. When a ship enters a U.S. port, for example, U.S. Customs, INS, USCG, and the U.S. Department of Agriculture (USDA) have overlapping areas of responsibility aboard the ship. INS has jurisdiction over the personnel on the ship, U.S. Customs is concerned with the ship's cargo, and the USDA has jurisdiction over certain goods. The USCG has authority over the ship while it is underway. In practice, the USCG relies on the INS to enforce U.S. immigration laws and prevent the entry of illegal immigrant into the U.S. Similarly, the USCG relies on U.S. Customs to seize any illegal cargo found onboard the vessel. However, these organizations may not always disseminate the information among themselves in a timely manner. The consequences: instead of detaining potential terrorists and monitoring and controlling all dangerous cargo at sea, our present structure can allow terrorists to enter our ports, exploit the danger of the cargo and sneak undetected into our society [3].

#### *B. U.S. Customs*

U.S. Customs established a new Office of Anti-Terrorism, and an Office of Border Security last October. Custom agents, working under Operation Shield America, are monitoring exports of strategic weapons and materials from the U.S. Customs agents are working round-the-clock to prevent international terrorist groups from gaining sensitive U.S. technology, weapons and equipment that could be used in another terrorist attack.

U.S. Customs proposed a program to safeguard the more than 5.7 million ocean going containers that enter and reenter the United States each year on over 214,000 vessels. The four-level program, entitled the Container Security Initiative, or CSI, is designed to achieve a more secure maritime trade environment while accommodating the need for efficiency in global commerce. The CSI consists of four elements: 1) establishing security criteria to identify high-risk containers, 2) pre-screening sea containers before they arrive at U.S. ports, 3) using technology to pre-screen high-risk containers, and 4) developing and using secure and smart containers [6]. The purpose of the CSI is to engage the ports, and the respective governments, that send the highest volumes of container traffic to the U.S. in a way that will facilitate detection of potential problems at the earliest possible opportunity [4]. U.S. Customs also contacted the governments of the top 10 "mega-ports" that send containers to the United States to solicit their participation in the CSI. Several of these "mega-ports" include Hong Kong, Shanghai, Singapore, and Tokyo.

In addition to CSI, Customs introduced an initiative called Automated Commercial Environment, or ACE, to assist in automating trade and enhance cargo targeting abilities within their vast database on shipping and trading activities known as the Automated Manifest System, or AMS. Using the ACE targeting system within the AMS, Customs agents will be able to sort through cargo manifests submitted by shippers and carriers, and identify those manifests that appear unusual, suspect, or high-risk [5].

#### *C. Immigration and Naturalization Service*

Accessing the Consolidated Consular Database, INS agents can look up via records and photos for immigrants and nonimmigrants as they arrive in ports. The database will complement the existing Interagency Border Inspection System, or IBIS, that is presently used by many agencies to keep track of information on suspect individuals, businesses, vehicles, aircraft, and vessels.

#### *D. Federal Bureau of Investigation*

The FBI created 21 new Joint Terrorism Task Forces, JTTFs, this year to expand the level of interaction and cooperation between FBI Special Agents and their Federal, state and local counterparts. The JTTFs also enhanced the flow of information between participating law enforcement agencies. Participants on JTTFs include U.S. Customs, INS, U.S. Coast Guard and other major federal organizations,

along with state and local agencies. Following the terrorist attacks last September, FBI established a permanent Terrorism Watch List, or TWL, to serve as a single integrated listing of individuals of investigative interest for the law enforcement and intelligence communities. The TWL assists both the intelligence and law enforcement communities during investigations by alerting officers or agents should a person of interest in a terrorism situation be encountered by another agency [6]. In addition, the FBI's newly established Office of Intelligence will ensure that information flows within the FBI and also to other agencies with the law enforcement and intelligence communities. The FBI Strategic Information Operations Center (SIOC) weapons of mass destruction desk works closely with the NRC for all terrorism alerts and incidents reported through the national system.

