Report of the DHS National Small Vessel Security Summit

"...Managing the Risk"

Homeland Security Institute

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Report of the DHS National Small Vessel Security Summit	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Department of Homeland Security,20 Massachusetts Avenue, NW,Washington,DC,20001**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**122**	

Homeland Security Institute

The Homeland Security Institute (HSI) is a federally funded research and development center (FFRDC) established by the Secretary of Homeland Security under Section 312 of the Homeland Security Act of 2002. Analytic Services Inc. operates HSI under contract number W81XWH-04-D-0011.

HSI's mission is to assist the Secretary of Homeland Security, the Under Secretary for Science and Technology, and the Department of Homeland Security (DHS) operating elements in addressing national policy and security issues where scientific, technical, and analytical expertise is required. HSI also consults with other government agencies, nongovernmental organizations, institutions of higher education, and nonprofit organizations.

HSI delivers independent and objective analyses and advice to support policy development, decision making, alternative approaches, and new ideas on significant issues.

HSI's research is undertaken by mutual consent with DHS and is organized by Tasks in the annual HSI Research Plan. This report presents the results of research and analysis conducted under

TASK RP07-12-01

of HSI's Fiscal Year 2007 Research Plan.

The purpose of the National Small Vessel Security Summit (NSVSS) was to engage private, commercial and government stakeholders in discussions on a range of issues involving the security risks posed by small vessels in the U.S. maritime domain, including those risks involving international arrivals.

The results presented in this report do not necessarily reflect official DHS opinion or policy.

Homeland Security Institute

Charles Brownstein
Task Lead
John Baker
Peter Hull
Nicholas Minogue
George Murphy
Phyllis Winston

REPORT OF THE DHS NATIONAL SMALL VESSEL SECURITY SUMMIT

19 October 2007

Prepared for the Department of Homeland Security

ACKNOWLEDGEMENTS

The National Small Vessel Security Summit (NSVSS) could not have occurred without the constructive collaboration of many people. The Summit was deftly hosted and guided by RDML Brian Salerno of the U.S. Coast Guard. Keynote speakers and panelists including the Secretary of the Department of Homeland Security (DHS) Michael Chertoff and the heads of several other key DHS components. Experts on maritime threats, state and local law enforcement and port security authorities, and representatives from the recreational and commercial vessel communities contributed immensely to the richness and transparent nature of the Summit.

Credit is due to the members of the interagency expert working group that participated in six pre-Summit workshops to explore the topics to be covered, help develop the agenda, and design the exercise scenarios. Many DHS staff improved this report with their comments and suggestions.

Special thanks are due to Lieutenant Commander Katherine Dunbar and Mr. Robert Gauvin of the U.S. Coast Guard. They worked tirelessly to guide and facilitate the entire enterprise, including selecting an exceptionally accommodating meeting venue, identifying and inviting meeting participants, and working actively and effectively in every phase of planning and implementation. Along with the sponsorship, participation and understanding provided by RDML Salerno, they made this effort a rewarding and pleasant collaboration in the best sense.

Behind the scenes was a dedicated and capable team of skilled analysts, facilitators, and staff from the Homeland Security Institute (HSI) who were supported by Analytic Services Incorporated (ANSER) contracting, meeting services, and information technology experts. Special appreciation is due to Anna Taylor for tireless exercise of her administrative and editorial skills, to George Murphy for his leadership in scenario development, to Peter Hull for his patience and leadership in meeting logistics, and to Nicholas Minogue for his efforts throughout but especially in managing the preparation of this report.

Charles Brownstein, Fellow, HSI

HOMELAND SECURITY INSTITUTE

Analytic Services Incorporated
2900 S. Quincy Street
Arlington, VA 22206
Tel (703) 416-3550 • Fax (703) 416-3530
www.homelandsecurity.org

HSI Publication Number: RP07-12-01

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The purpose of the National Small Vessel Security Summit (NSVSS) was to engage private, commercial and government stakeholders in discussions on a range of issues involving the security risks posed by small vessels in the U.S. maritime domain, including those risks involving international arrivals. The NSVSS brought together approximately 260 invited stakeholders and federal observers on June 19-20, 2007, at the Marriott Crystal Gateway Hotel in Arlington, Virginia, to begin a dialogue and share one another's concerns about small vessel operations, safety, and security.

The objectives of the Summit were to:

- Educate small vessel stakeholders on security risks in the U.S. maritime domain.
- Provide a national forum for small vessel stakeholders to present and discuss their ideas on the development of security measures to mitigate gaps in small vessel management and control in the maritime domain.
- Provide a national forum for state and local government officials, as well as private members of the small vessel population, to discuss transportation concerns regarding security threats and present their ideas towards addressing those threats.
- Record all issues and concerns from the small vessel stakeholders, and complete an after-action report for public, industry, and government to support conclusions for national-level decisions involving the development of small vessel security measures to detect, deter, interdict, and defeat terrorist use of small vessels in the U.S. maritime domain.

To achieve these objectives, the NSVSS was designed to fully engage the various stakeholder communities in order to leverage their experience and record their ideas and concerns on maritime safety and security issues. Distinguished speakers and national experts first informed the attendees on maritime homeland security threats, initiatives, and concerns. The Summit program then turned to breakout sessions in which stakeholder working groups were presented maritime terrorist attack scenarios to stimulate and provide context for facilitated discussions of related issues focused on answering the question: "What could have been done to deter, defeat or mitigate the attack and its effects?" Each working group reported key points of their discussions in plenary sessions. Throughout the conference, stakeholders were encouraged to take full advantage of this forum to engage speakers, panel members, fellow stakeholders and facilitators in meaningful dialogue.

The following are summaries of the major findings derived from the small vessel stakeholder dialogue throughout the Summit. These findings are in no specific order of importance.

Need for a national strategy. A reoccurring theme throughout the Summit was the need for the development of a coherent National Small Vessel Security Strategy based on a layered-security approach. Attendees stressed that the strategy must be appropriate to the

threat and not overly intrude on personal liberties or cause undue economic burdens. Participants also advocated a multi-option strategy that addresses the unique characteristics of various ports, waterways or coastal areas rather than a "one size fits all" strategy. The sense was that stakeholders be given options that meet a recognized federal standard so that security measures could be implemented to best fit local circumstances and vulnerabilities in a flexible way to deal with changing threats and risks.

Stakeholder view of the small vessel threat. Among stakeholders there was general agreement that at the present time it would be relatively easy for a terrorist organization to acquire or commandeer a small vessel to conduct a terrorist attack against the United States. Overall, commercial vessels were viewed as less of a terrorism threat than pleasure craft as the recreational boating community was thought to be less regulated and more diffuse than the commercial vessel sector. Another major concern was that, depending on the target, terrorists would be more likely to acquire small vessels to be used in terrorist attacks from foreign countries in close proximity to the United States (i.e. Canada, Mexico or nations in the Caribbean).

Utilization of risk assessments to inform decision makers and resource allocation. In order for the proposed strategy to be credible to the stakeholders, who must be engaged as partners, the Department of Homeland Security (DHS) was urged to conduct and convey systematic threat and risk assessments on an ongoing basis. Three types of assessments were viewed by the stakeholder community as necessary: 1) further definition of the threat; 2) determination of the specific security needs; and 3) gauging of the threat to the country from small vessels acquired in foreign countries.

Balanced trade-offs between freedom, security, and economy. Balancing the need to increase security with individual freedoms and economic viability was a major theme at the NSVSS. Members of the recreational boating community indicated that restrictive regulations imposed by the federal government on boaters and other small vessel operators were strongly perceived as having little impact on improving national security and would likely alienate the very community from which assistance is essential. As expressed by one attendee, if government policies and regulations negatively impact economic growth and personal liberties, then the terrorists have won without even conducting an attack.

A culture of partnership and trust within and across the boating community. There was near universal consensus among stakeholders that they are eager to participate in the common security of the country and to work with DHS as well as state, local, tribal and territorial government entities as long as they are treated as "partners" and "allies" and not as "adversaries." Simply stated, the small vessel community wants to be acknowledged as part of the solution and not viewed as part of the problem.

Establish Funding Streams. There was broad agreement among all stakeholder groups that adequate funding and resources for the U.S. Coast Guard (USCG), USCG Auxiliary, state, local, tribal, and territorial boating law enforcement authorities, and emergency response elements are critical to ensure the security and safety of the nation's ports, waterways and coastal areas.

Training toward enhanced coordination, cooperation and communications between federal, state, local, tribal and territorial authorities. Stakeholders noted a variety of training issues related to enhanced coordination, cooperation and communications among federal, state, local, tribal and territorial authorities. Several members of the law enforcement community expressed that there is a lack of equipment for tactical operations and training in interdicting criminal maritime activities; most of the training conducted by state and local marine law enforcement is directed toward safety regulations and not the homeland security mission. Moreover, law enforcement authorities indicated that periodic training drills and exercises are desperately needed to address shortcomings in homeland security as well as response and preparedness in the maritime domain.

Improved intelligence collection, analysis and dissemination. There was widespread agreement among stakeholders that the timely acquisition of intelligence and the ability to act on it during the planning stages before an attack is one of the best ways to prevent a waterborne terrorist attack. To have a better opportunity to stop a terrorist attack in the planning stages, a broad spectrum of stakeholders called for developing fusion centers to better share, analyze and disseminate intelligence.

Expanded education and outreach to citizen stakeholders for a variety of safety, security and trust-building purposes. One of the principal themes expressed at the Summit was that the general boating public is not sufficiently aware of the threat that terrorist exploitation of small vessels poses to U.S. national security. It was felt that more must be done to encourage citizen participation and to distribute safety and security information to them. There was near total unanimity that the America's Waterway Watch (AWW) or a similar program should be expanded, reenergized and funded. The program should go beyond public awareness to include training and a community watch component.

Improved boater situational awareness. Attendees expressed positive interest in participating in programs to identify and report suspicious activities. Several participants believed that the commercial industry understood maritime security much better than recreational boaters; for example, there is currently no education for the boating public on Maritime Security (MARSEC) levels. Regardless of the educational campaign used to improve situational awareness, it must be sustained as new boaters use American waters every day.

Enhanced mechanisms to report suspicious activities. There was a general stakeholder agreement that there is a need to develop standardized reporting mechanisms and contacts to alleviate confusion as to who should be contacted during emergency situations or for reporting suspicious activities. Participants recommended that a universal number (National Terrorism Hotlines), similar to 911, a 1-800 number, or a *number, be adopted for reporting suspicious and terrorist activities. This number needs to be broadly disseminated and should be similar to decals currently placed on vessels to report pollution prevention to the National Response Center (NRC).

Domain Awareness Systems. There was considerable controversy over the role and status of the Automatic Identification System (AIS). Numerous recreational boating

representatives were unequivocally opposed to applying AIS requirements to those vessels. Those stakeholders insisted that AIS should not be expanded for use beyond commercial boats because it is too costly and impractical for recreational vessels. Moreover, they felt that a requirement to have AIS on small vessels would have a minimal effect on security because attempting to identify every vessel would be too expensive and difficult to monitor with current resources as well as easily compromised by terrorists. The commercial industry expressed serious reservations about the cost of AIS. While acknowledging that AIS might be good for vessel identification, multiple stakeholders downplayed the role AIS would play in preventing an attack as terrorists would not comply with any requirement to install AIS or would disable it before an attack. However, some stakeholders did see limited application for AIS or similar technology in the vicinity of high value/high risk assets within limited geographic bounds in a port or waterway. The Vessel Identification System (VIS), Radio Frequency Identification (RFID) technologies and other systems were also mentioned as potential low cost solutions that might be an acceptable alternative to vessel tracking.

Operator and vessel identification. A diversity of views within and across stakeholder communities were expressed in regards to operator certification, licensing, and vessel registration.

Certification. Many stakeholders from the commercial vessel sector were not opposed to credentialing but were concerned that inconsistent credentialing regimes in different jurisdictions around the country resulted in inappropriate requirements and undue inconvenience for vessel operators. Other stakeholders argued that the government should not continue to impose burdensome requirements on mariners or companies without demonstrating the benefits of these new programs.

Licensing. The issue of licensing was contentious. Many stakeholders and panelists from the recreational boating community expressed the view that licensing is too expensive, is an intrusion on their personal liberties, and is ineffective in preventing terrorist attacks. They stressed that boaters should not have to procure any new type of identification or be treated any differently than automobile drivers or airline passengers. Other stakeholders suggested that requiring identification for recreational boat operators might be acceptable as long as it was an existing driver's license or other identification accepted by the Transportation Security Administration (TSA) rather than yet another identification card.

Vessel Registration. Vessel registration was another controversial topic. Several government attendees advocated the development of a nationwide database of U.S. numbered and documented vessels to be used by federal, state, and local law enforcement authorities to access boat registration information across the country. They also expressed a need to have uniform boating registration standards shared by all states. Other attendees did not support the concept of a national small vessel registry. They stated that such a database likely would not make the nation more secure because a terrorist bent on conducting an attack would not bother to register a vessel or would acquire a registered vessel by illicit means.

International cooperation. There was widespread consensus that a strong regime of international agreements and cooperation is needed to defeat threats before they reach

U.S. waters. Stakeholders indicated that it is important to work with other countries - particularly with countries in close proximity to the United States (i.e., Canada, Mexico and nations in the Caribbean) - to encourage them to deploy security systems, share intelligence information, and check vessels for weapons and people of interest before they depart for the United States.

Technologies and operational procedures to detect radiological and nuclear threats. There was widespread consensus to use radiation detectors, but concerns were raised about device technical and operational effectiveness. Several stakeholders mentioned that the detection of radiological materials overseas and their interdiction is the single most important issue facing federal law enforcement agencies. Some stakeholders also recommended that state and local law enforcement agencies and other first responders be provided with nuclear detection devices to inspect both vessels and cargo containers. A number of operators volunteered to place detectors on their vessels to help prevent an attack using Weapons of Mass Destruction (WMD).

Reassessment of Security Zones. There were divergent views among stakeholders as to whether or not security zones around vessels, ports, and other critical infrastructure are an effective means of protecting key facilities. According to several stakeholders, security zones should be charted, clearly marked with markers and buoys and patrolled to make waterside targets less attractive to attack. Multiple members of the recreational boating community also supported the expansion of security zones as this is one area of security that recreational boaters are familiar with. Regardless of the above mentioned stakeholder views on security zones, there was broad agreement that any increase in security zones would also require a corresponding increase in security personnel to patrol those areas.

Summary of Recommendations:

- DHS needs to develop a coherent National Small Vessel Security Strategy based on a layered security approach.
- DHS should not impose overly restrictive regulatory constraints on small vessel operators or their boats in the areas of licensing, registration, or tracking.
- DHS needs to conduct and convey threat and risk assessments on a continuing basis in order to: 1) define the nature of the threat; 2) determine port specific security needs; and 3) clarify the small vessel threat from foreign countries.
- DHS needs to take immediate steps to engage the small vessel stakeholder community and ensure their continual engagement, by keeping them informed on issues of safety and security.
- Funding is needed to support state, local, tribal, and territorial maritime law enforcement entities.
- Law enforcement training deficiencies need to be addressed to meet a variety of safety and security objectives.
- A universal hotline telephone number needs to be developed and disseminated so that the boating community can report both suspicious activities and emergency situations.

- At this time it is not recommended that AIS technologies be required for vessels under 65 feet in length until the technology is perfected, cost significantly reduced, or until law enforcement has the ability to track and respond to all vessels being tracked in their area of responsibility.
- Research into alternative technologies similar to but less expensive than AIS need to be conducted in order to evaluate the usefulness of such technologies in balancing cost with effectiveness in maintaining maritime domain awareness.
- More must be done to streamline credentialing to ensure that various jurisdictions accept the same standards, including solutions such as adding a boat operator endorsement to state driver licenses.
- A national boat registry should be created so that it can be indexed and searched by federal, state, local, tribal, and territorial law enforcement agencies.
- The federal government needs to enhance international cooperation and intelligence sharing with our foreign counterparts especially with those countries in close proximity to the United States.
- To help prevent a radiological or nuclear attack, state, local, tribal, and territorial law enforcement agencies need to be provided with radiological detection devices.
- The federal government should develop radiological and nuclear detection devices with a stand-off capability in order to provide detection with minimal impact on small vessel stakeholder operations.
- The federal government should strengthen counter-proliferation initiatives with our foreign counterparts to prevent shipments of WMD, their delivery systems, or related materials from ever taking place.

Conclusion: In summary, the findings of the stakeholders at the Summit guided the recommendations found in this report. These recommendations reflect opportunities for federal, state, local, and tribal governments in partnership with the small vessel community to better protect the nation from terrorist attacks via small vessels. Some of these recommendations are easily implemented and have broad appeal whereas others are more difficult to put into practice due to privacy, economic, and other concerns. Regardless of the level of difficulty, all of the recommendations found within this report have potentially high payoffs and could greatly increase the safety and security of the U.S. maritime domain.

I. INTRODUCTION

America's waterways are avenues for a vast range of commercial and recreational pursuits. They are the nation's largest borders and have an important place in our thinking about homeland security, as the ports, waterways, and coastal areas provide strong measures of value, pleasure, and vulnerability. Thus, national policy and a broad range of public and private sector interests are integral parts of the nation's strategy of "layered security" in the face of hostile intent.

Since the earliest days of the United States, and at an accelerated pace since the attacks of 9/11, measures have been taken to protect our nation's waterways, to make them as safe and secure as possible while simultaneously protecting our citizen's enjoyment of their maritime heritage. Today, the Department of Homeland Security (DHS) is charged with extending that protection by considering potential threats that could be conveyed by vessels of under 300 tons (small vessels) and developing methods to mitigate these risks.

The USCGC BOUTWELL (Coast Guard photo by Petty Officer Jonathan R. Cilley)

Small vessel operators represent the largest number of stakeholders directly involved in this issue, as there are over 70 million Americans who participate in some form of recreational boating across the country.[1] The large number of small vessels, the wide variation in designs and uses, and the freedom of the environment in which they operate raise complex issues for incorporating vessels and their operators into the overall strategy of layered security. Indeed, these very qualities are a key issue which makes small vessels vulnerable to being exploited by terrorists intent on attacking the United States.

[1] According to the National Marine Manufacturers Association (NMMA) estimated boating participation in 2005 was 71.3 million.

Terrorists have demonstrated their interest in and ability to use transportation assets, including small vessels, to achieve their destructive aims. In the aftermath of the 9/11 attacks, the earlier attack on the USS COLE, and other maritime attacks around the world, the threat has clearly been demonstrated. Terrorist groups and their supporters could also use small vessels to transport dangerous people and materials, including WMD into the United States. The challenge of ensuring maritime security is exacerbated by the limited authorities and capabilities available for identifying threatening small vessels and their operators in a timely manner.

Concern that small vessels could be exploited by terrorists to attack the U.S. homeland was the compelling reason for bringing together small vessel stakeholders. Minimizing the risk of terrorist activities involving small vessels requires a strong partnership among the diverse elements of the small vessel community, DHS and its operating components. The NSVSS thus sought to initiate a dialogue among stakeholders on how to reduce the threat of terrorists using small vessels to harm the nation.[2]

Nature of the Threat

Small vessels offer terrorists potential advantages as a means to smuggle dangerous persons and weapons into the United States, or to deliver an attack against important targets found in or along U.S. waters. These advantages include:

- An extensive population of largely unregulated small vessels, which can be operated by people with minimal training;
- Broad, unfettered access to high-value targets located in coastal population centers;
- Routine operation in proximity to high-value maritime ships and infrastructure;
- A complex maritime environment with overlapping jurisdictions, constraining effective law enforcement over large open ocean spaces, waterways, and coastlines;
- Limited existing capabilities for identifying and monitoring small vessel operations including a lack of access to hull identification and registration data by law enforcement personnel, as well as limited credentialing of small vessel operators;
- Limited ability to screen small vessels for weapons of mass destruction and a relatively weak notification and enforcement process for small vessels arriving from abroad; and
- Limited oversight for vessels under 300 gross tons, which operate below the requirements of the Maritime Transportation Security Act (MTSA) of 2002 or

[2] For the purposes of this Summit, a small vessel was characterized as any watercraft, regardless of method of propulsion, which is generally less than 300 gross tons, and used for recreational or commercial purposes. Small vessels include commercial fishing vessels, recreational boats and yachts, towing vessels, or any other small commercial vessels involved in foreign or U.S. voyages.

international agreements such as the International Maritime Organization (IMO) *International Ship and Port Facility Security* (ISPS) Code, without safety and security regimes such as standard practices found in the general aviation sector for small aircraft.