#### *E. Transportation Security Administration*

Created by the Aviation and Transportation Security Act of 2001, TSA is focused on protecting the vast network of roads, railways, and airways and waterways throughout the U.S. TSA is working to improve the safety of U.S. ports by partnering with private industry to conduct Port Vulnerability Assessments. TSA is starting these efforts by focusing on the critical national seaports to enhance facility and operational security. TSA obtains key information from other federal agencies using databases and situation reports submitted to the Transportation Information Operations Center, or TIOC and the Director of Transportation Intelligence (S-60). TSA has recently negotiated with the NRC to set up a nation-wide transportation terrorism tips hotline. It is interesting to note that the recently appointed head of TSA is Admiral James Loy, former Commandant of the USCG.

### V. USCG HOMELAND SECURITY

The United States Coast Guard has significantly enhanced its mission to reflect its lead role in securing the U.S. maritime environment. Under Operation Neptune Shield, the USCG has performed the following actions since September 11<sup>th</sup>:

- Established near shore and port domain awareness with 55 cutters, 42 aircraft and hundreds of small boats patrolling our coastlines
- Deployed 4 Port Security Units to the domestic ports of Boston, New York City, Seattle, and Los Angeles/Long Beach
- Recalled more than 2,700 selected reservists to support maritime security operations in 350 ports
- Changed the 24 hour Notice of Arrival requirement for ships entering U.S. ports to 96 hours [7]

These initial responses have since been scaled back but the overall presence and readiness of Coast Guard port security is higher now in many ports than it was in World War II.

As part of Neptune Shield, the Coast Guard adopted a Maritime Homeland Security Strategy to use their core competencies to aid other agencies operations. This approach extends the maritime borders outward to detect, deter, disrupt and intercept terrorist threats. The strategy incorporates the concepts of awareness, prevention, response, and consequence management into three scaleable maritime security (MARSEC) postures for ports:

- MARSEC-1 [New Normalcy]. Includes more interagency fusion, intelligence and information on cargo, people and vessels; enhanced command and control; increased port security patrols; establishing maritime safety and security teams, or MSSTs; and exercising Port Security Committees (PSCs) ability to exchange information on classified port threats.
- MARSEC-2 [Heightened Risk]. Set if credible intelligence suggests a high threat, but without a specific target or delivery method.
- MARSEC-3 [Incident Imminent]. Provide for maximum alert and will be appropriate when credible intelligence is obtained with a specific threat.

Note that MARSEC 2 and MARSEC 3 are surge operations for scenarios with elevated threats. Currently, these activities would often require some augmentation from DOD and could, over time, degrade the Coast Guard's ability to perform other missions such as drug interdiction operations, alien migrant interdiction operations, and fisheries law enforcement.

The Maritime Homeland Security Strategy is centered on five key principles:

#### *A. Build Maritime Domain Awareness*

An increasingly important concept in the Coast Guard's fight against the war on terrorism is maritime domain awareness. This concept requires information, intelligence, surveillance and reconnaissance of vessels, cargo and personnel. It can be viewed as a clear understanding and total awareness of maritime vulnerabilities, targets and threats. It provides operational units and command and control offices with a common operational picture, one that links intelligence and known threats to vessel movements, vessel crews and shipboard cargo.

The Coast Guard's new NVMC was established since September 11<sup>th</sup> to track the arrival and movement of all foreign flagged vessels intending to enter the United States. Commercial vessels over 300 gross tons are now required to provide information about their cargo, crew and vessel, 96

hours in advance of arrival. This requirement is up from just 24 hours in advance prior to last year's terrorist attacks. In September, the Coast Guard also established a new regulation prohibiting vessels from approaching closer than 100 yards of any U.S. Navy vessel in U.S. waters without permission. Entitled the Naval Vessel Protection Zone (NVPZ), the USCG is using also the regulation to require that vessel operators maintain slow speed when passing within 500 yards of any Navy ship.

The USCG has also fostered maritime domain awareness by increasing the number of patrol boats in ports and along the coast. In addition, the USCG has obtained funding to establish new intelligence fusion centers to collect, analyze and share information within the Coast Guard and with other agencies.