The risk of terrorist exploitation of small vessels as a threat vector takes multiple forms:

- *WMD transport*: Possible terrorist use of small vessels to transport or deliver weapons of mass destruction.
- *Conventional explosives delivery platform*: Terrorist groups have demonstrated a clear interest and ability to use small vessels to deliver waterborne improvised explosive devices (WBIED) in attacks against larger ships, as was the case in the attack on the USS COLE in 2000.
- *Smuggling people and material:* Terrorists and criminal organizations might exploit small vessels to smuggle dangerous people and materials into the United States.
- *Platform for weapon attack:* Terrorists could use small vessels as platforms for standoff weapon (e.g., Man-Portable Air Defense Systems [MANPADS] or surface-to-surface missile platforms) attacks.

Despite these significant concerns, substantial uncertainty surrounds how terrorists might use small vessels. First, the terrorist threat is very dynamic as terrorist groups are a "thinking enemy," always evolving and adapting to their environment. Second, terrorists have substantial flexibility in choosing targets and attack methods; they are likely to be opportunistic in taking advantage of vulnerabilities. Finally, they can have varying objectives. For example, they could seek to inflict incredible and sustained economic damage against the U.S. economy or they could settle for a more limited attack on a specific maritime target of opportunity to achieve a major psychological impact by demonstrating the continuing vulnerability of the U.S. public.

Since 2001, a major national effort has been made towards enhancing maritime security in order to reduce the risk that terrorist threats involving maritime assets could present to the United States and other countries. However, most of the security measures and procedures have focused on securing the broader maritime transportation system, particularly larger commercial vessels, from terrorist threats and exploitation. To supplement these efforts, a robust national small vessel maritime strategy, based on a layered security approach over the entire domain, is needed to further prevent terrorist attacks and improve safety and security. Such a strategy will provide additional layered defenses by protecting vital infrastructure and assets; assist in managing, regulating, and controlling vessels and individuals within the maritime domain; and push the terrorist threat out as far as possible, increasing the likelihood of successful intervention.

To improve maritime safety, security and stewardship, a combined and sustained effort is needed from the federal, state, local and tribal government, the private sector, the general public, and our international partners. The overriding question is how to improve maritime security for small vessels without applying measures that are unfeasible, overly expensive, or inappropriate for the operation of smaller vessels. *Thus, the key in devising*

and implementing a national small vessel maritime strategy is that it must balance security concerns with personal freedoms and liberties and the economic realities of the small vessel community.

Summit Purpose

The purpose of the National Small Vessel Security Summit (NSVSS) was to engage private, commercial and government stakeholders in discussions on a range of issues involving the small vessel security risk in the U.S. maritime domain. The NSVSS brought together approximately 260 invited stakeholders and federal observers on June 19-20, 2007, at the Marriott Crystal Gateway Hotel in Arlington, Virginia to begin a dialogue and share one another's concerns about small vessel operations, safety and security in the post-9/11 world with its ever-present terrorist threat.

United States Coast Guard Rear Admiral Brian Salerno addresses stakeholders at the Summit.

Summit Scope

The scope of the Summit was to focus the maritime stakeholders on a range of discussions and problems involving the small vessel security risk in the U.S. maritime domain. Defining the terms "small vessel" and "security risk" were two of the essential starting points that bound the scope of the conference. For the purposes of the Summit, a small vessel was characterized as any watercraft, regardless of method of propulsion, generally less then 300 gross tons, and used for recreational or commercial purposes. Small vessels include commercial fishing vessels, recreational boats and yachts, towing vessels, uninspected passenger vessels, or any other small commercial vessels involved in foreign or U.S. voyages. This characterization distinguishes small vessels from large

commercial vessels and yachts (generally 300 gross tons and over) for which security measures are already in place under the authority of the Maritime Transportation Security Act (MTSA) of 2002 and the International Ship and Port Facility Security (ISPS) Code.

Leading into the Summit, small vessel security threats were broken down into four general categories:

- Use of small vessels as a conveyance for smuggling weapons (including, but not limited to WMD);
- Use of vessels as WBIEDs – small, explosive laden vessels used as "boat bombs" against another vessel, critical maritime infrastructure, or key resources;
- Use of small vessels as a conveyance to smuggle terrorists into the U.S.; and
- Use of small vessels as a platform for standoff weapon (e.g., MANPADS or surface-to-surface missile platform) attacks.

Summit Objectives

The objectives of the Summit were to:

- *Educate small vessel stakeholders* of the security risks in the U.S. maritime domain.
- *Provide a national forum for small vessel stakeholders* to discuss and present their ideas on the development of security measures to mitigate gaps in small vessel management and control in the maritime domain.
- *Provide a national forum for state and local government officials, as well as private members* of the small vessel population to discuss transportation concerns regarding security threats and present their ideas.
- *Record all issues and concerns from the small vessel stakeholders* and complete an after action report for use by the public, industry, and government officials to support national decisions involving the development of small vessel security measures to detect, deter, interdict, and defeat terrorists using small vessels in the U.S. maritime domain.

To meet these objectives, the Summit began with plenary addresses by distinguished federal homeland security officials. These presenters addressed the small vessel terrorist threat and discussed measures currently being taken and those being considered in managing maritime risks. These informative speeches were followed by panel discussions among representatives of state and local law enforcement, the commercial small vessel industry, and the recreational boating community who expressed their interest and concerns in addressing the terrorist threat from small vessels. These thoughts and ideas presented were then brought forth in facilitated discussion working groups. To provide context for the working group discussions and draw out the maritime subject matter expertise of the Summit participants, a scenario-based approach was used to elicit stakeholder knowledge in identifying small vessel threats, and arriving at solutions to deter, detect, prevent, and mitigate terrorist maritime attacks.

Report Purpose

This report summarizes the proceedings of the NSVSS, forming a record of the discussions (in a neutral, non-attribution format) to serve as the starting point of an ongoing, unprecedented partnership by DHS and the private sector to address homeland security issues. It describes the Summit, defines the nature of the small vessel threat, describes the scenario development process, summarizes stakeholder feedback, and provides recommendations for DHS policy makers to better secure the U.S. maritime domain from terrorist attacks.

II. ISSUES

Threats

Terrorists have demonstrated their intention to use small vessels to harm U.S. interests. For example, on October 12, 2000, the USS COLE was attacked by al-Qaida suicide bombers using a small vessel loaded with explosives while she was harbored in the Yemeni port of Aden. The resulting explosion killed 17 sailors and injured 39 others.

Whenever an adversary has the capability to do us harm and has indicated an intention to do so, that constitutes a threat. Radical Islamic terrorist organizations have the capability to integrate small vessels into attacks, use small vessels for the transport of weapons, and/or use small vessels for activities in support of an attack. Those activities include surveillance, movement of people and material, and testing or probing our vulnerabilities and defenses.

MAYPORT, Fla. (Jan. 17)--A crew from Coast Guard Station Mayport escort the U.S. naval ship O'Bannon back to the Mayport naval Station Thursday afternoon. Boaters are required to keep 500 yards from any U.S. Naval ship as it moves through the water. The O'Bannon spent a few months in the Atlantic dry-docks in Mayport, Fla. (USCG photo by PA3 Dana Warr)

The U.S. and the world face very different challenges and threats today than those faced by previous generations. Key among them is the expansion of transnational threats. Transnational criminals, pirates, and terrorists seek to exploit the complexity of the modern maritime domain and the vulnerabilities of the global supply system. Weapons of mass destruction, contraband smuggling, and small vessel threats, such as WBIEDs, represent grave risks. Moreover, today's trafficking of drugs, migrants, and contraband by criminals has become increasingly sophisticated and threatening.

The vastness, anonymity, and limited governance of the global maritime domain further complicate the situation. The maritime domain, by its nature, creates its own challenges. Legitimate uses and criminal threats are growing in a realm that spans the globe, with

limited governance, providing almost no transparency of activity—particularly with respect to small vessels.[3]

The gravest maritime threat facing the nation is the potential for a terrorist group to obtain a nuclear weapon or other WMD, whether for use near or within the confines of a major U.S. port city or subsequent delivery to another target. While much attention has been focused on WMD detection in maritime containers, it is equally plausible that such a device, or the fissile material for such a device, would be loaded onboard a bulk freighter, a fishing boat, or a recreational boat that allows continuous control by possession of the device by a terrorist group. Many of these vessels operate under minimal regimes and control protocols, making their movements virtually anonymous to authorities. The catastrophic impacts of a terrorist attack launched within dense urban areas, makes maritime delivery or conveyance a particularly lethal threat.[4]

Moreover, the use of a small vessel as a platform for conducting a stand-off attack cannot be discounted. In August 2005, terrorists fired rockets at two U.S. warships docked in Aqaba, Jordan. While in that case the platform was a local warehouse, pirates have also used small vessels as a platform for stand-off attacks. In November 2005, a cruise liner was attacked by two 25-foot rigid hull inflatable boats 100 miles off the coast of Somalia. The pirates used rocket-propelled grenades and automatic weapons, and were repelled by the crew of the passenger vessel M/V SEABOURN SPIRIT using a sonic blast, and by increasing to full speed and outrunning the pirates.[5]

For more than two centuries, oceans have served to insulate America from many threats. They have served as a buffer, giving time to identify and deter an attack. But in today's environment, we are faced with a new reality. The oceans may be the avenues by which terrorists or others who mean to do us harm deliver devastating attacks against our ports, cities, economy and other national interests.

Vulnerabilities

Adversaries who have the capability to harm the United States may do so by exploiting our vulnerabilities, leveraging our weak spots towards their goals. All societies have vulnerabilities, and in free, open societies, such as the United States, there may be more vulnerabilities than in other nation states.

Consider these factors with regard to vulnerabilities in the maritime sector:

- *"Just-in-time"* delivery. The majority of freight moving by sea is shipped for "just-in-time" delivery - a means of reducing inventories and lowering operating costs through business efficiencies. Industries and retailers do not store supplies or products they will use or sell; rather, they schedule – and expect - the arrival

[3] *The U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship*, United States Coast Guard, January 19, 2007, Washington, DC, p. 5.

[4] Ibid., p. 24.

[5] At the time of the attack the M/V SEABOURN SPIRIT had approximately 150 passengers onboard. Only one passenger suffered minor injuries during the attack.

of shipments "just in time" to fill needs. As a result, the maritime transportation system operates within tight tolerances and has limited ability to deal with disruptions.

- *Mega-ports*. Out of 326 ports nationwide, just ten handle 85 percent of all ship-borne containerized cargo.[6] Disruption to one of these mega-ports would have serious economic consequences to the whole U.S. transportation system capability.
- *Economic impacts.* By one estimate, the cost to the U.S. economy from port closures on the West Coast due to a labor/management dispute in 2003 was approximately $1 billion per day for the first five days, rising sharply thereafter.[7] Ripple effects to the economies of U.S. trading partners resulted in similarly profound economic impacts.
- *Increased coastal density*. America's coastal population density is five times greater than the country as a whole, and the number of coastal residents could increase by another 21 million by 2015.[8] With that trend comes increasing vulnerability; a catastrophic maritime incident could impact large numbers of people and critical infrastructure.
- *Mega-ships*. The enormous growth in capacity of cruise liners, tankers, and container ships exemplifies the broader challenges created by the enormous vessels now used in the maritime industry. New ocean liners are 18 decks high, span the lengths of three football fields, and can carry nearly 6,000 people. Ultra-large crude oil carriers are approaching 1,500 feet in length and 300-foot widths. Today's largest container ship, the M/V EMMA MAERSK, carries 15,000 Twenty-foot Equivalent Units (TEUs) of containers. A catastrophic incident on one of these ships would test the nation's capacity for response and rescue at sea as well as have significant economic and environmental impact.

Could terrorists exploit any of these factors to harm the United States? Consider what has happened already. The ACHILLE LAURO hijacking; the attack on the M/V SEABOURN SPIRIT; the emergence of the Tamil "SeaTigers" in Sri Lanka; the al-Qaida-inspired attacks against the USS COLE and the M/V LIMBURG; and the terrorist bombing and sinking of the SUPERFERRY 14 in the Philippines; all show that maritime attacks are an established means for terrorists to achieve the psychological impacts they seek.

---

[6] U.S. Commission on Ocean Policy, *An Ocean Blueprint for the 21st Century*, Washington, DC: 2004, p. 193.

[7] Peter Chalk, "Maritime Terrorism in the Contemporary Era: Threat and Potential Future Contingencies," *The MIPT Terrorism Annual 2006,* p. 25.

[8] U.S. Commission on Ocean Policy, *An Ocean Blueprint for the 21st Century*, Washington, DC: 2004, p. 41.

Consequences

The U.S. Exclusive Economic Zone covers 3.4 million square nautical miles of ocean territory and is among the most valuable and productive natural resources on Earth. In 2000, offshore activities contributed more than $117 billion and two million jobs to American prosperity. The overall economic activity of the coastal areas totaled over $1 trillion, creating one-tenth of the nation's annual gross domestic product. About 30 percent of the nation's oil supplies and 25 percent of its natural gas supplies are produced from offshore areas.[9] U.S. fish stocks are harvested by recreational and commercial fishermen in a $48 billion industry.[10] These are just a few examples of the ways in which the United States is dependent upon the sea.

As described previously, the gravest maritime threat facing the nation is the potential for a terrorist group to obtain a nuclear weapon or other type of WMD and detonate it within the confines of a major U.S. port city. The consequences of such an attack would be catastrophic.

What are these potential consequences? In one scenario used by the U.S. Government, detonation of a ten kiloton weapon (slightly smaller than the Hiroshima or Nagasaki atomic bombs) near a city center could claim up to a quarter million lives and injure another 100,000.[11] The economic cost would be in the hundreds of billions of dollars, and the radioactive debris might restrict the use of the area for years, if not decades.

Other threats, such as chemical weapons, biological weapons, and conventional explosives also may have similar consequences.

Sometimes, there are secondary and tertiary effects from an event. For example, following Hurricanes Katrina and Rita, large populations moved away from the Gulf Coast—particularly New Orleans—and have stayed away creating a secondary impact. The permanent loss of population has further harmed the Gulf Coast's economy as a tertiary consequence of the hurricanes. One can imagine – with the loss of life and casualties, devastation to infrastructure and radioactive fallout – an attack with a nuclear device would have multifold regional and national consequences.

Cascading effects are consequences caused when one event triggers another. For example, a flood could cause a loss of petrochemical pipeline pumps which could result in a lack of petroleum products throughout a broad geographic area.[12]

---

[9] Ibid., p. 18.

[10] Scott Borgerson, "Breaking the Ice Up North," *The New York Times*, October 20, 2005, accessed from http://www.nytimes.com/2005/10/19/opinion/19borgerson.html?ex=1177560000&en=7ee8ddfc7e66ff21&ei=5070 on April 24, 2007.

[11] These figures were taken from the DHS National Planning Scenario briefing in April 2006.

[12] In fact, this exact consequence of cascading effects was one of the results of Hurricane Katrina's strike on the Gulf Coast in 2005.

In the maritime domain secondary and tertiary consequences, as well as cascading of events, are highly probable. Consider the long-term impact on fishing, charter boats, tourism, and the shipping and commerce industries from a large-scale terrorist attack along the coast line or in one of our ports. For example, while standards for construction and operation of oil tankers have improved dramatically since the EXXON VALDEZ oil spill, the world must now be more aware terrorists could hijack and use a tanker as a weapon to intentionally spill millions of gallons of oil.[13] From a small vessel perspective – terrorists could conceivably achieve similar results simply by detonating a WBIED alongside a tanker. If the oil spill were to catch fire as a result of the attack it could burn for several days causing serious environmental and economic damage.

It is difficult to estimate the consequences of a harmful event directed from, or aimed at, our maritime environment even with historic events to draw upon. The secondary and tertiary effects and possible cascade of events that could follow are dependent upon many different variables. However, one thing is certain; those who work and recreate on our waters would be affected. It is not difficult to imagine scenarios in which a terrorist attack harms the ocean, the rivers, or the coastal zone. The subsequent economic impacts for the nation would be significant.

Risk

The three preceding sections have described the threat, vulnerabilities, and possible consequences. The concept of "risk" integrates these three elements allowing us to prioritize and anticipate.

There are multiple ways to express risk. Some methodologies are complex, while others may be applied more easily. At its most basic, risk may be expressed as:

$$Risk = Threat \times Vulnerability \times Consequence$$[14]

Threat is the likelihood of an attack occurring. Capability and intent are hallmarks of threats. When considering terrorism, an enemy must have both the capability and the intention of doing us harm to be categorized as a threat. Al-Qaida has demonstrated both repeatedly.

Vulnerability is our relative exposure. For example, could an enemy use a small vessel to sink a large vessel, thus blocking a channel? Or could an enemy transit from overseas undetected, blend into our domestic maritime traffic, and detonate a weapon in one of our ports?

---

[13] Scott Borgerson, "Breaking the Ice Up North," *The New York Times*, October 20, 2005, accessed from http://www.nytimes.com/2005/10/19/opinion/19borgerson.html?ex=1177560000&en=7ee8ddfc7e66ff21&ei=5070 on April 24, 2007.

[14] Todd Masse, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues and Options for Congress*, Washington, DC: Congressional Research Service, February 2, 2007.

Consequence is the expected impact of an attack. Much has been written on the economic impact to the nation of an attack on one of our ports. What has not been discussed in great detail is the impact of an attack on our maritime industries and on the lives and livelihood of those involved in the maritime sector.

DHS strives continuously to improve the methodology for calculating risk. Because this methodology influences how funds are allocated, it has been subject to rapid evolution as better approaches are defined. The Department has implemented a variety of systems to methodically assess each of these components of risk so that it can allocate resources appropriately; but this is a complex and challenging problem. While these methodologies attempt to produce qualitative and quantitative results, the unique characteristics of the maritime domain inject significant variance into the process.

The broad risks and the complexity of the global maritime environment led the President to issue the *National Strategy for Maritime Security (NSMS)* in September 2005.[15] Some of the key points of the NSMS include:

- Terrorist groups have used shipping as a means of conveyance for positioning their agents, providing logistical support, and generating revenue.
- Terrorists have taken advantage of criminal smuggling networks to circumvent border security measures.
- Terrorists have indicated a strong desire to use WMD.
- Terrorists can develop effective attack capabilities quickly using a variety of platforms, including:
  - Explosives-laden suicide boats;
  - Use of a vessel, itself as a weapon; and
  - Small vessels as platforms for launching an attack.
- Vessels can be used to transport conventional explosives or WMD for detonation in a port alongside an offshore facility. Terrorists could also take advantage of a vessel's legitimate cargo, such as chemicals, petroleum, or liquefied natural gas, as the explosive component of an attack.

Simply stated, there is an enemy who has the capability and intention of doing harm to the United States, our maritime assets are vulnerable, and the consequences would be grave. Could this enemy use a small vessel for an attack? Weapons of mass destruction do not occupy much space and could be carried in small vessels. A WBIED can be very small. Given that, this Summit sought to engage stakeholders about ways to understand risk by focusing on threats, vulnerabilities, and consequences.