#### *B. Enhance Presence and Response Capabilities*

This element focuses on the USCG's role to deter, detect, intercept, and interdict potential threats. The events of September 11<sup>th</sup> demonstrated that the global reach of terrorism requires a higher maritime security posture and a "new normalcy" for Coast Guard mission priorities and capabilities. The Coast Guard has developed a maritime homeland security strategy that incorporates core competencies into a layered operation that will push our maritime borders outward, and detect, deter, disrupt, intercept, and respond to terrorist threats across the maritime domain as well as ensure the protection of maritime infrastructure from within. This strategy recognizes that terrorism can strike from within our nation or from outside our territorial boundaries. The Coast Guard is preparing to counter both vectors of attack. That strategy is preemptive in nature, and requires the Coast Guard to develop special capabilities with new skills. One of these required specialized capabilities are Maritime Safety and Security Teams (MSSTs).

Following the events of last September the USCG deployed four of its six Port Security Units (PSUs) to enhance security in the ports in Boston, New York City, Los Angeles/Long Beach and Puget Sound. Staffed with approximately 140 Selected Reserve personnel PSUs are equipped with heavily armed rapid response boats. Although the primary mission focus of the PSU is providing antiterrorism/force protection in foreign ports they were quickly pressed into domestic service. The USCG also established two Interim Maritime Safety & Security Teams (IMSSTs), one for each coast, using personnel and equipment from existing Tactical Law Enforcement Teams (TACLETs). TACLET personnel are highly trained law enforcement specialist typically employed for interdiction of illegal drug and alien migrant smuggling. Using emergency legislation and funding provided by Congress, the USCG is in the process of establishing a total of twelve MSSTs. By Fiscal Year 2003, four MSSTs commissioned will be operating in Seattle, Chesapeake, San Pedro and Galveston.

Staffed with 72 active duty personnel and augmented by 33 Selected Reservists, MSSTs provide a new specialized capability necessary to address the spectrum of operational requirements associated with the ports, waterways and coastal security mission. MSSTs will protect military load-outs, enforce security zones (moving and fixed), defend critical waterfront facilities in strategic ports, conduct maritime law enforcement operations, and provide a modest level of shore-side force protection.

In April 2002, one IMSST and other USCG personnel trained and tested the Coast Guard's response capability during Exercise Harbor Shield. The exercise, held near the port of Charleston, focused on small boat defensive tactics and the combined ability of federal, state, and local agencies to join forces to protect the port. The training included shore-side and waterfront protection of piers, marinas, and bases including anti-swimmer tactics, mock underwater mine sweeps, the enforcement of security zones, and escort of an arriving cruise ship. Many of the lessons learned from Harbor Shield have been used to develop the training now being used during the initial standup training of the MSSTs.

#### *C. Ensure the Controlled Movement of High Interest Vessels*

The Coast Guard uses both boarding teams and a new program referred to as Sea Marshals to prevent criminal and catastrophic events as a HIV transits a port. The armed Sea Marshals guard against possible terrorist attacks that may be attempted from those already onboard the ship. The boarding teams are capable of conducting thorough searches of the ship to ensure that no hidden threats exist prior to the vessel being allowed entry to the port. Sea Marshals and boarding teams generally protect against internal threats while patrol boats and MSSTs generally protect against external threats. This layered approach helps to ensure that positive control of the vessel is maintained throughout the vessel's transit.

#### *D. Protect Critical Infrastructure and Enhance Force Protection*

The USCG has adopted measures to enhance protection to critical facilities within our marine transportation system. The USCG has increased patrols and established security zones in the waters near potential terrorist targets such as chemical facilities, nuclear power plants, bridges, and military facilities.

The Coast Guard is presently conducting Port Vulnerability Assessments at 50 critical U.S. ports. Working with the Maritime Administration (MARAD), TSA and private industry, these assessments will help to identify existing security gaps within ports. The assessments will provide COTPs with recommendations for enhancing force protection at key U.S. ports. The USCG also requested \$51 million in funding for anti-terrorism and force protection measures which include physical infrastructure, cyber-security, personal protective equipment, and firearms.