[15] "The Role of the Coast Guard in Border Security, Statement of VADM Thad Allen, Chief of Staff, Before the Committee on Appropriations, Subcommittee on Homeland Security, U.S. Senate," Department of Homeland Security—U.S. Coast Guard, April 6, 2006, p. 4.

Operational Considerations

Terrorist organizations have demonstrated through their actions such as previous attacks that there are specific characteristics they seek when identifying a target. These characteristics include: the potential for multiple casualties, the effect on the economic base of the target nation, the symbolic or iconic nature of the targeted infrastructure, the potential of the attack to create fear throughout the populace, the ability to impact citizens' daily lives, and the probability of success.[16]

Studies have demonstrated a specific "chain of events" which normally leads up to an attack. Researchers have provided variation on the chain, but among those various versions there are some steps that are consistent. Assuming the adversary has a trained and capable team, an attack would likely include these steps:

- Detailed planning;
- Surveillance and intelligence collection against the intended target;
- Acquisition of the weapon (e.g., a conventional explosive or a Radiological Dispersal Device [RDD]);
- Acquisition of the delivery platform (e.g., a small vessel);
- Mating of the weapon to the platform;
- Transiting to the U.S. without raising suspicion (which may be accomplished well in advance of even the planning stage);
- Conducting of rehearsals or "dry runs;" and
- Executing the attack (e.g., transiting to the target and then detonating the weapon).[17]

Each of these steps has component steps. For example, "transiting to the target" can include approaching close enough to the target for the particular weapon onboard the vessel to be effective.

One common theme across all component steps is that the adversary must avoid detection and interception.

In the chain of events leading up to the attack, there exist multiple opportunities which can potentially be leveraged to thwart the terrorists plans. Opportunities for detection and interception heighten terrorist's risk of exposure. Understanding these opportunities enables security personnel to better target those weaknesses.

- *New boat owners.* Terrorists can acquire a boat via theft, rental, or purchase.

---

[16] *Small Boat Threat Information Paper*, Sector Seattle Boat Attack Working Group, September 15, 2006, p. 1.

[17] LT Matthew Michaelis, "Defending Against a Small Vessel WMD Attack," SIS 425/590, Winter Quarter, December 12, 2006.

- *Repeated visits.* Detailed planning may involve repeated visits to the same target or multiple alternative targets to observe daily operations and typical security measures.[18]
- *Security assessment.* Terrorists may frequently photograph and/or keep written records of security measures and monitor enforcement agency patrols to ascertain routine habits and tactics and to identify vulnerabilities.
- *Rehearsals and dry runs.* Activities such as maneuvering boats alongside the target, e.g., alongside cruise ship berths or close to terminals as ferries load and unload passengers, are often employed to develop plans and event sequences for the final operation.
- *Probing.* Rehearsals and dry runs, in addition to gathering operational information, can also be used to test the reaction of security personnel.
- *Hidden preparation sites.* Terrorists need hidden locations for preparation. For example, in case of a WBIED, terrorists would need a site to build the device and place it on a small vessel. Such a site may not even be on the water, if the delivery platform is a small vessel capable of being towed by a vehicle.
- *Load.* A large amount of explosives is required for an attack on a large vessel.[19] If the vessel is carrying a large amount of explosives, it may ride low in the water rendering it more readily noticeable. Moreover, operational considerations (e.g., rapid loading of the vessel) may lead terrorists to store some or all the explosives on deck under concealment.
- *Swarm.* Terrorists may achieve the combined effect of large explosives by swarming a target with multiple attackers. Movement, particularly rehearsals, by groups of vessels may be evident to local boaters, commercial operators, and law enforcement/security personnel.
- *Periods of vulnerability.* Potential targets may be most vulnerable to boat attack while moored at a pier, anchored, while approaching or departing a pier, while transiting in restricted waterways, or during large marine events.

Although the examples provided above are varied, they highlight the likelihood that terrorists planning to use a vessel in an attack will conduct activities prior to and during the attack that are anomalous, setting the terrorists apart from the rest of the maritime community. If these actions can be detected, an attack may be avoided or defeated.

---

[18] A recent example of would be terrorists repeatedly visiting a target was the arrest of six radical Islamic men on May 8, 2007, for allegedly plotting to attack the Fort Dix military base in New Jersey. According to the indictment against these men, they conducted firearms training in the Poconos, trained with paintball guns, and scouted several military facilities for an attack, including Fort Monmouth in New Jersey, Dover Air Force Base in Delaware, the U.S. Coast Guard building in Philadelphia and other targets. One of the members of this group, Serdar Tatar, alleged knew the layout of Fort Dix "like the palm of his hand" after making numerous pizza deliveries to the base.

[19] By way of example, various sources estimate that between 600 and 1,000 pounds of C4 explosives were used in the October 2000 attack on the USS COLE in Aden, Yemen.

Maritime Vulnerabilities in Historical Perspective

Several historical maritime tragedies have resulted in the deaths of hundreds of innocent civilians, impacted the lives of thousands more, and caused multi-million dollar damages. Some were deliberate acts of sabotage whereas others were accidents. Regardless of the cause, these events illustrate the danger posed by small vessels and portray what could conceivably happen if a terrorist organization were to detonate a large conventional explosive on a maritime vessel near a major port, population center, or critical infrastructure.

Black Tom Island

During World War I, Black Tom Island in New York Harbor was a major munitions depot for explosives destined for the Allied Powers to be used against the Central Powers. Although the depot was used to load high explosives onto vessels, the facility was not securely gated to "safeguard the nearby civilian population from the potential for foul play."[20]

On July 30, 1916, several fires were deliberately set by German saboteurs at the depot to prevent deliveries from being made to the Allies. On the evening of the attack, barges and freight cars at the depot were reportedly filled with over two million pounds of ammunition. The fires set off a series of explosions causing damage to the Statue of Liberty and buildings over a mile away. According to some accounts, the explosions on the island were so powerful that they registered over 5.0 on the Richter Scale. Windows were blown out of every building in lower Manhattan and shock waves were felt over 90 miles away.

The Black Tom depot with its freight cars, warehouses, barges, tugboats and piers was totally destroyed. Property damage from the attack was estimated at nearly $20 million dollars (approximately $365 million dollars today).[21] The Statue of Liberty alone sustained an estimated $100,000 thousand dollars in damage to its skirt and torch. The Statue was damaged so extensively that, to this day, tourists are not allowed in the torch section of the monument due to structural instability.

Reports on the number of victims vary but as many as seven people were killed and those injured numbered in the hundreds. Newly arriving immigrants at Ellis Island had to be evacuated as smaller explosions continued to occur hours after the initial blast. Some 500 people living on houseboats and barges in the harbor also had to be evacuated.

In the aftermath of the attack, the Lehigh Valley Railroad Company, which owned the island, and other claimants sued the government of Germany for damages under the 1921 Treaty of Berlin through the German-American Mixed Claims Commission. In 1939,

[20] http://www.njcu.edu/programs/jchistory/Pages/B_Pages/Black_Tom_Explosion.htm

[21] Ibid.

after seventeen years of deliberation, the commission ruled that Germany had been responsible for the attack and ordered it to pay $50 million damages to the company.[22]

This sabotage at Black Tom Island was one of the primary drivers of the passage of the Espionage Act of 1917. Now codified in Title 50 of the U.S. Code, this legislation provides the original statutory underpinnings for vetting workers at regulated waterfront facilities and other activities.[23]

Halifax, Nova Scotia

On December 6, 1917, the French cargo ship SS MONT BLANC exploded while carrying munitions in the Halifax harbor. The blast leveled approximately two square kilometers of the city of Halifax, killed almost 2,000 individuals, and injured and displaced thousands more. This tragedy serves to illustrate that a similar loss of life and property could occur in the United States if a terrorist organization were to detonate an explosive device off one of the nation's seaports or next to a vessel filled with passengers like an ocean liner.

On the date of the explosion the MONT BLANC was loaded with 2,300 tons of picric acid, 200 tons of TNT, 10 tons of gun cotton and 35 tons of benzol.[24] At 8:40 am the Norwegian vessel SS IMO collided with the MONT BLANC. Although the collision was not severe, fire broke out on the MONT BLANC and the crew abandoned ship to flee the impending explosion. The collision and resulting fire drew crowds of onlookers who were unaware of the danger. Twenty-five minutes later the MONT BLANC exploded, immediately killing 1,600 individuals. In all, 1,630 homes were destroyed and another 12,000 damaged; 6,000 individuals were left without shelter.[25] The explosion was the largest man-made blast in history, a distinction it held until the first atomic bomb was detonated in 1945. The MONT BLANC blast remains the largest non-nuclear accidental explosion in history.[26]

The Texas City Disaster

A similar incident to the explosion of the MONT BLANC occurred in 1947 in Texas City, Texas. On the morning of April 16, 1947, the French liberty ship SS GRANDCAMP was being loaded with tons of ammonium nitrate destined for Europe when it caught fire. Perhaps unaware of the danger, members of the volunteer fire

---

[22] Black Tom was only one of a number of homeland attacks in retaliation for the British naval blockade of Germany during WWI. In New Jersey, on January 1, 1915, a fire was set at the Roebling Steel foundry in Trenton. After the Black Tom incident, on January 11, 1917, another fire took place at the Canadian Car and Foundry plant in Kingsland. These facilities had contracts for goods being sent to the Allied forces in Europe, resulting in their being targeted by the Central Powers. http://www.njcu.edu/programs/jchistory/Pages/B_Pages/Black_Tom_Explosion.htm

[23] The Water is Different," U.S. Naval Institute (USNI) Port Security Conference (June 7, 2006).

[24] http://museum.gov.ns.ca/mma/AtoZ/HalExpl.html

[25] Idid.,

[26] http://www.collectionscanada.ca/education/firstworldwar/05180202/0518020203_e.html

department and the Republic Oil Refining Company fire-fighting team mobilized on the dock to put out the fire on the ship. In addition, crowds gathered to watch the spectacle. Around 9:12 in the morning the GRANDCAMP exploded, sending a column of smoke two thousand feet into the air. The shockwave knocked two small planes out of the air.[27] A few moments later the Monsanto Chemical Plant, located across the slip, caught fire and collapsed, killing 145 workers. According to some accounts, the blast was so powerful that the shock could be felt in Louisiana 250 miles away.

The explosion caused another liberty ship, the HIGH FLYER, moored near the GRANDCAMP, to catch fire. The HIGH FLYER was loaded with sulfur as well as a thousand pounds of ammonium nitrate fertilizer. Rescue crews tried unsuccessfully to free the HIGH FLYER from its anchor and other debris. At approximately 1:10 am the following day, the HIGH FLYER exploded in a blast some thought more severe than that of the GRANDCAMP.[28] Although the loss of life was significantly less than the initial explosion of the GRANDCAMP, the explosion of the HIGH FLYER compounded already severe property damage throughout the city.

The Texas City disaster is considered to be the worst industrial disaster in the nation's history. In all, 581 people were listed in the official death toll. Estimates on the number of individuals injured in the explosions range between 3,500 and 5,000. Overall, the number of dead or injured accounted for roughly 25 percent of the town's entire population of 16,000. Aggregate property loss amounted to almost $100 million or more than $700 million in today's dollars.[29]

Port Chicago Naval Magazine Explosion

On the Suisan Bay in the estuary of Sacramento and San Joaquin Rivers, in Port Chicago, California, the Port Chicago Naval Magazine exploded on July 17, 1944.[30]

At the time of the explosion, 4,606 tons of high explosives and incendiary bombs, depth charges and ammunition were being loaded on the merchant ships SS QUINAULT VICTORY and SS E.A. BRYAN for use in the Pacific theatre. In addition, sixteen rail cars were on the pier with another 429 tons of ammunition.[31] Around 10:18 p.m., an explosion occurred on the pier and started a fire. A few seconds later a more powerful explosion occurred as the entire cargo of the E.A. BRYAN detonated, destroying the pier and every building in Port Chicago. The explosion also killed 320 cargo handlers, crewmen and sailors injuring more than 400 others.

---

[27] http://www.local1259iaff.org/disaster.html

[28] Ibid.

[29] Ibid.

[30] The port no longer exists. In 1968 all property was bought and buildings demolished by the Federal Government to form a safety zone around the adjacent Concord Naval Weapons Station loading docks.

[31] http://www.history.navy.mil/faqs/faq80-1.htm

Relevance in Today's Maritime Environment

How do these historical incidents pertain to today's maritime world and those who live and work in it? Some have said that those who fail to learn from history are doomed to repeat it. This is why after events such as the explosion at Black Tom Island; the explosions in Halifax, Texas City, and Port Chicago; the grounding of the EXXON VALDEZ; 9/11; and Hurricane Katrina, authorities undertook efforts to learn as much as they could about what happened. From those investigations came recommendations and actions intended to protect us from repeating past mistakes.

However, there is an important difference now that did not exist at the time of the attacks and accidents previously listed. As massive as those explosions were, they would be small when compared to the devastation that could befall us from a nuclear device. The United States cannot afford to let such an incident or other equally catastrophic events occur and then learn from them.

Weapons of Mass Destruction

Among the grave threats faced by the nation is the potential for terrorists to acquire Weapons of Mass Destruction. Terrorist organizations have publicly stated their intent to do so and such devices represent the greatest capacity to do the gravest harm to the United States and the World. Radiological and nuclear (RAD/NUC) weapons are two types of WMD of high concern. Not only do they have the potential to do tremendous damage, but they may be easily concealed as they can be relatively small—small enough to be carried onboard a small vessel.

Senator Richard G. Lugar summed up the WMD concern in *The Lugar Survey on Proliferation Threats and Responses*. "The September 11 attacks do not come close to approximating the destruction that would be unleashed by a nuclear weapon. Weapons of mass destruction have made it possible for a small nation, or even a sub-national group, to kill as many innocent people in a day as national armies killed in months during World War II."[32]

How might terrorists obtain a nuclear weapon? They might buy or steal a nuclear warhead. Or they might acquire the components of a nuclear weapon and try to assemble their own improvised nuclear device (IND).[33] Analysts believe that due to the dissolution of the former Soviet Union and the spread of its nuclear technology to other states, these scenarios are becoming more plausible.

A more likely scenario that has lesser, though still very serious consequences, involves radioactive material. The most well known such threat is an RDD, or "dirty bomb." In a dirty bomb explosion, the blast from conventional explosives is used to spread radioactive material over an area. The contamination resulting from such a detonation

---

[32] Richard G. Lugar, "The Lugar Survey on Proliferation Threats and Responses," June 2005, p. 2.

[33] Jonathan Medalia, *Terrorist Nuclear Attacks on Seaports: Threat and Response*, Washington, DC: Congressional Research Service, January 24, 2005.

could have profound effects, including physiological, which significantly magnify the actual damage done by the explosion.

Terrorists contemplating WMD attacks could use small vessels in several ways, as previously outlined in this report.

Open Maritime Environment

The waters in which terrorists may operate offer unencumbered access to many different users—no other domain, including space, air, land, or cyberspace, offers greater access than the maritime domain.[34] This level of access presents opportunities, threats, and challenges to the safety, security, and responsible stewardship of our national maritime interests.

Entries into the air and space domains are inhibited by technology and regulatory regimes that have been in place since those domains began to be exploited, but the sea presents a different case. For centuries, people have embarked on the sea, and now more than ever, access is easy and relatively inexpensive.

Many millions of square miles of ocean are under no nation's jurisdiction. Unlike national land and air space, with clearly defined borders, much of the ocean is sparsely regulated and not every nation is signatory to what international regulations exists (e.g., the United Nations Law of the Sea Convention). The sea also has a tradition of secrecy. Stretching back millennia, sea farers have found safety in anonymity. Even commercial operations have sought to avoid detection, with such industries as fisheries striving to keep the location of prime fishing spots from competitors.

This problem is exacerbated by sheer numbers. Over 70 million people in the United States participate in some form of recreational boating. There are 350 commercial ports and 95,000 miles of coastline (including bays, lakes, and rivers) in the U.S. and trends show the numbers of boaters to be increasing. By way of historic example, since the Federal Boating Safety Act was enacted in 1971, the number of registered boats has more than doubled within the United States to nearly 13 million.

The challenge in the post-9/11 environment is to reconcile the use of these waters for commerce, transportation, and recreation with the need to protect the nation. This involves understanding the situation on the water, identifying threats, and defeating those threats at the greatest possible distance from the shore. Simply put, the challenge is to balance national security concerns with traditional maritime heritage.

The United States faces the daunting challenge of distinguishing between legitimate and illicit activity in an operational maritime environment crowded with many unknowns. There are no easy answers to this challenge. There is no single fence, sensor, screening

[34] "New Threats, New Challenges, New Strategy." George Schultz Lecture Series.

technology, security regime, or operational asset that can address the problem adequately.[35]

SAN FRANCISCO (Oct. 6, 2007)- Three Coast Guard 25-foot boats help enforce the security zone set for the Parade of Ships as it enters the San Francisco Bay. The Parade of Ships is one of several activities that make up the annual Fleet Week event, which honors the men and women of the armed forces. (Coast Guard photo by Petty Officer Kevin J. Neff)

Strategic Environment

The U.S. Coast Guard *Strategy for Maritime Safety, Security and Stewardship*, released on January 19, 2007, focuses on enhancements to legal regimes, awareness, and operational capabilities to position the Coast Guard to defeat the threats Americans likely will encounter in the future.[36]

Awareness is a critical element of this three-part strategy. To quote, "Maritime Domain Awareness (MDA) is the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States."[37] MDA includes information about vessels (e.g., dynamic track data, static data on history, ownership, and characteristics, etc.), people (e.g., passengers, crew, dock workers, agents), cargoes, weather, the environment, and infrastructure.

[35] "Comments of Admiral Thad Allen at the National Conference of State Legislatures." (December 6, 2006).

[36] http://www.uscg.mil/comdt/speeches/docs/CGS-Final.pdf

[37] *National Plan to Achieve Domain Awareness*, Washington, DC, 2005, p. *i*.

However, U.S. maritime authorities are hampered by many gaps in awareness - in their access to and ability to share, fuse, and analyze large amounts of information regarding maritime activities; their ability to monitor the domain itself; and their ability to disseminate information through a national common operating picture.

Of particular concern is the inability to monitor smaller vessels, which have little or no reporting requirements and are largely anonymous. Terrorist groups have, as discussed previously, used small boats as WBIEDs and could also use such vessels to smuggle WMD materials, weapons, and people into the United States. Detecting and tracking small vessels is one of the most pressing priorities for awareness efforts in the maritime domain.[38]

The nation needs solutions that improve MDA in order to obtain a clearer picture of what is happening on the seas. There are thousands of seafarers who make their living from the sea and the millions who enjoy recreation on the water who can help improve the clarity of that picture. The day-to-day awareness of neighbors watching out for neighbors, combined with technical solutions, has the potential to make a significant difference in the safety and security of the U.S. maritime domain.

Marine and Air assets from CBP patrol the waters off of southern Florida. (photo by James Tourtellotte)

A Layered Security System

To address the challenges described above, federal agencies involved in maritime activities use a layered security approach. This approach addresses each vulnerability

[38] *The U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship* (USCG: January 19, 2007), p. 31.

through appropriate means and partnerships. Layered security results in a comprehensive mutually reinforcing system with deliberate redundancies to serve as fail-safe mechanisms.[39] These layers begin as far from U.S. shores as practical while leveraging law enforcement, intelligence, military, diplomatic, and private sector activities to best effect. Thus, even though a check at one stage has a low probability of uncovering a problem, multiple checks throughout the layers have the potential to greatly increase the probability of detection.[40]

Much effort to date has focused on applying a layered security approach to the security challenges presented by large commercial vessels. The *Maritime Transportation Security Act of 2002* (MTSA) and the *International Ship and Port Facility Security Code* (ISPS Code) set requirements aimed at curtailing theft, crime, and vulnerability to terrorism through the gateways of international trade. By improving security, MTSA and ISPS initiatives have reduced the likelihood that a terrorist could smuggle weapons, people, or illicit materials on a vessel without being detected, or that they could gain access to infrastructure.

In addition to the MTSA and ISPS, the USCG and U.S. Customs and Border Protection (CBP) have implemented layers of "trip wires" along the stages of an overseas shipment. This layered set of measures occurs in three broad arenas: overseas, in transit, and in U.S. waters.

Overseas efforts include:

- *The Container Security Initiative* (CSI). All U.S.-bound containers are screened for risk prior to being loaded onto a vessel. Suspect containers are targeted and identified for additional scrutiny.[41]
- *24-Hour Advanced Manifest Rule*. With some exceptions, sea carriers provide cargo descriptions and valid consignee addresses 24 hours before cargo is loaded in a foreign port bound for the United States.
- *Customs-Trade Partnership Against Terrorism* (C-TPAT). C-TPAT is a partnership system in which industry voluntarily implements security standards to secure its supply chains and in return receives direct benefits through enhanced trust with government regulators.
- *International Port Security Program.* Host nations work jointly with the USCG to assess the host countries' overall compliance with the ISPS Code, and in many cases assist the country with identifying potential areas for improvement.

---

[39] *The U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship* (USCG: January 19, 2007), p. 15.

[40] Michaelis, "Defending Against a Small Vessel WMD Attack."

[41] Jon D. Haverman and Howard J. Schatz, *Protecting the Nation's Seaports: Balancing Security and Cost*, San Francisco: Public Policy Institute of California, 2006, p. 197.

In Transit efforts include:

- *Automated Targeting System* (ATS). This is a CBP system for risk assessments used to evaluate the risks posed by inbound cargo.
- *Ship Security Alert System* (SSAS). The SSAS allows a vessel operator to send a covert alert to shore in case of onboard violence or the hijacking of a vessel.
- *Automatic Identification System* (AIS). AIS is an international standard for ship-to-ship, ship-to-shore, and shore-to-ship data communication approved by the International Maritime Organization (IMO). It is used mostly by commercial vessels and large vessels engaged in international voyages and those vessels operating within the U.S. Vessel Traffic Service or a Vessel Movement Reporting System area.

In U.S. Waters efforts include:

- *Transportation Workers Identification Card* (TWIC). A biometric identification card currently being developed and deployed, TWIC cards will be carried by all transportation workers requiring unescorted access to secure areas at major transit locations and on vessels.
- *America's Waterway Watch* (AWW) Program. The program educates the boating public, commercial operators and others on how to recognize and proactively report potential terrorist activities.
- *Port Security Assessment Program.* The USCG has examined key infrastructure in 55 of the nation's major ports, with the results used to inform local security plans.
- *Non-Intrusive Inspection Technology.* Using large-scale gamma ray and x-ray imaging systems, CBP scans cargo for contraband, including materials associated with WMD.[42]

A greater description of existing supply chain security efforts is given in the draft DHS Strategy to Enhance International Supply Chain Security, available on the Department web site.[43]

Although there are many efforts underway to promote security in the maritime environment, none of these regulations and systems apply to smaller vessels, despite concern that small vessels could be exploited by terrorists in various ways to harm the United States. Many of the layered security measures designed for large vessels have not been applied to small vessels because of cost, complexity and other concerns. Some measures may be applicable and could help protect the nation from threat vectors involving small vessels. Key questions, many of which were addressed at the Summit, include the following:

- How best should the government engage the small vessel community?

---

[42] Michaelis, "Defending Against a Small Vessel WMD Attack," p. 6.

[43] http://www.dhs.gov/xprevprot/publications/

- What is needed to enhance the role of the small vessel community as a fully engaged partner in the layered security approach protecting the nation?
- What forms of education, information-sharing, and outreach are best for involving the disparate elements of the small vessel community as an integral part of the "eyes and ears" contributing to maritime security?
- What types of measures are available and appropriate for improving the ability of authorities to identify vessels and operators in a timely manner?
- What are the limitations of current identification systems for protecting the nation against terrorist exploitation of small vessels?
- Could changes in existing operator certification procedures or adoption of new technologies make vessel identification more reliable and timely?

Addressing these questions is a key component in further protecting the United States from the threat of a maritime terrorist attack. The following sections present highlights from the NSVSS dialogue that involved both public and private sector stakeholders concerned with improving maritime security, and what they had to say about these issues and related questions.

III. SUMMIT CONCEPT & METHODOLOGY

This section discusses the NSVSS development process that enabled the exchange of concerns and ideas among federal homeland security officials and small vessel community stakeholders. It begins by describing the basic concept and conference structure that guided the Summit interaction to capture stakeholder thoughts in a variety of data gathering activities. This section also reviews the methodology used to develop the scenarios, providing the necessary context for the breakout session facilitated discussions.

Dr. Charles Brownstein, from the Homeland Security Institute, explains the concept of the scenarios presented at the Summit to the stakeholders.

Summit Concept

The Summit was intentionally designed to fully engage the various stakeholder communities to leverage their experience and record their ideas and concerns on maritime safety and security issues. It identified small vessel threat issues and solutions from the perspective of the small vessel stakeholder through a scenario-driven approach. Distinguished speakers, expert panels, keynote addresses, plenary sessions, and facilitated discussion working groups were utilized to inform the attendees and engage them in exploring possible solutions to homeland security concerns. Throughout the conference, stakeholders were encouraged to take advantage of the forum and engage speakers, panel members, fellow stakeholders and facilitators in meaningful dialogue.

On the morning of the first day of the Summit, participants heard from several distinguished speakers representing the federal government. Speakers included: the Honorable Michael Chertoff, Secretary U.S. Department of Homeland Security; Admiral

Thad Allen, Commandant of the U.S. Coast Guard; W. Ralph Basham, Commissioner of U.S. Customs and Border Protection; Vayl Oxford, Director of the Domestic Nuclear Detection Office; and Dr. Christopher Merritt of the U.S. Coast Guard Intelligence Coordination Center.

The speakers' presentations introduced the participants to the issues and concerns involved in the use of small vessels by terrorists to attack the U.S., its maritime domain, critical infrastructure and/or the general public. More importantly, the discussions were designed to stimulate interest in thinking about ways to best prevent, protect against and mitigate a terrorist attack and encourage attendees to share their insights and knowledge throughout the Summit. Through this dialogue, DHS and the small vessel community developed a range of issues and ideas regarding solutions to better secure our nation's ports, waterways and coastal areas. Each presentation was followed by a question and answer session which allowed further exploration of the subject matter.

In the afternoon of the first day, representatives of stakeholder agencies, industries, associations and private citizens participated in three panel discussions addressing security concerns and issues for particular small vessel communities. Similar to the opening session, each panel was followed by a question and answer period to address stakeholder concerns and answer their questions. Representatives were divided into the following three panels:

Recreational Boater Interests:

Mr. Richard Schwartz, Boat Owners Association of the United States

Mr. Jim Browning, Marine Retailers Association of America

Mr. Earl Waesche, National Boating Federation

Mr. Jim Muldoon, National Boating Safety Advisory Council

Ms. Cindy Squires, National Marine Manufacturers Association

Commercial Vessel Interests:

Ms. Emily Reiblein, American Waterways Operators

Capt James Ruhl, Commercial Fishermen of America

Capt Ed O'Brien, National Association of Charter Boat Operators

Capt Elizabeth Gedney, Passenger Vessel Association

State and Local Government Interests:

LtCol Don Holway; Florida Fish and Wildlife Conservation Commission

Maj John Fetterman, Maine Department of Marine Resources

Lt Bill Krul, Marine Patrol, St. Clair County, Michigan

Sgt Jim Lambert, Marine Patrol, Alameda County, California

Following the panel discussions, Summit participants adjourned into six working group sessions that provided the small vessel community participants the opportunity to offer their reactions to the remarks of plenary speakers and panels, as well as to discuss other concerns and issues. In order to obtain a good mix of perspectives, each working group consisted of approximately 50 individuals that represented a smaller sampling of attendee groupings represented at the Summit. A structured discussion process was employed to increase the opportunities for the full range of Summit participants to offer their views. Each working group was facilitated by representatives of the Homeland Security Institute (HSI) research staff. In addition, each working group had two HSI staff recorders who captured the discourse for later analysis.

Beyond panel presentations, all discussions were conducted in an atmosphere of non-attribution to ensure that participants felt free to express their views and opinions openly.

On the second day of the Summit, the six working groups reconvened. Each group was presented with two scenarios by an HSI facilitator depicting waterborne terrorist attacks via small vessels. The scenarios were designed to provide a threat and issue oriented context for facilitating an analytic discussion among the stakeholders to answer the following questions:

- What could have been done to *prevent* this attack from occurring?
- What could have been done to *protect* against the consequences of this attack?
- What could have been done *in advance* to *mitigate* the consequences of this attack?

Each working group discussion was followed by a report to the plenary. A spokesperson for each group presented the key issues emanating from the dialogue. The Summit concluded with an open plenary in which participants shared thoughts and overall view of the NSVSS.

Post-Summit Data Collection

Post-Summit feedback from attendees was obtained through an electronic survey that was prepared by Knowledge Engineering and Associates (KEA). As proof of a highly engaged constituency at the NSVSS, of the nearly 260 stakeholders who attended the Summit, 183 surveys were completed for a return rate of 70 percent.

All of the notes taken at the Summit during the plenary sessions and the two working group scenario discussions (six working groups for each discussion period), as well as the results from the post-Summit survey, were used to develop the findings and recommendations presented in this report.

Scenario Development Methodology

Concept: The Summit program and objectives were intended to inform small vessel stakeholders on security risks in the U.S. maritime domain and, with that background, these subject matter experts were asked to apply their marine knowledge and experience in facilitated discussions of security concerns. In order to provide the context for these

discussions, six maritime terrorist attack scenarios were developed to address the question: "What means or methods could have deterred, defeated or mitigated the attack and its effects?"

Scenario Development Process: The HSI project team collaborated with the Federal Interagency NSVSS Working Group to develop hypothetical attack story lines in a series of scenario development workshops.[44] To guide this process, the HSI team developed a framework of elements common to all scenarios. Those elements are:

- Threat – the weapon or device which could be used to cause the violence or destruction of the attack;
- Threat vector – the means of conducting the attack. Given the subject of the Summit, the type of small vessel which could be used or exploited to conduct the attack;
- Target – the objective of the attack, the destruction of which could cause significant to grave consequences;
- Consequences – the results of such an attack in terms of death and injury, economic impact, national security concerns, symbolic effects, environmental impacts and other direct and indirect effects; and
- Venue – the site of the attack.

Added to these elements was a representative listing of small vessel security means or methods which helped guide the scenario development process. By applying these potential discussion items, the scenario developers were able to compose storylines which allowed for a robust dialogue among the breakout session participants. Those means or methods applied to the scenario development process were (in no particular order):

- Restricted access areas;
- Vessel tracking;
- Vessel registration;
- Public awareness;
- Operator certification/identification;
- Vessel identification systems;
- Law enforcement intelligence/data fusion;
- Directed standards;
- Performance standards;
- Vessel of interest;

[44] The Federal Interagency NSVSS Working Group consisted of representatives from the United States Coast Guard; Domestic Nuclear Detection Office; Federal Bureau of Investigation; Immigration and Customs Enforcement; Transportation Security Administration; Customs and Border Protection; and DHS Headquarters.

- Technical detection capabilities; and
- International cooperation.

The small vessel security means and methods derived from the breakout session discussions are further defined in Appendix D of this report.

The task posed to the HSI and the NSVSS Working Group was to combine the various scenario elements into a plausible storyline from which to develop a discussion about ways to deter, defeat, or mitigate an attack. This framework is depicted in Table 1 and further explained below.

Table 1: Scenario Development Elements

Scenario Development Elements					
Threat	**Threat Vector**	**Target**	**Consequences**	**Venue**	**Means/Methods**
Radiological/ Nuclear IND RDD	Recreational	Population	Death/Injury	Port A	Restricted Access Areas
Waterborne Improvised Explosive Device	Small Cargo	Waterway	Economic Impact	Port B	Vessel Tracking
	Off-Shore Supply	Critical Infrastructure	Symbolic Effect	Port C	Vessel Registration
	Pilot	Shipping	National Security	Waterway	Public Awareness
	Small Passenger		Environmental Impact	Small Port	Certification/ Identification
	Commercial Fishing		Small Vessel Owners/ Operators	Inland Port	Identification Systems
	Towing				Law Enforcement Intelligence/ Data Fusion
	Tourism				Directed Standards
	Utility				Performance Standards
					Vessels of Interest
					Technical Detection Capabilities
					International Cooperation
					Layered Defense

The scenarios were developed taking all elements into consideration simultaneously throughout the process, rather than in a linear, sequential fashion, i.e., one element at a time.

Threats: DHS leadership had particular interest in two threats. The radiological/nuclear (RAD/NUC) threats were of particular concern because of their potential consequences. Waterborne improvised explosive devices (WBIEDs, i.e., "boat bombs"), while not presenting the catastrophic effects of a RAD/NUC, were also of interest based on recent such terrorist attacks around the world. Each of the six breakout groups were presented with and discussed a WBIED incident in one breakout session, then a RAD/NUC incident in the other session.

Threat Vectors: All types of small vessels, as listed in Table 2, were considered potential threat vectors. The working group attempted to apply a variety of small vessels across the six scenarios. Factors considered in this selection included the likely mix of particular small vessels in the port and the appropriateness of that vessel for the prescribed threat/target combination.

Targets: The selection of targets considered the threat weapons and devices, the particular ports, the vulnerabilities of potential targets in those ports, and the consequences of attacks on those targets.

Consequences: The consequences of an attack reflected the combination of the method of attack and the target; considered the likelihood and extent of human death and injury; direct and indirect economic impact; symbolic or iconic effect; national security concerns; environmental impact; and damages to stakeholder enterprises.

Venues: The selection of attack venues sought a diversity of ports and waterways by geographic location, size, targets and vulnerabilities offered, and type of vessel. Proximity to foreign ports in Canada, Mexico and the Caribbean also factored into certain scenarios to capture the international threat elements. Coast Guard Port Security Assessment Reports were used and considered in the selection of each venue. Working group members' familiarity with the environs of candidate ports was also a consideration.

The results of this deliberative process are outlined in Table 2. Due to security concerns, the actual venues, targets, dimensions of the threats and extents of the consequences are not identified.

Table 2: Scenario Outlines

VENUE	THREAT	THREAT VECTOR(S)	TARGET(S)	CONSEQUENCES
A - NORTHEAST PORT	WBIEDs (2)	COMMERCIAL FISHING BOATS (2)	OIL TANKERS (2)	INJURY/LOSS OF LIFE ECONOMIC IMPACT ENVIRONMENTAL IMPACT
B – SOUTHEAST PORT	RDDs (2)	FOREIGN RECREATIONAL YACHTS (2)	CRUISE SHIP WATERSIDE MALL/ POPULATION	INJURY/LOSS OF LIFE ECONOMIC IMPACT ENVIRONMENTAL IMPACT
C – INTERNATIONAL WATERWAY	WBIED	RECREATIONAL BOAT	COMMERCIAL ORE CARRIER/ WATERWAY	ECONOMIC IMPACT
D – CENTRAL U.S. WATERWAY	WBIED	BARGE & TOW	WATERWAY LOCK	ECONOMIC IMPACT
E – NORTHWEST PORT	RDD	COMMERCIAL FISHING BOAT	STATE FERRY DOWNTOWN/ POPULATION	INJURY/LOSS OF LIFE ECONOMIC IMPACT ENVIRONMENTAL IMPACT
F – SOUTHWEST PORT	IND	FOREIGN CHARTER FISHING BOAT	POPULATION CENTER/ CRITICAL INFRASTRUCTURE	CATASTROPHIC INJURY/LOSS OF LIFE ECONOMIC IMPACT ENVIRONMENTAL IMPACT

The HSI project team took the combinations of scenario elements and developed them into six storylines, which were then validated in consultation with subject matter experts. Each storyline included the six primary phases of a terrorist attack[45]:

- Research and planning phase – the concept, potential weapon and target selection, and overall plan determination.
- Preparation and staging phase – the assembly and training of necessary personnel and materials and their positioning for mobilization.
- Surveillance – reconnoitering of the target and its environments to assess the viability of the initial attack plan, identify impediments, and determine necessary tactics for success.
- Rehearsal – practice of the approach and tactics to be executed in the attack.
- Execution – the actual conduct of the attack.
- Aftermath – the egress and/or assessment of the attack.

[45] For more detailed discussions of the chain of events involved in terrorist activities, see Operational Considerations," p. 18.

Scenario development is an inexact science and, as in real life, countless variables and situational quirks inform the process, resulting in outcomes which are not predictive but which are representative of what might happen. To inform the scenario development process, certain issues germane to the present-day maritime security environment were introduced into the phases of each attack. Those maritime security issues included in the scenario development process were:

- Inadequate or untimely actionable intelligence;
- Missed threat indicators;
- Lack of public awareness about threats and the proper responses to those threats;
- Lack of communication among the public and homeland security and law enforcement authorities;
- Stove-piped agencies;
- Inadequate information sharing among homeland security and law enforcement agencies;
- Lack of a capability to identify and distinguish threats from non-threats;
- Inadequate planning and/or preparation;
- Lack of resiliency; and
- Unique features of particular ports and/or waterways.

The matrix in Table 3 illustrated the means or methods which were captured within the content of each scenario.

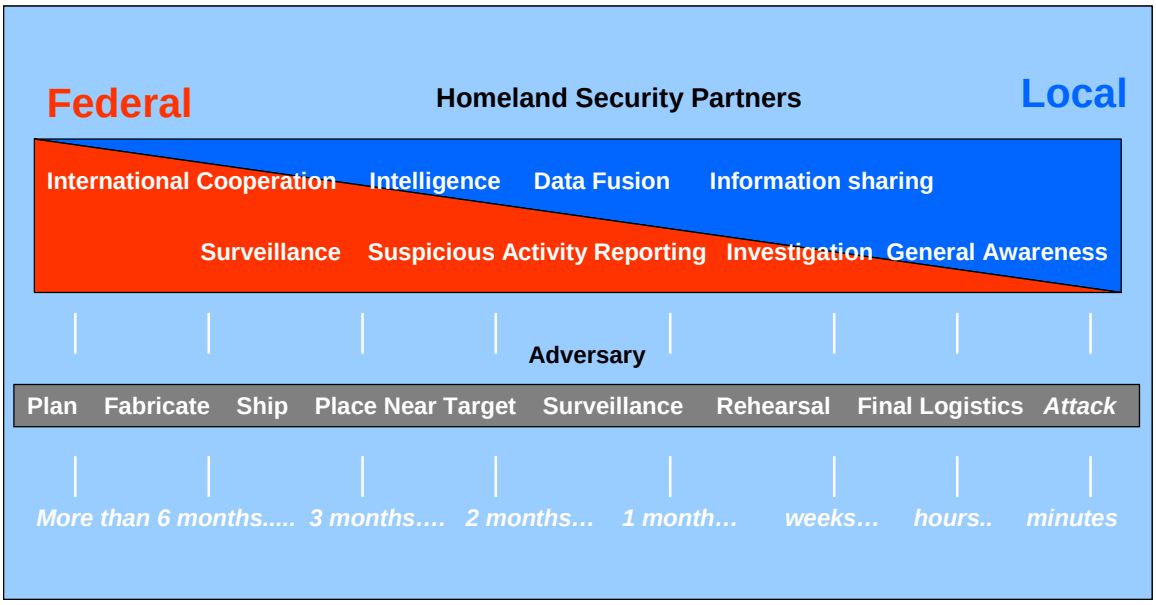
Table 3: Scenarios – Means/Methods Matrix

SCENARIO METHOD	NORTHEAST PORT WBIEDs	SOUTHEAST PORT RDDs	INTERNATIONAL WATERWAY WBIEDs	CENTRAL U.S. WATERWAY WBIEDs	NORTHWEST PORT RDD	SOUTHWEST PORT IND
RESTRICTED ACCESS AREA	√	√				
VESSEL TRACKING	√		√		√	√
VESSEL REGISTRATION	√	√	√	√	√	√
PUBLIC AWARENESS	√	√	√	√	√	√
CERTIFICATION/ IDENTIFICATION	√	√	√	√	√	√
VESSEL IDENTIFICATION SYSTEMS	√			√	√	
LAW ENFORCEMENT INTELLIGENCE/ DATA FUSION		√	√		√	
DIRECTED STANDARDS						√
PERFORMANCE STANDARDS						√
VESSELS OF INTEREST		√	√		√	√
TECHNICAL DETECTION CAPABILITIES		√			√	√
INTERNATIONAL COOPERATION		√	√		√	√

Table 3 illustrates that each scenario bore the potential for a discussion of a significant number of methods, and that all the representative methods were accommodated within the context of at least one of the scenarios.