### *E. Increase Domestic and International Outreach*

The USCG has adopted a homeland defense concept of “pressing out our borders.” This layered defense concept will protect vessel approach areas to the U.S. including overseas departure zones, trans-oceanic routes, coastal zone routes within the U.S. and U.S. port zones. The consequences in first discovering a weapon of mass destruction on a vessel, in a U.S. port, would be devastating. Our goal should be to counter the terrorist threat before it reaches U.S. soil. Hence, protecting our marine transportation system should start overseas in foreign ports and conclude with the homeland defense of our nation’s ports and infrastructure.

The Coast Guard is promoting a public campaign on terrorism because of the enhanced public awareness of illegal activities. The Homeland Security Harbor Watch Program was established to inform, educate, and enlist the support of all individuals who see suspicious activities. The program provides the public with telephone numbers to report illegal activities witnessed near or around recreational boats, commercial vessels, waterfront facilities, bridges and other places of particular interest. Information on this program is available on several Coast Guard MSO websites.

The USCG increased its planning and coordination with local first responders, law enforcement and fire and maritime organizations that have a stake in port and waterway security. Each COTP now hosts periodic Port Security Committee meetings. The meetings are a convenient method for the USCG and other federal, state and local agencies to discuss security and first responder plans. The meetings also foster the sharing of information among maritime organizations that are responsible for keeping our ports, waterways and coastlines safe.

## VI. MARITIME FIRST RESPONDERS

Maritime first responders are the first line of defense for consequence management. First responders include federal, state, local, and civilian personnel within fire and rescue departments, law enforcement, nuclear and weapons of mass destruction emergency support teams, and environmental protection and hazardous material teams. No one agency has sufficient resources to singularly fight all major vessel fires or respond to a significant number of concurrent maritime security incidents. First responders must coordinate with public safety agencies, waterfront facility owners and operators, vessel owners and operators, USCG, and other military departments or agencies to render an incident safe.

The COTP exercises primary federal responsibility for the security and safety of the port. As such, the COTP enforces munition loading regulations, marine terminal safety regulations, pollution prevention regulations, and navigation regulations. Many COTPs use a port-specific Marine Fire Fighting Contingency Plan, linked to facilities response plans and Area response plans to establish policies, responsibilities, and procedures for coordination of on-scene forces.

Responsibilities of the COTP in a maritime security incident aboard a vessel or waterfront facility include:

- Support and directly coordinate with the incident command for a burning vessel underway or at anchor where the local fire department, state fire fighting agency or contracted fire fighting service has lead responsibility in the plan
- Establish safety or security zones
- Provide information on involved waterfront facilities and the location of hazardous materials on the vessel or at the facility
- Provide technical data of ship’s construction, stability, and marine fire fighting considerations
- Respond to oil or hazardous materials discharges
- Alert owners and operators of terminal or vessel at risk
- Augment incident commander’s communications capabilities to improve coordination with response personnel

Possible first responders to a maritime security incident include the following:

- Vessel crews
- Local fire, rescue, and emergency service personnel
- Marine firefighting boat crews
- Local law enforcement and civilian port security
- Natural resource police and marine police units
- USCG MSSTs and harbor patrol boats
- USCG Strike Teams and Port Security Units
- Environmental Protection Agency (EPA) radiological response teams (RAD) and EPA contracted HAZMAT teams.
- Hazardous material response units
- FBI SWAT teams
- National Guard Civil Support Teams
- U.S. Special Operations Command forces
- Navy Explosive Ordnance Disposal teams
- Civil Air Patrol
- Others

Interagency communications using a compatible communications network is an important factor in establishing a unified operational response. Coast Guard operational units and local fire departments generally rely on hand-held VHF radios and landline/cellular communications during response operations. Several MSOs maintain contingency communications kits, consisting of VHF radios and base stations, for use during an oil spill response. USCG

Strike Teams also have a suite of programmable hand-held VHF-FM radios, portable repeaters, and portable satellite telephone systems. COTPs also have the ability for secure communications using secure telephone units, scrambled cellular portable telephone, and data encrypted security VHF-FM radios. Coast Guard Strike Teams have portable communications vans that substantially can augment local incident commander's communications capabilities. The National Response Center has three INMARSAT M-4 portable "points of presence" satellite video-conference sets that were deployed to the NYC site of the 9-11 attack. Coast Guard 115 meter Cutters and several other platforms are floating communications and command centers that can be brought into a disaster zone and provide a viable mobile, offshore platform for command post and forward logistics coordination.