To ensure the accuracy and fidelity of each scenario, HSI project team researchers, experts within the working group, and security officials at each selected venue corroborated the content and context throughout the scenario development process.

Timelines were developed to outline the events preceding each attack and break down the scenario into phases for discussion. On further analysis, these timelines also illustrated that as events approached the moment of attack, the nature of the means and methods to defeat or deter the attack transitioned from "strategic" preventative operations to "tactical" operations just prior to the attack. Another way of considering this relationship is to note that the more strategic operations were exclusively federal responsibilities with a gradual continuum along the timeline toward the attack where they become, immediately prior to the attack, local responsibilities (though the local responsibility may, as in the case of the Coast Guard field units, include federal efforts). Figure 1 is a generic scenario timeline which illustrates this concept.



Relationship of Partner Actions, Adversary Actions and Time

Figure 1: Locus of Responsibility for Defeating or Deterring an Attack

IV. SUMMARY OF SPEECHES AND PRESENTATIONS

Plenary and Keynote Speeches*

For continuity purposes, the review of the plenary speakers' remarks is presented in order of their appearance at the Summit:

- Admiral Thad Allen, Commandant U.S. Coast Guard
- W. Ralph Basham, Commissioner U.S. Customs and Border Protection
- Vayl Oxford, Director Domestic Nuclear Detection Office
- Dr. Christopher Merritt, U.S. Coast Guard Intelligence Coordination Center
- Hon. Michael Chertoff, Secretary U.S. Department of Homeland Security
- Michael Wermuth, RAND Corporation

The Summit commenced with the welcoming remarks of the official host, Rear Admiral Brian Salerno, Assistant Commandant of Safety, Security and Stewardship for the Coast Guard. He emphasized that the Summit was an important step in creating a continuing dialog among small vessel stakeholders and government leaders at all levels to address security risks in the U.S. maritime domain. He noted that the Summit participants would hear from several top DHS leaders and that this national forum provided an opportunity to hear back from the small vessel community participants through their questions and discussions with the speakers and during the subsequent breakout scenario sessions.

Admiral Thad W. Allen, Commandant U.S. Coast Guard

In his remarks, Admiral Allen stated that the NSVSS was an unprecedented event on the part of DHS to address homeland security issues with the private sector. He warned that the nation remains vulnerable to small boat terrorist attacks and that stakeholder ideas, insight, and cooperation are needed to come up with a comprehensive and integrated approach to preventing this problem. Admiral Allen urged the attendees at the Summit to share their insights and recommendations as to what regimes the private sector might want DHS to implement, what kind of systems make sense, and how small vessel operators would employ them.

* Presentation materials used during speeches at the Summit are the property of the individuals who presented or the organization they represent. Unless noted in this report, these materials have not been archived by DHS. Requests for, or inquiries about, such materials should be addressed to speakers or their organization.

Coast Guard Commandant Adm. Thad Allen address attendees at the DHS Small Vessel Security Summit in Crystal City, Va. June 19. (USCG photo by Telfair H. Brown Sr.)

W. Ralph Basham, Commissioner U.S. Customs and Border Protection

Commissioner Basham opened his statement describing the 1917 explosion of the French cargo ship SS MONT BLANC carrying munitions in the Canadian City of Halifax, resulting in many thousands killed and injured.[46] Commissioner Basham used this example to remind the stakeholders at the NSVSS that similar loss of life could occur in the United States if a terrorist bomb were detonated off one of the nation's seaports. He highlighted the relevancy of terrorist attacks conducted via small vessels by noting several recent maritime attacks including the bombing of the USS COLE in 2000, the attack on the French oil tanker LIMBURG in 2002, and the suicide boat attack on Iraq's main oil terminal in Al-Basra in 2004.

In addition, Commissioner Basham described the extensive activities of U.S. Customs and Border Protection (CBP) in securing the nation's borders in the six years since 9/11. He emphasized that CBP has accomplished a great deal in building layered security, so that the borders are not the first line of security, but the last. CBP's strategy to secure trade and travel includes five interrelated initiatives none of which existed before 9/11 and they are:

[46]On December 6, 1917, the MONT BLANC, which was loaded with wartime explosives, accidentally struck another vessel and ran aground near the port of Halifax, Nova Scotia, and exploded. A large part of the city of Halifax was destroyed; approximately 2,000 people were killed and another 9,000 injured. The MONT BLANC explosion was the largest man-made explosion until the first atomic bomb explosion in 1945, and remains the largest non-nuclear explosion in history.

- Requiring advance electronic information on all cargo and all passengers and crewmembers arriving from abroad by air or sea.
- Analyzing the information received at the National Targeting Center (NTC) to gauge the risk of terrorism.[47]
- Partnering with other countries through the Container Security Initiative (CSI) to ensure that high-risk containers are screened before they are shipped to the United States.[48]
- Working with private industry to secure the international supply chain utilizing the Customs-Trade Partnership Against Terrorism (C-TPAT).[49]
- Using the latest and most sophisticated technologies to screen for radiation and imaging of cargo containers for anomalies at our nation's ports of entry.

Commissioner Basham also commented that in November 2006, CBP and the USCG signed a joint memorandum directing each agency to coordinate vessel enforcement operations. In particular, CBP and the Coast Guard are sharing information, targeting and training together, boarding vessels together, and exchanging liaison officers. This coordination is also working to identify ports where CBP/USCG can share the same workspace for command and operations centers. A number of these command centers are already operational.

---

[47] The NTC was established in October 21, 2001, in direct response to the terrorist attacks of 9/11. Since then it has become a preeminent anti-terrorism facility within the Department of Homeland Security (DHS). NTC analysts filter through advance information on people and products looking for potential terrorists or terrorist weapons. The NTC is a prime example of pushing the zone of security outward and keeping terrorism at arms length by screening people and cargo before they arrive at U.S. shores.

[48] CSI addresses the threat to border security and global trade posed by the potential for terrorist use of a maritime container to deliver a weapon. CSI involves a security regime to ensure all containers that pose a potential risk for terrorism are identified and inspected at foreign ports before they are placed on vessels destined for the United States. CBP has stationed multidisciplinary teams of U.S. officers from both CBP and Immigration and Customs Enforcement (ICE) to work in cooperation with their host foreign government counterparts. Their mission is to target and prescreen containers and to develop additional investigative leads related to the terrorist threat to cargo destined for the United States.

[49] The Customs-Trade Partnership Against Terrorism (C-TPAT) program is CBP's premier trade security program. The purpose of C-TPAT is to foster partnerships with the trade community for the purpose of securing the U.S. and international supply chains from possible use by terrorist organizations. C-TPAT requires trade company participants to document and validate their supply chain security procedures in relation to existing CBP C-TPAT criteria or guidelines as applicable. CBP requires that C-TPAT company participants develop an internal validation process to ensure the existence and implementation of security measures documented in their Supply Chain Security Profile and in any supplemental information provided to CBP. As a part of the C-TPAT process, CBP C-TPAT Supply Chain Security Specialists (SCSS) and the C-TPAT participant jointly conduct a validation of the company's supply chain security procedures. The validation process is essential to verifying the company's commitment to C-TPAT.

Commissioner of U.S. Customs and Border Protection W. Ralph Basham meets with stakeholders at the Summit.

In conclusion, Commissioner Basham stressed that what is missing in the small vessel environment is Maritime Domain Awareness (MDA). This is the ability to see and understand who is operating in the maritime domain and determine what risk they pose. He stated that authorities know a great deal about large vessel operators, their crew and cargo, and how they operate. Conversely, relatively little is known about small commercial vessel operators and even less is known about recreational vessel owners/operators. He expressed that technology used by air traffic controllers such as transponders and radar to identify aircraft operating in their airspace also needs to be used in the maritime domain to track vessels.[50]

Vayl Oxford, Director Domestic Nuclear Detection Office

Director Oxford began by citing the establishment of the Domestic Nuclear Detection Office (DNDO) on April 15, 2005 as a component of DHS manned by both dedicated staff and detailees from throughout the DHS component agencies. DNDO's mission is to improve the nation's capability to detect and report unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the nation, and to further enhance this capability over time.

Director Oxford observed that the risk of a terrorist acquiring and using a nuclear or radiological device as one of the greatest threats facing the nation. He emphasized that a robust layered defense must be developed and that each layer must reduce the terrorist's

[50]Mr. Basham noted that the USCG, the Royal Canadian Mounted Police, CBP, and the Ohio State Division of Watercraft are currently testing state-of-the-art vessel tracking technology in the Great Lakes.

ability to use such threats against the United States. The layered security concept includes:

- Eliminating excess stocks of nuclear materials and weapons;
- Protecting existing stocks from theft or diversion;
- Detecting illicit movement of nuclear or radiological material overseas; and
- Enhancing domestic detection and interdiction efforts.

He also highlighted the importance of the Port Partnership Initiative (PPI), which is creating a close working relationship between DNDO and maritime stakeholders to enhance maritime Preventive RAD/NUC Detection (PRND) capabilities. DNDO is actively working with detection equipment and technology such as Human Portable Radiation Detection Systems (HPRDS) and the development of new mobile and fixed standoff detection systems, although an effective PRND Program needs to be built within a POETE/Ops (People, Organization, Equipment, Training, Exercise and Operations Support) framework.

Dr. Christopher Merritt, U.S. Coast Guard Intelligence Coordination Center

In his presentation on small vessel threats, Dr. Merritt presented several open-source video clips showing small boat attacks committed by terrorists. He also presented an extensive list of terrorist attacks around the world using small vessels, which included maritime attacks by al-Qaida, Abu Sayyaf Group (ASG), and the Liberation Tigers of Tamil Eelam (LTTE). He made several key points. First, the al-Qaida threat, which is reconstituting itself, is the preeminent concern of the Intelligence Community. Dr. Merritt emphasized that al-Qaida possesses the intent to attack targets in the United States as well as the capability in the form of a demonstrated expertise and capacity to undertake such attacks. Second, he noted that the U.S. Navy, USCG, CBP, Immigration and Customs Enforcement (ICE) and the Federal Bureau of Investigation (FBI) are all working hard at understanding, identifying, and preempting this maritime threat. Third, active involvement by state, local and the private sector (including those attending the NSVSS) is essential and critical to counterterrorism and maritime security efforts. He concluded by noting that we are facing a dynamic threat and that we cannot rule out the possibility of the use of small vessels being used by terrorists such as al-Qaida for maritime attacks. Terrorists currently have the capacity, capability and the know how to successfully use small vessels as an effective tool against world shipping and critical transportation infrastructure.

Hon. Michael Chertoff, Secretary U.S. Department of Homeland Security

Secretary Chertoff was the keynote speaker at the NSVSS.[51] The Secretary opened by stating that the prime reason for the Summit was to provide an opportunity to engage stakeholders in a conversation on what can be done collectively to understand the security risks associated with small vessels. He stressed the need for homeland security officials and the small vessel stakeholders to talk about steps to reduce that threat across the maritime domain, as part of the effort to protect the nation from terrorist attacks. He stated that terrorist groups, including al-Qaida, have conducted terrorist attacks via small vessels (e.g., the USS COLE and the failed attack on the USS THE SULLIVANS) and that there is a continued terrorist threat from small vessels.

Secretary Chertoff asserted that the stakeholders attending the NSVSS and small vessel community are a "very powerful asset" for maritime security as part of the eyes and ears on the water that provide us with visibility and situational awareness about potential threats. Secretary Chertoff indicated that the challenge is finding a way to address the security concerns with small vessels in a way that does not treat them like large vessels that require protective measures such as automatic identification systems and vessel security plans. At the same time, we must recognize that we are operating in a maritime environment where safety is not the only concern because security is a necessity as well.

Department of Homeland Security Secretary Michael Chertoff delivered the Keynote Address on the first day of the conference

[51] A complete transcript of Secretary Chertoff's remarks to the Summit, along with the questions and answers session, is available at: http://www.dhs.gov/xnews/testimony/testimony_1184599844214.shtm.

The Secretary observed that small vessels are an important part of the economy, and that they are not the only sector of our transportation arena receiving new attention. He noted that DHS is preparing to work collaboratively with the general aviation community on measures for raising the level of security and screening for small personally operated planes.

More specifically, Secretary Chertoff highlighted three possible attack vectors of primary concern in the maritime domain.

First and foremost is the concern that a small vessel could be used as a conveyance to smuggle weapons, including weapon of mass destruction, into the United States. He noted that while much of the public attention has been focused on seaports and weapons being smuggled in containers, there is also a concern that an attacker might seek to smuggle a WMD into a seaport, or between seaports, using a small vessel.

Second, a small vessel can be used as a WBIED similar to improvised explosive devices (IEDs) used on land in Iraq and other parts of the world. The USS COLE attack in 2000 illustrates this type of terrorist attack and has implications for other maritime assets, including passenger ships, tankers, and port facilities. Finally, he indicated that we have to worry about small vessels being used to smuggle dangerous people into the United States.

Secretary Chertoff suggested taking a risk management approach to defend against this threat. A risk-based approach needs to be balanced in terms of carefully identifying the greatest threats, understanding the greater vulnerabilities, and recognizing the worse consequences of a possible attack. This offers a means of devising a balanced security system that is stringent enough to prevent and respond to a terrorist attack, yet at the same time will not destroy the livelihood or pleasure using small vessels. He indicated that this measured approach must be cost-effective, focused on the highest risk, use multiple layers of security, and be defined by the use of information and intelligence.

Perhaps most importantly, the Secretary expressed to the attendees at the NSVSS that he was not there to pass down an edict from Washington telling them what they have to do but rather to work in partnership with them to identify the way forward. Secretary Chertoff stated: “We're here to listen to your ideas, to carefully consider your concerns, to leverage your experience, because you all have a serious investment in your own vessels and the people who work with you, so you have a concern every bit as urgent as ours is to make sure we are securing our seas and our waterways. And we want to understand from you what you think works and what you think doesn't work.”

Michael Wermuth, RAND Corporation

Mr. Wermuth was the luncheon speaker on the second day of the NSVSS. He prefaced his remarks by stating that they were his opinions and did not necessarily reflect those of the RAND Corporation, which is a nonprofit research institute that focuses on public policy research. He went on to explain that violent Salafist jihadists are our principal adversaries. Al-Qaida continues to serve as propagandists, strategists and leaders but beyond them there are numerous groups around the world who are inspired to commit

violent acts. The intent of terrorist attacks is to garner media attention and force us to change our way of life in response to those atrocities. Concerning small vessels, Mr. Wermuth indicated international terrorist attacks in the maritime domain have been effective in the past even though terrorists have traditionally focused mainly on land-based attacks. According to Mr. Wermuth, the trend of terrorists rarely using small vessels as platforms to conduct terrorists attacks could change in the future as terrorists shift tactics and gain expertise in the maritime domain. The two most serious threats related to the maritime domain are smuggling Chemical, Biological, Radiological, and Nuclear (CBRN) weapons by containerized cargo or vessel into the country and using traditional explosives against soft targets. Mr. Wermuth indicated that at the Federal level huge investments are being made to prevent CBRN attacks but that we must recognize that there is no silver bullet for security and that a layered approach is the best option in defending against a flexible and agile enemy.

Following the plenary speakers, the first day Summit proceedings turned to three panel discussions representing the diverse interests and concerns of the small vessel community. The panels addressed the following aspects of small vessel security:

- Recreational vessel interests
- Commercial vessel interests
- State and local government interests

Panel I: Recreational Vessel Interests

Richard Schwartz, Boat Owners Association of the United States

Chairman Schwartz represents the Boat Owners Association of The United States (BoatU.S.), which is the largest organization of recreational boat owners in the country with approximately 650,000 members. He indicated that on April 23, 2007, BoatU.S. convened a panel of experts in waterway security and policy-making to assess a number issues associated with the small vessel threat. The panel proceeded on the assumption that it would be relatively easy for a terrorist organization to acquire or commandeer a recreational boat to conduct an attack on high value maritime assets or infrastructure. The panel concluded that short of walling off the entire U.S. shoreline or radically altering freedom of movement and association, the government needs to make the public a contributor of information and intelligence to prevent an attack from occurring and to make small vessels less attractive means for terrorists to use.

Mr. Schwartz stressed that it is exceedingly important that waterways users “buy in” to any security measures implemented by the government. To accomplish this he recommended that the Coast Guard Captains of the Port (COTP) serve as the connection between the USCG and the commercial and recreational small vessel operators. They should be given responsibility for funding to develop grassroots programs that include members of the Coast Guard Auxiliary, the U.S. Power Squadrons, non-emergency assistance towing fleet, marina operators, the general boating public and the commercial sector. He also suggested that the America’s Waterway Watch (AWW) adopt the “Lock Up. Look Out.” approach implemented by the Aircraft Owners and Pilots Association

(AOPA). This program encourages private pilots to secure their aircraft to prevent possible thefts, which could help impede terrorists. He also called for creating a nationwide Coast Guard-alerting Maritime Mobile Service Identity (MMSI)[52] that would simultaneously enhance the use of Digital Selective Calling (DSC)[53] thus providing a routine way for boaters to contact the Coast Guard about suspicious activities.

Chairman Schwartz also stated that in the interest of national security the recreational boating public would support producing identification as long as it is the same identification required by the TSA when boarding a commercial flight. He suggested that there is no need to develop a duplicative information system solely for recreational boat owners that will be costly to develop and take years to implement, especially as states are in the process of implementing the provisions of the Real ID Act of 2005.[54]

In regard to security zones, Mr. Schwartz recommended that much more information needed to be provided to the boating public so that they can comply with established security zones. Once information on security zones has been distributed to the public, the USCG should make it clear that incursions into these zones will result in civil penalties.

Lastly, BoatU.S. uniformly and strongly opposed requiring recreational boaters to install any form of the Automatic Identification System (AIS). He stated three rational for his opposition to AIS: 1) potential terrorists would not comply with this identification requirement, 2) adding millions of recreational vessels AIS signatures would overwhelm the USCG's ability to effectively monitor the system, and 3) the cost of such equipment for recreational boaters is prohibitive at a cost of $500 per device.

---

[52] A Maritime Mobile Service Identity (MMSI) is a series of nine digits which are transmitted over the radio path in order to uniquely identify ship stations, ship earth stations, coast stations, coast earth stations, and group calls. These identities are formed in such a way that the identity can be used by telephone and telex subscribers connected to the general telecommunications network to call ships automatically.

[53] The U.S. Coast Guard offers MF/HF radiotelephone service to mariners as part of the Global Maritime Distress and Safety System. This service, called digital selective calling (DSC), allows mariners to instantly send an automatically formatted distress alert to the Coast Guard or other rescue authorities anywhere in the world. Digital selective calling also allows mariners to initiate or receive distress, urgency, safety and routine radiotelephone calls to or from any similarly equipped vessel or shore station, without requiring either party to be near a radio loudspeaker. DSC acts like the dial and bell of a telephone, allowing you to "direct dial" and "ring" other radios, or allow others to "ring" you, without having to listen to a speaker. New VHF and HF radiotelephones have DSC capability.

[54] The REAL ID Act of 2005 is Division B of the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub.L. 109-13, 119 Stat. 231, enacted 2005-05-11). This legislation was intended to deter terrorism by implementing the following: 1) establishing national standards for state-issued driver's licenses and non-driver's identification cards; 2) waiving laws that interfere with construction of physical barriers at the borders; 3) updating and tightening the laws on application for asylum and deportation of aliens for terrorist activity; 4) introducing rules covering "delivery bonds" (rather like bail bonds but for aliens who have been released pending hearings); 5) funding some reports and pilot projects related to border security; and 6) changing visa limits for temporary workers, nurses, and Australian citizens.

A CBP marine unit patrols the waters to provide additional security at a national special event. (photo by Gerald L. Nino)

James Browning, Marine Retailers Association of America

Mr. Browning is a member of the Board of Directors for the Marine Retailers Association of America (MRAA) and is on the USCG subcommittee for recreational vessels concerning port safety and security. At the NSVSS, Mr. Browning spoke very briefly as the previous speaker (Richard Schwartz) addressed many of his points and he did not want to be redundant. Mr. Brown reiterated the importance of educating the boating public and favored increased education over government regulation. He also backed the view that national licensing of recreational boaters would do little to improve homeland security. Finally, he supported strong efforts to have recreational boaters report on suspicious activity, similar to the program undertaken at airports.

Earl M. Waesche, National Boating Federation

Mr. Waesche is the Legislative Director of the National Boating Federation (NBF). The NBF is the largest nationwide alliance of recreational boating organizations, totaling two million members. In his statement, Mr. Waesche expressed that many boaters are not aware of the threat posed by terrorists using small vessels and he recommended that a formal risk assessment be conducted to better understand the level of deterrence needed and the amount of resources required to implement a solution. He stated that such a formal risk assessment should provide information on the fiscal implications and likely locations of an attack. Moreover, he pointed out that current assessments do not address the threat of vessels coming to the U.S. from foreign ports, as they are thought to be a greater threat than small vessels harbored at U.S. ports.

With regards to licensing, Mr. Waesche indicated that it is clearly not the solution because it is expensive and ineffective given that prospective terrorists would be able to obtain boating licenses legally. He further suggested that if boarding a vessel was deemed necessary to verify the operator, a boating education certificate or driver's license could be used as identification.

He also advocated implementing a real-time reporting system for stolen vessels over 20 feet in length. Moreover, Mr. Waesche recommended developing a system to track vessels similar to the one implemented in the National Capital Region (NCR) to track general aviation.[55] Lastly, he stated that programs like the AWW program have lost momentum and that there needs to be greater media attention paid to them.

James P. Muldoon, National Boating Safety Advisory Council

Mr. Muldoon is Chairman of the National Boating Safety Advisory Council (NBSAC), Vice President of U.S. Sailing, and holds numerous other distinguished titles. Like many other panelists, Mr. Muldoon was concerned about how to protect our nation's ports and waterways from a terrorist attack without overly restricting boaters or damaging the maritime industry. Highlighting the accessibility of the national capital and important locations along the Chesapeake Bay area, he acknowledged that there is a potential threat because of waterborne access to important locations. Despite this, Mr. Muldoon expressed that most boaters are only marginally aware of the threat and that few feel vulnerable to it.

He further stated that there is no guarantee that closing every security gap with increased security requirements for boaters would prevent a terrorist attack. He identified five security concerns associated with small vessels: vessel identification; personal identification; lack of resources; unmonitored access points; and the risk that theft of vessels could go unnoticed for long periods of time. Before any future maritime security solutions are implemented, Mr. Muldoon stressed that the following issues be considered:

- Will it be effective?
- Are there resources available to implement it?
- Is it economically viable?
- Can it be implemented in a timely manner?
- Will it threaten the financial stability of maritime industries?
- Will the public accept it?

Most importantly, he argued that the only way to increase security of ports and waterways is to obtain "buy-in" from the public.

---

[55] The Transportation Security Administration (TSA), along with Federal government agencies and local jurisdictions, has enhanced airspace protection in the NCR through flight restrictions for general aviation aircraft operating in the airspace over the Washington, DC metropolitan area and added security measures for smaller aircraft using Ronald Reagan National Airport and certain local airports.

Mr. Muldoon identified several short-term measures to increase security until more comprehensive security plans are developed and implemented. The first measure is to greatly expand the America's Waterway Watch program across the country to include outreach to public facilities, yacht clubs, fishing clubs, boat leasing/rental facilities, and marinas. Secondly, he suggested requiring boaters to carry their driver's license or other state-issued identification while on the water. Third, expanded public service announcement campaigns were suggested, to increase boater awareness of any security measures being implemented. Fourth, he recommended requiring small vessel operators to carry radio equipment or cell phones on board at all times. Fifth, he urged dissemination of safety and homeland security information through mailings already sent to small vessel owners by government agencies and other boating organizations. Last, he recommended providing decals for all boaters to place on their vessels listing general security information and procedures for reporting suspicious activity.

Mr. Muldoon also recommended mid-term and long-term security measures. The proposed mid-term security measure would be to implement a Radio Frequency Identification (RFID) program for all boats.[56] According to Mr. Muldoon, installing an RFID would allow law enforcement to passively identify vessels at stationary monitor points without inconveniencing boaters. His long-term recommendation, which would require significant investments in both personnel and financial resources, is to increase maritime patrols throughout the ports as well as in the exclusion zones near sensitive structures.

Cindy Squires, National Marine Manufacturers Association

Ms. Squires represents the Regulatory Counsel for Government Relations of the National Marine Manufacturers Association (NMMA). The NMMA represents nearly 1,700 boat builders, engine manufacturers, and marine accessory manufacturers in the United States. NMMA members produce over 80 percent of all recreational marine products sold in the U.S. and are the largest organizer of boat shows in the country, producing 25 consumer shows each year.

She expressed that a balanced approach to security issues is critical and it is NMMA's strongly held view that any additional effort to address small vessel security by the USCG or the states should ensure that boating remains a fun and easy activity. The NMMA is greatly concerned that if boating becomes an activity filled with inspections, checkpoints, blocked access and high costs the general public will simply turn to other recreational activities.

Ms. Squires urged authorities to build on existing programs before implementing new initiatives. This includes adequate funding for the USCG, USCG Auxiliary, state boating

[56] RFID technology is similar in theory to bar code identification. With RFID, the electromagnetic or electrostatic coupling in the RF portion of the electromagnetic spectrum is used to transmit signals. An RFID system consists of an antenna and a transceiver, which read the radio frequency and transfer the information to a processing device, and a transponder, or tag, which is an integrated circuit containing the RF circuitry and information to be transmitted.

enforcement personnel, and the America's Waterway Watch program. To buttress these programs the NMMA supports the National Association of State Boating Law Administrators (NASBLA) "Partners on the Water" proposal to enhance the current homeland security program with a new Federal-state partnership and $60 million in grants for maritime security and emergency response.

She also suggested engaging stakeholders beyond the NSVSS, identifying new stakeholders such as marine bankers, and expanding outreach for the America's Waterway Watch program. To expand the AWW program, NMMA offered to publicize the program in its Boat Show Directory that reaches approximately one million boaters annually. The NMMA also offered to include an AWW program and invite USCG representatives to their National Marina Day on August 11, 2007. Moreover, she advocated that the USCG work with the Association of Marina Industries (AMI) to educate marina operators on security risks and to ensure marina and boater cooperation in programs designed to find threats and preserve access.

As did other panelists, Ms. Squires argued against requiring recreational boaters to procure any new types of identification or that they be treated any differently than automobile drivers. If identification is required she advocated that boaters should be given additional time to produce any ID after a stop and that exemptions for children should be included. With respect to security zones, Ms. Squires stated that they should be limited to critical areas, be well marked, charted and patrolled. Lastly, she stated unequivocally that the Automated Identification System (AIS) should not apply to recreational boaters.

Table 4: Panel 1 – Recreational Boating Interests

Richard Schwartz	James Browning	Earl M. Waesche	James P. Muldoon	Cindy Squires
Boat Owners Association of The United States	Marine Retailers Association of America	National Boating Federation	National Boating Safety Advisory Council	National Marine Manufacturers Association (NMMA)
• Waterways users need "buy in" of government security measures. • Government needs to make the public a contributor of information and intelligence. • America's Waterway Watch (AWW) should adopt the "Lock Up. Look Out." approach implemented by the Aircraft Owners and Pilots Association (AOPA). • Security zone: provide much more information to the boating public so that they comply. • Identification: use same identification required by the Transportation Security Administration (TSA) when boarding a commercial flight. • AIS : strongly opposed for	• Agreed with points addressed by Richard Schwartz. • Need increased education of the boating public over government regulation. • Supported strong efforts to have recreational boaters report on suspicious activity, similar to the program at airports. • National licensing of recreational boaters would do little to improve homeland security.	• Many boaters are not aware of the threat posed by terrorists using small vessels. • Risk assessment: • Conduct a formal risk assessment to better understand the level of deterrence needed and the amount of resources required • Current assessments do not address the threat of foreign-owned pleasure craft, which pose a greater threat than U.S.-owned vessels. • Implement a real-time reporting system for stolen vessels over 20 feet in length. • Develop a system to track vessels similar to the one implemented in the National Capital Region	• Protect ports and waterways without overly restricting the boater or damaging the maritime industry. • Security concerns: vessel and personal identification; lack of resources; unmonitored access points; and risk that theft of vessels could go unnoticed for long periods. • Issues for security measures: effectiveness, available implementation resources, economic viability, timely implementation, effects on financial stability of maritime industries, and public acceptability. • Expand AWW outreach to: public facilities, yacht / fishing clubs, boat leasing/rental facilities, and marinas.	• Balanced approach to security. • Build on existing programs before implementing new ones. • Provide adequate funding for the USCG, USCG Auxiliary, state boating enforcement personnel, and the AWW program. • Support the National Association of State Boating Law Administrators (NASBLA) "Partners on the Water" • Identify and engage new stakeholders. • USCG should work with the Association of Marina Industries (AMI) to educate marina operators about security risks. • NMMA could expand outreach for the AWW program.

Richard Schwartz	James Browning	Earl M. Waesche	James P. Muldoon	Cindy Squires
recreational boaters. • Potential terrorists would not comply with AIS. • Adding millions of recreational vessels would overwhelm the USCG ability to effectively monitor vessels. • Prohibitive equipment cost. • Recommends that the Captains of the Port (COTP) serve as the connection between the USCG and commercial / recreational vessel operators. • Create a nationwide Coast Guard alerting Maritime Mobile Service Identity (MMSI).		(NCR) to track general aviation. • AWW programs have lost momentum and need to greater media attention. • Licensing: not the solution because it is expensive and ineffective as prospective terrorists would be able to obtain boating licenses legally. • Identification: use a boating education certificate or driver's license.	• Identification: use driver's license / state-issued identification. • Expand public service announcements for security awareness. • Require on board radio or a cell phone. • Add safety / homeland security information to mailings sent to small vessel owners. • Provide boat decals with: general security information and suspicious activity reporting procedures. • Use RFID for passive vessel identification. • Increase maritime patrols.	• Publicize in the NMMA Boat Show Directory • National Marine Day – could include an AWW program and invite USCG representatives. • Security zones: should be limited to critical areas, be well marked, charted and patrolled. • Identification: against any new types of identification. • AIS: should not apply to recreational boaters.

The second panel discussion shifted the focus to commercial aspects of the small vessel community.

Panel II: Commercial Vessel Interests

Ms. Emily Reiblein – American Waterways Operators

Ms. Reiblein works for Moran Towing Corporation and represented the American Waterways Operators (AWO), a national trade organization for tug boat and barge operators in the United States. The AWO represents over 400 member companies that account for more than 80 percent of the U.S. fleet. In her remarks she indicated that there are three key concerns particularly relevant to her association membership:

- Hijacking a vessel and ramming it into critical structure or another vessel;
- Hijacking a vessel in order to cause substantial disruption to port and/or city commerce; and
- Hijacking a vessel for use in escaping after a terrorist attack or other criminal activity.

Ms. Reiblein explained what her industry does to prevent security breaches and suggested that many of the concepts could be adopted by the broader boating community to deter terrorism. She recommended relying on the tug boat and barge operator industry as the first line of defense on the waterways, as their captains are able to note changes in the harbor more than other individuals due to their familiarity with the particular harbor. In addition, she stressed the concept of no "free access" in terms of making their industry a less attractive target to terrorists and criminals by implementing simple security measures such as installing gates and adding lights around docks.

Moreover she advocated identification matches and searches during all Maritime Security (MARSEC) levels.[57] Ms. Reiblein further suggested that all crewmembers be required to go through formalized security training with onboard testing. Lastly, she recommended quarterly and annual exercises to include an explanation of MARSEC levels; vessel / facility security plans; recognition and detection of suspicious individuals, activities, substances and devices; search and screening procedures; response and reporting procedures; communication protocols; and security and navigation equipment use and maintenance.

[57] The Coast Guard has a three-tiered system of Maritime Security (MARSEC) levels which parallels with the Department of Homeland Security's Homeland Security Advisory System (HSAS). MARSEC levels are designed to readily communicate changes in security conditions, triggering pre-planned scalable responses. The Commandant of the U.S. Coast Guard sets MARSEC levels to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the U.S.

Captain James Ruhl – Commercial Fishermen of America

Captain Ruhl stated that he has spent nearly his entire life as a member of the commercial fishing industry and is a founding member of the Commercial Fishermen of America (CFA), a new national organization founded by and for commercial fishermen. He indicated that the commercial fishing industry is one of the nation's oldest professions, that its members are fiercely independent, and that they provide a great service to the country. In regard to tracking requirements, Captain Ruhl was concerned about the high cost of the equipment and the lack of competition among vendors that keeps costs of such equipment artificially high. He also had concerns with the Vessel Monitoring System (VMS)[58] and AIS because these technologies do not tell who is on a vessel nor the speed or intent of the vessel. He suggested that codes be developed so that vessel operators could be able to communicate with authorities in a way that an infiltrator on a vessel would not understand. Captain Ruhl implored authorities to treat the commercial fishing industry as equals. He stressed that it is important to "get the relationship right" as the industry covers the entire country and they can be additional sets of eyes and ears for the homeland security community. Lastly, he repeated the idea widely held throughout the NSVSS, that the AWW needed to be expanded.

A Coast Guard Maritime Safety and Security Team patrol boat escorts a vessel through the Brownsville Ship Channel. (photograph by Petty Officer 3rd Class David Schuhlein)

[58] A VMS system uses electronic transmitters, placed on fishing vessels that transmit information about the vessel's position to enforcement agencies via satellite. This allows someone on land, monitoring such transmissions, to determine if a vessel is in a closed area. There are several issues related to the implementation of VMS, including the variety of equipment types and associated costs, vessels' ability to carry VMS, VMS operating requirements, vessel coverage, and collaboration with traditional enforcement techniques.

Captain Edward O'Brien – National Association of Charterboat Operators

Captain O'Brien is the Vice President of the National Association of Charterboat Operators (NACO), which has a membership including maritime charterers who provide fishing, sailing, diving, eco-tours, and other excursion vessels for paying passengers. Captain O'Brien explained that requirements to implement the AIS system brought panic into the charter boat industry. He stated that NACO is opposed to AIS because the hardware is not yet fully developed and that it should be done right the first time. Moreover, he expressed that his industry is watching with great interest the results of ongoing AIS testing in Delaware because if it is not done right there, it will poison the minds of other stakeholders around the country.

Regarding the maritime threat from small vessels, Captain O'Brien emphasized that speed and spotter boats are the greatest concern, and that small vessels could be used as a diversionary tactic to divert authorities from the real target of an attack. He also called for an analysis of current licensing practices of commercial and charter boat vessels and suggested the possibility of an interim step for licensing to cover regions of the country that are totally devoid of licensing.

Captain Elizabeth Gedney – Passenger Vessel Association

Captain Gedney is the Director of Safety, Security and Risk Management for the Passenger Vessel Association (PVA). The PVA is a national organization representing approximately 600 member companies that operate passenger vessels, including owners and operators of dinner cruise vessels, sightseeing and excursion vessels, ferries, gaming vessels, as well as tour and overnight cruise vessels. Captain Gedney opened her remarks with a quote from a June 2004 statement made by then Deputy Secretary of Homeland Security ADM James Loy (ret):

> "Though no cost is as great as that of human lives lost, as we build and a explain new security paradigm to the country, we must do so while minimizing any negative impacts on commerce and insisting on good stewardship of the tax payer's invested dollar."[59]

This quote was an overarching theme of Captain Gedney's remarks, as she emphasized balancing security and commerce. She also expressed that all vessels do not pose the same level of risk and that a determination of risk for various vessels is crucial. Captain Gedney explained that operators must conduct risk assessments to determine the correct security measures. Moreover, she indicated that regulators must recognize the risk-assessment when conducting verification examinations. One of Captain Gedney's main points was to avoid "toothpaste tube thinking," as an overly stringent application of security screening standards does not always create more secure operations, and that operators should have leeway in implementing security measures. Lastly, she implored industry and government to work together to identify reasonable and appropriate security

[59] For a complete transcript of remarks of former DHS Deputy Secretary James Loy please visit the following site: http://www.dhs.gov/xnews/speeches/speech_0184.shtm

measures, retain customers, obtain new customers, provide new services, build more boats, and grow business.

Table 5: Panel II – Commercial Vessel Interests

Emily Reiblein	Captain James Ruhl	Captain Edward O'Brien	Captain Elizabeth Gedney
Works for Moran Towing Corporation and represented the American Waterways Operators (AWO)	Commercial Fishermen of America (CFA)	National Association of Charterboat Operators (NACO)	Passenger Vessel Association (PVA)
• Hijacking Concerns: • Hijacking a vessel and ramming it into a critical structure or another vessel; • Hijacking a vessel in order to cause substantial disruption to city and to commerce • Hijacking a vessel to escape from a terrorist attack or other criminal activity • Rely on tug boat and barge operators industry as the first line of defense – captains are able to note changes in the harbor more than other individuals because of their familiarity with the particular harbor activities • Make their industry a less attractive target to terrorists and criminals by implementing simple security measures – adding gates and lights around docks • Maritime Security (MARSEC) • Perform identification matches and	• Concerns: • High cost of the equipment and the lack of competition among vendors that keeps the cost of such equipment artificially high. • VMS and AIS –cannot determine who is on the vessel nor the speed or intent of the vessel. • Recommendations: • Develop code so that vessel operators would be able to communicate with authorities that an infiltrator on a vessel would not know. • Industry can be additional sets of eyes and ears for the homeland security community. • Expand AWW	• Concerned with AIS: • Hardware is not yet fully developed and that it should be done right the first time. • Industry is watching the results of ongoing AIS testing in Delaware – if not done right there, it will poison the minds of other stakeholders • Speed and spotter boats are the greatest concern – small vessels could be used as a diversionary tactic to divert authorities from the real target of an attack • Licensing: • Need analysis of current licensing practices of commercial / charter boat vessels • Suggested possible interim step for licensing to cover regions of the country that are totally devoid of licensing	• Implored industry and government to work together to come up with reasonable and appropriate security measures; • Overly stringent application of security screening standards does not always create more secure operations • Minimize any negative impacts on commerce – wants to retain customers; obtain new customers; provide new services; build more boats; and grow business • Operators should have leeway in implementing security measures • Risk issues: • Determination of risk for various vessels is crucial • Operators must conduct risk assessments to determine the correct security measures • Regulators must recognize the risk-assessment when conducting verification examinations

Emily Reiblein	Captain James Ruhl	Captain Edward O'Brien	Captain Elizabeth Gedney
searches at all levels • Require crew members to go through formalized security training with onboard testing. • Perform quarterly and annual exercises to include explanation of MARSEC security levels; vessel / facility security plans; recognition and detection of suspicious individuals, activities, substances and devices; search and screening procedures; response and reporting procedures; communication protocols; and security and navigation equipment use and maintenance			

The final panel discussion focused on the role of state and local law enforcement interests in the small vessel community.