The timely sharing of critical information on a regular basis would assist first responders in planning for crisis management and engaging in consequence management. Selective and current information on vessels, personnel, and cargo contained in USCG, INS, U.S. Customs, FBI and other government databases must be made reasonably accessible to first responders.

A recent maritime security incident required inter-agency communication and a well-coordinated response effort. In November of last year the M/V Aurora Opal, a Philippine-flagged vessel, arrived at the deep-water port in Bucks County, Pennsylvania to offload a cargo of steel wire rope. Located along the Delaware River, the port is privately owned and employs union dockworkers. The vessel originated from St. Petersburg, Russia in mid-October and was on her third port-of-call in the U.S. during this trip. The vessel was boarded and inspected by the USCG prior to entering the U.S.

While attempting to offload huge coils of steel located in the forward lower cargo hold of the 174 meter vessel, the dock workers noticed the foot-high letters "Bin Laden" spray-painted on the coil packaging, as shown in Fig. 2. Though the Bin Laden family leads a well-known international construction firm, some additional observations required closer scrutiny of this situation. Further inspection of the wire rope, revealed a white powdery substance on the outer layers of the zinc wire rope and on the vessel deck near the steel coils. Although the powdery substance appeared to be zinc oxide, the result of seawater dripping through the deck hatch covers and reacting with the wire rope, the terminal supervisor took precautionary measures to guard against a possible anthrax case. The terminal supervisor promptly called the Fire Marshal of the Falls Township Emergency Services to report the incident. The situation was reported to local authorities.



Fig.2. Zinc wire coils on M/V Aurora Opal with the word "BIN LADEN" spray painted on coil (Falls Township Emergency Services, 2001).

The fire marshal, serving as the Incident Commander for the situation, responded and performed a risk assessment to determine if the substance was anthrax. This situation was handled in accordance with local and federal policies for dealing with an unknown hazardous material. The fire marshal also reported the situation to the COTP for Group Philadelphia and contacted local law enforcement. The COTP, in turn, called the NRC and the NCC. The NRC notified both the FBI and the Centers for Disease Control in Atlanta. An FBI Special Investigations Team was dispatched to the scene to lead security tasking. Cargo operations were suspended and the COTP ordered the vessel, with its crew onboard, to remain in port at its current mooring until a public health official determined if the substance was anthrax.

An environmental testing company sampled the powder and turned it over to the FBI. The FBI also brought the samples to the Pennsylvania Health Office for examination. After a four-day period required by the test, the results were found to be negative for anthrax. Furthermore, there were no reported cases of crew members becoming ill. Because the fire marshal and the USCG had proof that the substance was not anthrax, the USCG allowed the M/V Aurora Opal to resume offload operations. After the remaining steel was transferred off the ship, the vessel left the port and proceeded to Wilmington, North Carolina.

The incident was categorized as an anthrax scare and received national press. The first responders and local authorities worked with the USCG and handled the situation correctly. Collectively, they communicated critical data to the proper authorities and took the necessary precautions and actions to render the situation safe.

## VII. SUPPORTING ORGANIZATIONS FOR MARITIME SECURITY

Many organizations are recognizing the need to work together in support of maritime security. Numerous organizations have regular representation on the USCG Port Security Committees. In the Port of Philadelphia, for example, the committee consists of personnel from Department of Defense units, critical industrial facilities, marine pilots and tugboat operators, commercial shipping lines, regional port authorities, stevedores and terminal workers, and maritime law. The information shared at these meetings has enhanced the awareness, prevention, response and consequence management of maritime security in the Philadelphia region. Selected members of security committees serve as a rapid means of disseminating warnings and alerts to the maritime community.