Panel III: State and Local Government Interests

Lieutenant Colonel Don Holway – State of Florida

Lieutenant Colonel Don Holway is the Deputy Director of Law Enforcement for the Florida Fish and Wildlife Conservation Commission (FWC). The FWC is the primary waterborne law enforcement authority in Florida, with over 700 sworn officers. His presentation highlighted some of the initiatives the state of Florida has undertaken to address maritime security. He stated in Florida, waterborne issues have recently been considered within the state's Domestic Security Plan. This is important as agencies involved in waterborne security now have a seat at the decision making table and the funding process for waterborne security is considered a statewide priority. Lieutenant Colonel Holway stated that as waterborne security became a higher priority for the state, the FWC and their local partners received additional funding through the State Homeland Security Grant Program and the Law Enforcement Terrorism Protection Program grant process to acquire equipment to help them better secure the maritime domain. Despite these additional monies, personnel costs and operational costs for homeland security operations are still being paid from their core mission appropriations.

During his presentation Lieutenant Colonel Holway stressed that the overarching principle of Florida's strategic plan was to build upon existing plans that had been successful in addressing domestic security issues. He emphasized that funding should be used to increase existing law enforcement capabilities and capacities to enhance maritime security issues including the small vessel threat. An example of this is the Waterborne Response Teams (WRT) that are used to augment the USCG maritime security mission. These teams are composed of six members and one lieutenant and are the same officers who are on the water everyday performing law enforcement patrols. Teams are assigned to one of seven Task Force Regions throughout the state and assist the USCG with perimeter security, exclusion zone enforcement, and tactical operations. Multi-tasking of patrols by law enforcement officers with adequate training to make operations seamless was a major theme of Lieutenant Colonel Holway's presentation.

In addition, Lieutenant Colonel Holway focused on the use of technology to enhance Maritime Domain Awareness. Some of this technology includes AIS, offshore radar, and infrared / video camera systems. He explained that the technology already exists to place transponders on law enforcement vessels and to overlay that information on a radar grid. This allows for efficient management of assets during routine patrols as well as emergency responses. Lastly, similar to previous panelists, Lieutenant Colonel Holway expressed that there is a need to expand the AWW program to help fill gaps in law enforcement patrols.

Major John C. Fetterman – State of Maine

Major Fetterman currently serves as Vice President of the National Association of State Boating Law Administrators and for the last 30 years has been a patrol officer for the State of Maine. He stated that many of his officers have spent nearly 20 years at a single coastal port and their knowledge of their home port is a significant factor in identifying illicit small vessel activities. When a strange or seemingly out of place vessel enters a maritime community, it will attract the attention of his officers.

Major Fetterman was concerned that occasional requests to assist the USCG have evolved into a routine operational occurrence for state maritime law enforcement agencies. He stated that his officers backfill for traditional USCG calls for service, assist with search and rescue, and augment security missions. Major Fetterman stated that this practice has essentially become an unfunded mandate, as Maine is forced to use dedicated funds to assist the USCG with maritime security. He further noted his opinion that DHS has done little to support state marine security forces.

Major Fetterman also stated that Maine was the first state in the nation to enter into a Memorandum of Agreement (MOA) with the USCG for enforcement of safety and security zones. He recommended that other states enter into a similar MOA with the USCG as it promotes a comprehensive maritime law enforcement strategy and builds partnerships across jurisdictional boundaries. Another benefit of entering into an MOA with the USCG would be that agencies will be eligible and identified as sub-grantees under a comprehensive and standardized security program. He stressed that the farther the borders are pushed out through prevention partnerships, the safer our nation will be.

Lieutenant William J. Krul – St. Clair County, Michigan

Lieutenant Krul is the Commanding Officer of the Marine Division of the St. Clair County Sheriff's Department in Port Huron, Michigan. His responsibilities include the overall administration and command of the marine division (law enforcement unit and dive/rescue recovery unit). Lieutenant Krul began his statement by explaining the threat posed by terrorists to the Great Lakes region, specifically the International Bridge between the United States and Canada and the locks system in Sault St. Marie, Michigan. He explained that a successful attack against these targets would result in serious economic hardships, shut down waterways and bridges, and cause loss of life.

Lieutenant Krul expressed, as did others on the panel, that maintaining control of hundreds of miles of waterways is beyond the means of existing law enforcement in terms of manpower and budget. He stated that maritime law enforcement patrols by Federal and local agencies are spread thin and that there is no certainty of around the clock protection. Lieutenant Krul further explained that most of the training that his officers receive is on how to deal with safety regulations and not homeland security concerns. In his remarks, he indicated that their security level is not much more than a "plug in a dike ready to burst."

Lieutenant Krul indicated that the current goal of law enforcement is to provide periodic but irregular patrols in order to produce uncertainty of presence to any terrorist. Patrols

are maintained, but the region is so vast that it cannot be patrolled as regularly as is desired given current manpower, funding, and training. In an effort to increase presence, cameras are being set up to watch for suspicious activity and periodic hidden surveillance also takes place. In addition, Integrated Border Enforcement Teams and Joint Operations Teams meet on a regular basis to share information to assist with security.[60] Moreover, Riverwatch and Waterway programs have been initiated to enlist local citizens in informing law enforcement officials of suspicious activity.

Sergeant James W. Lambert – Alameda County, California

Sergeant Lambert is the supervisor of the Alameda County Sheriff's Office Marine Patrol Unit and Commander of the 85-foot fast boat ALCO-85. Sergeant Lambert first described the structure of the Neptune Coalition, which is a program to bring together the resources of approximately 30 different agencies in a concerted effort to enhance the safety and security of the ports and the general public within the San Francisco Bay and River Delta Area. He went on to describe experimental efforts by the Lawrence Livermore National Laboratory and the Naval Postgraduate School to detect sources of radiation on the water. Sergeant Lambert emphasized the importance of partnerships, cooperation with all stakeholders, and information sharing, although he noted that such cooperative efforts were often personality driven and labor intensive.

[60] The Integrated Border Enforcement Team (IBETS) program is a Department of Justice sponsored multi-faceted law enforcement initiative comprised of both Canadian and American partners. This bi-national partnership enables the five core law enforcement partners involved in IBETS to share information and work together on a daily basis with other local, state and provincial enforcement agencies on issues relating to national security, organized crime and other criminality transiting the Canada/US border between the Ports of Entry (POE).

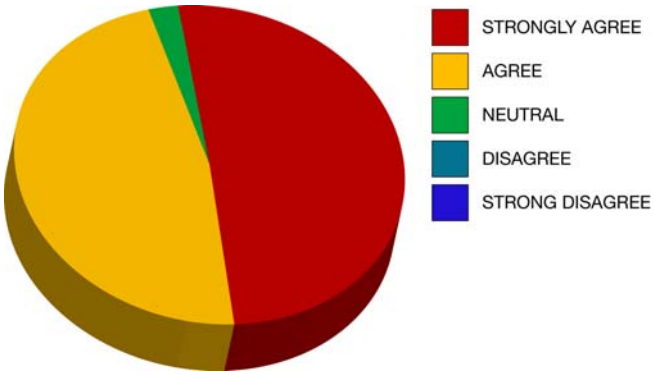
Table 6: Panel II1 – State and Local Law Enforcement Interests

Lieutenant Colonel Don Holway	Major John C. Fetterman	Lieutenant William J. Krul	Sergeant James W. Lambert
Deputy Director of Law Enforcement, Florida Fish and Wildlife Conservation Commission (FWC)	Vice President of the National Association of State Boating Law Administrators and a patrol officer for the State of Maine (30 years)	Commanding Officer of the Marine Division, St. Clair County Sheriff's Department in Port Huron, Michigan	Supervisor of the Alameda County Sheriff's Office Marine Patrol Unit
• State of Florida has undertaken initiatives to address maritime security within the state's Domestic Security Plan. • Principle: build upon existing successful plans that address domestic security issues and • Enhance existing law enforcement capabilities and capacities: • Waterborne Response Teams (WRT) that are used to augment the USCG mission • Multi-tasking of patrols by law enforcement officers with adequate training to make operations seamless • Use of technology to enhance Maritime Domain Awareness: AIS, Offshore radar, and Infrared / video camera systems. • Expand AWW program to help fill gaps in law enforcement patrol	• Concern: occasional requests to assist the USCG have evolved into a routine operational occurrence for state maritime law enforcement agencies • Unfunded mandate: Officer's backfill for traditional USCG calls for service, assist with search and rescue, and augment security missions • Recommended that other states enter into a single MOA with the USCG • Promotes a comprehensive maritime law enforcement strategy and builds partnerships across jurisdictional boundaries • Agencies will be eligible and identified as sub-grantees under a comprehensive and standardized security program	• Location: Great Lakes region, specifically the International Bridge between the United States and Canada and the locks system in Sault St. Marie, Michigan • Current goal: provide periodic but irregular patrols in order to produce uncertainty of presence to any terrorist – region too vast to patrol regularly • Officer training mostly deals with safety regulations, not homeland security concerns • Suspicious Activity Reporting: • Cameras are being set up • Riverwatch and Waterway programs have been initiated for local citizens • Periodic hidden surveillance also takes place • Information sharing: Integrated Border Enforcement Teams and Joint Operations Teams, meet on a regular basis	• Neptune Coalition: resources of approximately 30 different agencies within the San Francisco Bay and River Delta Area • in a concerted effort to enhance the safety and security of the ports and the general public • Experimental efforts by the Lawrence Livermore National Laboratory and the Naval Post Graduate School to detect sources of radiation on the water • Emphasized the importance of partnerships, cooperation with all stakeholders, and information sharing

Stakeholder Views of Panelists

Stakeholders at the NSVSS were very complimentary of the panelists at the Summit. Respondents to the post-Summit survey indicated that speaker's spoke to issues that were important to them, provided valuable information regarding the small vessel threat, stimulated discussion, and provided important insights into small vessel security issues. Below are results taken from the post-Summit survey:

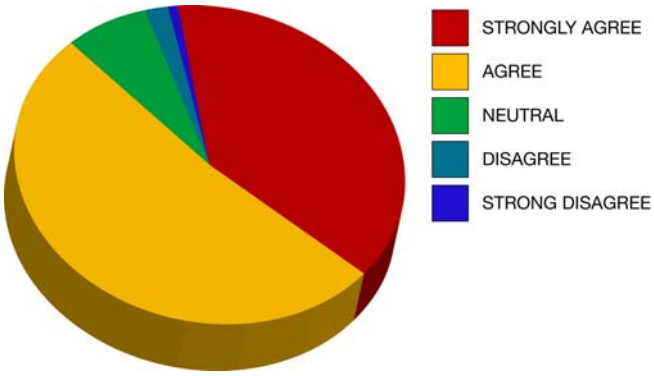
The speakers spoke on topics that were important to me.



All Respondents (*n = 174*)

Strongly Agree	50.6 percent	(87)
Agree	47.1 percent	(81)
Neutral	2.3 percent	(4)
Disagree	0.0 percent	(0)
Strongly Disagree	0.0 percent	(0)

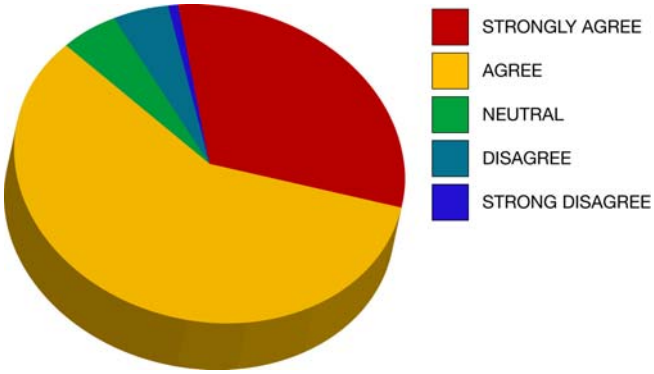
The speakers provided valuable information regarding small vessel security.



All Respondents (*n = 174*)

Strongly Agree	35.6 percent	(65)
Agree	48.3 percent	(91)
Neutral	6.8 percent	(11
Disagree	1.8 percent	(3)
Strongly Disagree	0.6 percent	(1)

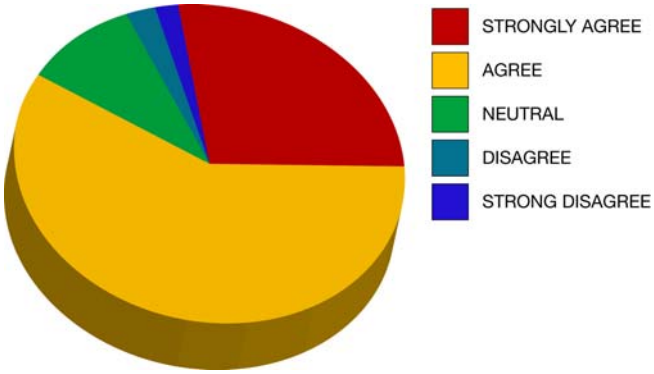
The panels stimulated important discussion regarding small vessel security.



All Respondents (*n = 172)*

Strongly Agree	30.8 percent	(53)
Agree	58.7 percent	(101)
Neutral	5.2 percent	(9)
Disagree	4.7 percent	(8)
Strongly Disagree	0.6 percent	(1)

The panel discussions provided insight important to small vessel security issues.



All Respondents (*n = 170*)

Strongly Agree	26.5 percent	(45)
Agree	59.4 percent	(101)
Neutral	10.0 percent	(17)
Disagree	2.4 percent	(4)
Strongly Disagree	1.8 percent	(3)

V. STAKEHOLDER FEEDBACK AND FINDINGS

Listed below are the major issues and themes discussed by stakeholders during the question and answer sessions following the speeches, panels, and during breakout sessions at the Summit. Responses to the post-Summit survey were also included in this section of the report. The following major points are qualitative and do not represent solicited consensus or the priorities of any particular stakeholder group and are not in order of priority.

Small vessel stakeholders representing recreational, commercial, and government interests listen to a speech at the Summit.

Develop a national strategy

There was a reoccurring theme at the Summit on the need for the development of a coherent National Small Vessel Security Strategy based on a layered-security approach. Although many attendees advocated a national strategy, they stressed that it must be appropriate to the threat and not overly intrude on personal liberties or cause undue economic burdens. Participants insisted that security solutions called for in the national strategy strengthen ongoing successful initiatives before introducing any invasive, burdensome, expensive, or untested approaches.

This national strategy should also include an international solution for partnering with other countries to detect threats before they depart in order to engage the threat before it enters the U.S. maritime domain. This is specifically important when reducing the risk from WMD threats.

Participants advocated a multi-option strategy that addresses the unique characteristics of various ports, waterways or coastal areas rather than a “one size fits all” strategy. The

sense was that stakeholders be given options that meet a recognized federal standard so that security measures could be implemented to best fit local circumstances and vulnerabilities in a flexible way, taking into account changing threats and risks.

Stakeholder view of the small vessel threat

Among stakeholders there was general agreement that at the present time it would be relatively easy for a terrorist organization to acquire or commandeer a small vessel to conduct a terrorist attack against the United States. Of primary concern are vessels under 30 feet in length that travel at high rates of speed. Once such vessels are detected during the execution phase of an attack, law enforcement authorities would not have enough time to respond or prevent the attack.

Overall, commercial vessels were viewed as less of a terrorism threat than pleasure craft. The recreational boating community was thought by many stakeholders to be less regulated and diffuse than the commercial vessel sector making it more difficult to monitor. Stakeholders from the commercial boating sector indicated that their communities tend be small and well connected, which increases the likelihood that they would recognize suspicious individuals. Moreover, members of the commercial vessel community indicated that they are on the water everyday as part of their profession, thus increasing the probability that they would notice and report suspicious activity.

Another major concern among attendees at the Summit was that terrorists would be more likely to acquire small vessels to be used in attacks from foreign countries in close proximity to the United States (i.e., Canada, Mexico or the Caribbean). Foreign countries were considered to be a more advantageous location for terrorists to launch attacks from due to weaker regulations in those countries, the fact that the terrorists would never have to enter the United States prior to the attack, and that only a short distance would need to be crossed before an attack commenced.

Several respondents thought there was too much emphasis placed on major coastal ports as opposed to inland waterways and the thousands of miles of open coastline. For example, some respondents felt that inland waterways are wide open to attack and that such an attack would have a devastating psychological impact, emphasizing vulnerability even in the heartland of the country. Other attendees indicated that that there is virtually no security along coastlines making these areas the most vulnerable to attack.

Employ risk assessment-based measures to best determine actions and allocate resources

In order to be credible to the stakeholders who must be engaged as partners, they repeatedly stated that DHS needs to conduct and convey systematic risk and threat assessments, on an ongoing basis. Three types of assessments were considered necessary:

- further define the threat to improve public awareness and guide funding;
- determine specific security needs; and
- gauge the threat to the country from small vessels acquired in foreign countries.

Multiple stakeholders suggested that formal risk/threat assessments are needed to determine the likelihood of different types of small vessel attacks, the financial implications of attacks on various ports and waterways, and to identify which targets are most likely to be attacked. Such assessments, if openly communicated, would provide awareness to the boating public of the ongoing terrorist threat and guide funding to prevent and mitigate such attacks.

As mentioned, several attendees stated that marinas and ports around the country are unique, so that one universal solution to solving their security needs is unrealistic. Instead of being presented with one security model, they suggested that marinas and port operators be given several options (through federal guidance) that meet a recognized standard. Then marina and port operators could choose the options most applicable to their specific needs. In order to do this, risk assessments need to be conducted at each marina and port to determine their specific needs.

There was also general agreement among participants that small vessels acquired in foreign countries were considered a greater threat to U.S. national security than vessels in the U.S. maritime domain. Stakeholders recommended that a risk and threat assessment be conducted specifically to assess the probability of such attacks and identify what should be done to prevent and mitigate such attacks.

Balance the trade-offs between freedom, security, and economy

Balancing the need to increase security in a post 9/11 world with individual freedoms and economic sustainability was a major theme at the NSVSS. Members of the recreational boating community were especially concerned about this issue. They indicated that restrictive regulations imposed by the federal government on boaters and small vessels will do little to improve national security and will likely alienate the very community from which assistance is essential. As expressed by one attendee, “if government policies and regulations negatively impact economic growth and personal liberties, then the terrorists have won without even committing an attack.”

In addition, the recreational boating community was concerned that new regulations and fees will have a deleterious impact on the sale and rental of recreational boats, possibly causing some companies to lay-off employees or go out of business. Their fear is that as regulations and fees increase for boating, the general public will spend their money on other recreational activities that are more convenient, affordable, and accessible. Essentially, if boating becomes an activity filled with inspections, checkpoints, blocked access, and high costs (equipment and fees), boaters will find other things to do with their leisure time.

Build a culture of partnership and trust within and across the boating community

There was near universal consensus among stakeholders that they are eager to participate in the common security of the country and to work with DHS as well as state and local

government entities as long as they are treated as "partners" and "allies" and not as "adversaries." Simply stated, the small vessel community wants to be acknowledged as part of the solution and not part of the problem.