Other supporting organizations within the maritime industry include the International Maritime Organization (IMO), American Waterways Operators (AWO), and the American Association of Port Authorities (AAPA). IMO's International Code for the Safe Operation of Ships and for Pollution Prevention (ISM Code), which was mandatory for most ships trading internationally on 1 July 2002, addresses procedures for dealing with shipboard emergencies and also that adequate communications between vessel and shore-based personnel exist. The AWO and the Coast Guard are also working to improve vessel and personnel safety and strengthen communications between the USCG and the barge and towing industry. The AWO's sample Ship Security Plan, available on its website, is another step in the correct direction. Similarly, the AAPA has supported the concept of "pressing out our borders" by continuing research and development of inspection technologies that could identify chemical, biological, radioactive or nuclear cargo risk.

Unique maritime security and training organizations are also providing key support to the first responders. On the east coast, for example, the Tri-state Maritime Safety Association (TMSA) is enhancing maritime safety, preparedness, and response. TMSA, a private/public nonprofit partnership, is responsible for administering the day-to-day operations and training programs of the Delaware River and Bay Marine Fire Fighting Task Force and the Tri-state Search And Rescue. TMSA provides training in shipboard fire fighting, maritime first responder, and consequence management for vessel operators and marine management.

Maritime security is certainly an "all hands" evolution. All of us have a role in fighting terrorism. We can assist our maritime first responders and the marine community by reporting any suspicious activities that we encounter aboard vessels, in ports, and near waterfront facilities to the Coast Guard's National Response Center at 800-424-8802.

## VIII. CONCLUSION

The U.S. maritime terrorist threat is real. Preventing terrorist attacks to our ports, waterfront facilities, vessels, and offshore structures is a top priority for our government and private industry. In order to effectively and rapidly respond to maritime security incidents the first responder community must maintain communication paths to key federal, state, and local organizations.

Maritime first responders must continue to work with the USCG, INS, U.S. Customs, FBI and other key organizations to ensure that critical data is available and effectively communicated during a security incident. The dissemination of critical data between USCG and other organizations will enable fire/rescue and law enforcement personnel and other first responders to meet the challenge of crisis and consequence management. In addition, maritime first responders must liaison with supporting organizations of maritime security to enhance the informational "tool kit" necessary for countering attacks to our waterways, ports, and vessels.

The rapid dissemination of critical data to first responders is a significant requirement in defending our maritime environment and safely protecting our vessels, people, and marine infrastructure.

### Acknowledgments

The authors wish to thank CAPT Dennis Egan (USCG), LCDR Chris Clark (USCG), and CDR Steven Danielczyk (USCG) from the National Response Center for their assistance in explaining the roles of the NRC, NCC and other USCG units. Special thanks to LTjg Ben Perman (USCG), Group Philadelphia Marine Safety Office, for discussions on maritime security and port operations. The authors also thank Mr. Ed Copper (Fire Marshall, Falls Township) and Chief William Doty (Philadelphia Fire Academy) for, respectively, information on the M/V Aurora Opal incident and hazardous material response. The authors also express gratitude to Mr. Doug Dillon (TMSA) for discussions on consequence management and marine firefighting.

### References

- [1] 107<sup>th</sup> Congress, 1<sup>st</sup> Session, Port and Maritime Security Act of 2001 (S. 1214), December 2001.
- [2] J. LoBiondo, U.S. House Committee on Transportation and Infrastructure, Maritime Transportation Anti-Terrorism Act of 2002 (H.R. 3983).
- [3] President George W. Bush, The Department of Homeland Security, June 2002.
- [4] U.S. Customs Service, Office of Public Affairs, U.S. Customs Container Security Initiative to Safeguard U.S., Global Economy, February 2002.

- [5] R.C. Bonner, Hearing on Security at U.S. Seaports, U.S. Senate Committee on Commerce, Science, and Transportation, February 2002.
- [6] R.J. Jordan, FBI Information Sharing Initiatives, U.S. Senate Committee on the Judiciary Subcommittee on Administration Oversight and the Courts, April 2002.
- [7] USCG Office of Public Affairs, Homeland Security and the New Normalcy, [www.uscg.mil/homeland security](http://www.uscg.mil/homeland%20security).

Additional information for this paper was obtained from press releases by the USCG's Atlantic Area, Office of Public Affairs, and from the Coast Guard's website.