To alleviate some of the concerns of small vessel operators, authorities must be sensitive to local stakeholder interests and conduct operations in a way that generates trust. It was expressed by one stakeholder that small vessel operators are not all "bad until proven good."

U.S. Coast Guard units deployed to Ohio to assist flood victims. (U.S. Coast Guard photo)

The call for authorities to treat mariners with respect went beyond just U.S. citizens but also to foreign merchant sailors. The sentiment here was that if U.S. authorities treat foreign merchant sailors with dignity and respect, it would encourage them to report suspicious individuals or activities.

It was expressed on numerous occasions at the Summit that one of the best ways for DHS and the USCG to build trust with the small vessel community was for authorities to provide feedback to boaters who report suspicious activities. Small vessel operators want to know that the information they provide is appreciated and is being used by law enforcement authorities. Moreover, by letting boaters know that they have helped and that their vigilance is appreciated by law enforcement further encourages continued reporting on suspicious activities from small vessel operators.

A reoccurring theme among stakeholders at the Summit was that constant turnover of USCG personnel seriously impedes relationship building with the small boat community. To partially remedy this claim, several stakeholders recommended that the Coast Guard Captains of the Port (COTPs) serve as the link between the USCG and the commercial and recreational vessel operators. Stakeholders also suggested that the COTP be given responsibility to develop grassroots programs that include members of the Coast Guard

Auxiliary, U.S. Powerboat Squadrons, the non-emergency assistance towing fleet, marina operators, the general boating public and the commercial sector. Some attendees strongly recommended that the USCG should require that each COTP have a written understanding with all maritime law enforcement agencies in their area that identifies their various roles and responsibilities. In addition, stakeholders want DHS to consider creating an Advisory Group with members of the small vessel community.

Another suggestion by the small vessel community was that law enforcement increase partnerships by reaching out to non-traditional stakeholders such as marine bankers, boat dealerships, and members of the insurance industry. A partnership with marine bankers was suggested because they could assist in identifying stolen vessels and suspect purchases. Boat dealerships and the insurance industry were identified because they might be able to provide safety materials to boat owners when they purchase their vessel or their insurance policies.

Perhaps the two mostly widely stated trust-building measures advocated by the small vessel community were for DHS and the USCG to continue reaching out to stakeholders beyond the Summit and that they take substantive actions on stakeholder suggestions. Stakeholders expressed their desire to be kept in the decision making process so that they can remain involved. To do this, they recommended having regional small vessel conferences similar to the NSVSS and that a web site be developed so that the small vessel community could provide ongoing input and receive information from DHS.

In a move to emulate the success and openness of the NSVSS, several attendees suggested that recreational and commercial boating stakeholders as well as other small vessels interests, get together on their own to further understanding of each others concerns and interests.

Establish Funding Streams

There was broad agreement at the Summit among all stakeholder groups that adequate funding and resources for the U.S. Coast Guard, USCG Auxiliary, state, local, tribal, and territorial boating law enforcement authorities, as well as emergency response elements is critical to ensuring the security and safety of the nation's ports, waterways, and coastal areas.

In light of this overarching consensus, state and local law enforcement representatives at the Summit indicated that homeland security missions have become unfunded mandates which drain their budgets and negatively impact other public safety and security operations. This sentiment was best expressed by one state and local government stakeholder at the Summit in the following statement: "DHS cannot expect state and local government to provide homeland security patrols and training unless DHS provides funding support."

State and local law enforcement stakeholders stressed that any federal funds allocated towards this mission should be used to build upon existing capabilities and capacities that have been successful in addressing maritime security issues in the past. Essentially, new funds for the homeland security mission should serve the dual purpose of increasing

safety as well as protecting the nation from terrorist attacks. This constituency also emphasized that minimal security and participation standards need to be established before law enforcement agencies should receive DHS grant money.

Enhance coordination, cooperation, and communications between federal, state, local, tribal, and territorial agencies

Stakeholders noted a variety of issues related to coordination, cooperation and communications that require resolution. With regard to training, several members of the law enforcement community expressed that there is a lack of training on how to interdict criminal maritime activities and equipment for tactical operations. They indicated that most of the training conducted by state and local marine law enforcement is directed toward safety regulation enforcement and not the homeland security mission.

A Coast Guard rescue crew assists vessel that was disabled in a storm (U.S. Coast Guard photo by Petty Officer 2nd Class Kip Wadlow)

Moreover, law enforcement entities indicated that periodic training drills and exercises are desperately needed to address shortcomings in homeland security as well as response and preparedness in the maritime domain. The training is not just needed to prevent and respond to terrorist attacks but to address the wide range of non-terrorist threats such as maritime disasters brought on by man-made (e.g., oil spills) and natural causes (e.g., hurricanes).

To address some the above mentioned concerns, members of state and local law enforcement agencies proposed that training should be interagency and cross-jurisdictional to include the USCG and other federal agencies; state, local, tribal, and territorial law enforcement agencies; and even members of the private sector so that

tactical coordination and operational skills can be developed and professional relationships fostered.

State and local law enforcement attendees also expressed a need for a minimal threshold of qualification and equipment standards for all marine officers across the nation.

Improve intelligence, analysis and dissemination

There was broad agreement among stakeholders at the Summit that the timely acquisition of intelligence, and the ability to act on it during the planning stages leading up to an attack is one of the best ways to prevent a waterborne terrorist attack. Most stakeholders indicated that once a waterborne terrorist attack was in the execution phase, it would be virtually impossible to stop because authorities would not have enough time to respond even if the attack were detected.

Attendees further stressed that one agency working by itself is not enough to ensure the safety and security of a major port, waterway, or coastal area. To have a better opportunity to stop a terrorist attack in the planning stages, a broad spectrum of stakeholders called for the development of fusion centers to better share, analyze, and disseminate intelligence. Stakeholders recommended that these fusion centers be fully funded and staffed by personnel from DHS, the Department of Defense (DoD), Harbor Master, and state, local, tribal and territorial law enforcement agencies. There was a general expectation at the Summit that fusion centers would improve communication, cooperation, and coordination among participating agencies.

Stakeholders also called for the development of a nationwide system to share information on stolen vessels in near real-time among all law enforcement agencies. Since the National Crime Information Center (NCIC) already indexes individuals and information on stolen vessels, several stakeholders wanted to ensure that all maritime law enforcement agencies put information on stolen vessels into this system and check suspect vessels against it.[61] However, stakeholders noted that any system used to index stolen vessels would be fallible because some recreational boaters use their boats so infrequently they might not notice a theft for days or even weeks.

[61] NCIC is a computerized index of criminal justice information such as criminal record history, fugitives, stolen properties, and missing persons. It is available to Federal, state, and local law enforcement and other criminal justice agencies and is operational 24 hours a day, 365 days a year. The purpose for maintaining the NCIC system is to provide a computerized database for ready access by a criminal justice agency making an inquiry and for prompt disclosure of information in the system from other criminal justice agencies about crimes and criminals. This information assists authorized agencies in criminal justice and related law enforcement objectives, such as apprehending fugitives, locating missing persons, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system. All records in NCIC are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include: restricting access to those with a need to know to perform their official duties, and using locks, alarm devices, passwords, and/or encrypting data communications. Data contained in NCIC is provided by the FBI, federal, state, local and foreign criminal justice agencies, and authorized courts.

Expand education and outreach to citizen stakeholders for a variety of safety, security, and trust-building purposes

One of the primary themes expressed at the Summit is that the general boating public is not sufficiently aware of the threat of terrorists using small vessels against U.S. national security. More must be done to encourage citizen participation and disseminate safety and security information.

There was near total unanimity at the Summit that the America's Waterway Watch (AWW) program needs to be expanded and reenergized. Many attendees indicated that the AWW needs a new implementation strategy, consistent support from senior USCG officials, and adequate funding as it is likely the best mechanism to reach the recreational boating public. Furthermore, stakeholders stressed that the AWW or similar program needs to be more than just a public awareness campaign; it also needs to a training program similar to a community watch program. In the cogent summary of one attendee, AWW should be more than "just passing out brochures at a conference."

As one stakeholder mentioned, "the AWW is a low cost program with a potentially high payoff." To publicize the AWW program, stakeholders recommended direct outreach by AWW representatives at yacht clubs, fishing clubs, boat leasing/rental facilities, marinas, and boat shows. They also had numerous other suggestions for outreach that included: intensifying public service announcements; placing advertisements in boating magazines; saturating ports, boatyards, marinas and boating stores with signs; placing notices in new-boater materials; having display booths at boat shows; and disseminating safety and security information through direct mailings sent out by government agencies and private organizations. In addition, one stakeholder suggested that each USCG District Office designate one officer as an AWW point of contact for additional information and follow-up.

One stakeholder recommended that the AWW adapt the "Lock Up. Look Out" program implemented by the Aircraft Owners and Pilots Association (AOPA). This program encourages private pilots to secure their aircraft, get to know their fellow hangar tenants, pilots, and aircraft owners, in an effort to prevent the possible theft or use of aircraft by potential terrorists.

In an effort to increase public participation and outreach to citizen stakeholders, one attendee advocated the resurrection of a version of the Office of Civilian Defense (OCD). The OCD was created during World War II so that cities could organize civil defense systems to mitigate a surprise attack from the Axis powers. Following the conclusion of the war this agency was terminated on June 4, 1945.[62] With the ongoing threat of terrorism, the stakeholder hoped that there might be millions of volunteers among the organized recreational boating, sport, and charter fishing communities to assist in safety and security.

[62] On May 20, 1941, President Franklin Roosevelt created the OCD so that cities could organize civil defense systems to mitigate a surprise attack from the Axis powers.

Improve situational awareness

At the Summit, attendees expressed positive interest in participating in programs to identify and report suspicious activities. Members of the commercial industry believed that they would notice suspicious activity more readily than members of the recreational boater community because they know other crew members in their profession and how commercial vessels typically operate in their domain. In addition, several attendees believed that commercial industry understood maritime security much better than recreational boaters; for example, there is currently no education for the boating public on maritime security (MARSEC) levels.

Some stakeholders recommended the TSA security awareness course as an effective training course to improve situational awareness. This security course could be modified to fit the needs of the recreational and commercial boating communities. Regardless of which educational campaign is chosen to improve situational awareness, it was strongly recommended that it be continuous and sustained in recognition of new boaters joining the community every day.

Improve and publicize mechanisms to report suspicious activities

There was a general stakeholder agreement that there is a need to develop standardized reporting mechanisms and contacts to alleviate confusion as to who should be contacted during emergency situations or to report suspicious activities. They recommended that a universal number (National Terrorism Hotline), similar to 911, a 1-800 number, or a *number, be adopted to report terrorist activities. The universal number should be kept simple as many boaters are not going to make a concerted effort to learn multiple numbers. Additionally, it was felt that this number should have appropriate filters that enable calls to be routed to those agencies in most need of the information.

Several stakeholders recommended that all new vessels have emergency numbers permanently installed on them by boat manufacturers. This number should be similar to decals currently placed on vessels to report oil and chemical spills to the National Response Center.[63] They also suggested that existing vessels have stickers placed on them with emergency contact information. Representatives from the AWW indicated that the latter is already being done to some extent.

Beyond devising a national terrorism hotline for boaters, attendees also recommended creating a nationwide USCG alerting Maritime Mobile Service Identity (MMSI). The development of such a system would enhance Digital Selective Calling to allow boaters to instantly alert the USCG of suspicious activities. Other stakeholders suggested that the USCG implement a secure channel for the boating community to send reports of suspicious activity directly to the USCG.

[63] The National Response Center (NRC) is the sole federal point of contact for reporting oil and chemical spills.

A member of the commercial vessel community at the Summit proposed another way to improve suspicious activity reporting. This stakeholder suggested that licensed Merchant Marine captains take an additional course in order to acquire a certification that would provide them with an identification number to be used when reporting suspicious activities. This identification number would help validate that a suspicious activity report was from a professional mariner, thus giving it greater credibility.

Improve Domain Awareness

There was considerable controversy over the role and status of the Automatic Identification System (AIS) at the NSVSS. Multiple representatives from the recreational boating industry were unequivocally opposed to applying AIS requirements to recreational boats. Their reasons for opposing AIS were extensive and substantial. Stakeholders from the recreational vessel community insisted that AIS should not be expanded for use beyond commercial vessels as it is too costly and impractical for recreational vessels. Moreover, they felt that a requirement to have AIS on small vessels would have a minimal effect on security as attempting to identify every vessel would be too expensive and difficult to monitor with current resources.

The commercial industry was also concerned about the cost of AIS. Several stakeholders expressed serious reservations about the cost of AIS for small vessel owners and cited a lack of competition among vendors that keeps the cost of AIS artificially high. Some stakeholders worried that the cost of purchasing vessel tracking systems like AIS could put them out of business.

Although AIS might be good for vessel identification, multiple stakeholders downplayed the role AIS would play in preventing a terrorist attack since terrorists might not comply with any requirement to install AIS or would disable it before an attack. Moreover, a representative from the law enforcement community reinforced the argument that requiring every private recreational boater to purchase an identifier or transponder does not make the maritime domain any safer as law enforcement does not have the capability to track all of those vessels. Some stakeholders indicated that they saw some limited applications for AIS and similar technologies in the vicinity of high value/high risk assets within limited geographic areas in a port or waterway.

While AIS was widely criticized as a means to track small vessels under 65 feet in length,[64] other alternatives were discussed. One proposal was to adopt a stripped-down, less expensive alternative such as the Vessel Identification System (VIS). VIS is a nationwide system for collecting information on vessels and vessel ownership to help identify and recover stolen vessels, deter vessel theft, and assist in deterring and discovering security-interest and insurance fraud. While VIS was recommended as an acceptable alternative to AIS, other stakeholders explained that nearly twenty years after

[64] The Maritime Transportation Security Act of 2002 currently requires AIS on certain commercial vessels 65 feet and greater, and the USCG is implementing regulations to comply with the Act.

legislation required the USCG to develop it, the system has not been fully implemented and future plans for development remain uncertain.

Some stakeholders pointed out that a short-term solution to identify vessels might be to implement a Radio Frequency Identification Program (RFID) for all boats. Installation of an RFID would allow law enforcement to passively identify vessels at stationary monitor points with minimal inconvenience to the boater. RFID would also allow suitably equipped boarding teams or law enforcement patrols to positively validate displayed hull registration numbers.

Another attendee encouraged small vessel owners to install real-time tracking and monitoring systems such as Sea-Watch Technologies on vessels to prevent theft and to speed return if stolen. It was noted that doing so had a positive impact on insurance rates for the boat owner.

Operator and vessel identification

A variety of views within and across stakeholder communities were expressed regarding operator certification, licensing, and vessel registration. Given the variety of state and local approaches to licensing, registration and identification requirements, some stakeholders are looking for DHS to provide guidance on these issues.

Certification

Several stakeholders from the commercial vessel sector were not opposed to credentialing but were concerned that inconsistent credentialing regimes in different jurisdictions around the country could result in inappropriate requirements and undue inconvenience for vessel operators. As one stakeholder expressed, “no two points of entry handle professional mariners the same way.” Some commercial vessel operators viewed the existence of different credentialing requirements from jurisdiction to jurisdiction more as federal, state and local government gambits to raise revenue rather than increasing safety and security.

Other stakeholders argued that the government should not continue to impose burdensome requirements on mariners or companies without demonstrating the benefits of these new programs. Transportation Worker Identification Credential (TWIC) cards were singled out as one such program by commercial vessel operators. They indicated that TWIC cards do little to increase port security as personnel are already required to possess numerous other forms of identification such as port identification, company identification, a state drivers license, in some cases a passport, and several other forms of identification. Several stakeholders pointed out that all of these forms of identification were required even before the advent of the TWIC card.

Members of the yachting community were critical of inconsistent interpretations of the Code of Federal Regulation (CFR) and U.S. Customs and Border Protection (CBP) policies that apply to large yachts in various USCG districts, sectors, and ports. For example, the USCG may require a 96-hour Notice of Arrival for foreign-flagged vessels under 300 gross tons while another port in the same district does not. Similarly, some

CBP officials familiar with yachts may inform a crew that a B1/B2 visa is appropriate while another CBP official in a different port demands a C-1/D visa. As a result, stakeholders from this sector indicated that crews are barred entry and their jobs are often put at risk. In extreme cases, their careers might even be placed in jeopardy when one customs official failed recognize what others have accepted previously. Members of this industry plead with decision makers to recognize this sector of the maritime industry, determine where they fit in the interpretation of regulations, and then educate sector-level officers on enforcement requirements.

Licensing

The issue of licensing was a contentious. Many stakeholders and panelists from the recreational boating community expressed the view that licensing is too expensive, is an intrusion on their personal liberties, and is ineffective in preventing terrorist attacks. Members of this constituency stressed that boaters should not have to procure any new type of identification or be treated any differently than automobile drivers or airline passengers. They also stated that if licensing is required, that it should only be required for operators and not for passengers. Moreover, they expressed that licensing would only create additional administrative overhead and not necessarily increase safety or security since terrorists might not take the time or effort to acquire a boating license.

Although a negative view of licensing was widely expressed among members of the recreational boating community, it was not universally held among stakeholders at the Summit. Other stakeholders suggested that requiring identification for recreational boat operators might be acceptable as long as it was an existing driver's license or other identification accepted by the TSA rather than another, new identification credential. In addition, still other stakeholders indicated that nationwide licensing of recreational boaters could ensure a minimal competence for all boaters' with a resultant increase in boater safety.

As no national licensing standard for small vessel operators currently exists, stakeholders recommended two provisional solutions to the licensing dilemma. The first recommendation would be to require all boaters to carry their driver's license or other state issued identification while on the water. The second recommendation would be for states to add a boat operator endorsement, similar to those required to operate a motorcycle or school bus, to their driver licenses. Some stakeholders also suggested that a boater could be required to complete an approved boating safety and security course before acquiring this endorsement.

Vessel Registration

Similar to licensing, the issue of vessel registration was another controversial topic at the NSVSS. Several government stakeholders advocated the development of a nationwide database of U.S. numbered and documented vessels to be used by federal, state, and local law enforcement authorities to access boat registration information across the country. They also expressed a need to have uniform boating registration standards, as the current standards differ from state to state.

Other attendees did not support the concept of a national small vessel registry. They felt that such a database likely would not make the nation more secure because a terrorist bent on conducting an attack would not bother to register a vessel.

If a nationwide boat registration system is mandated, one stakeholder recommended that it be modeled on motor vehicle registration (MVR) databases. State MVR databases are sophisticated and generally accessible by any authorized local, county, state or federal enforcement agency. Furthermore, MVRs are well maintained increasing data accuracy. Boat registration database designs would need to consider interoperability to ensure that they are accessible to the many, varied law enforcement agencies across the country.

Enhance International Cooperation

There was widespread agreement that a strong regime of international agreements and cooperation is needed to intervene at the earliest opportunity and defeat small vessel threats before they reach U.S. waters. Stakeholders indicated that it is important to work with other countries to encourage them to deploy security systems, share intelligence information, and check vessels for weapons and people of interest before they depart for the United States.

CARIBBEAN SEA (Nov. 17, 2004)--During Exercise CHOKEPOINT '04, A boarding team from the Coast Guard Cutter Harriet Lane, along with technical advisors from the U.K., Netherlands and France are delivered by a British Royal Navy small boat to board a simulated Liberian motor vessel believed to be carrying material to be used in the development of weapons of mass destruction. This Proliferation Security Initiative (PSI) exercise involved 19 nations and focused on improving information sharing and interdiction capabilities in an effort to prevent the proliferation of WMDs and the material required to make them. (USCG photo by PA3 Stacey Pardini)[65]

Attendees specified that they want the U.S. government to enhance international cooperation, particularly with countries in close proximity to the United States (i.e., Canada, Mexico and nations in the Caribbean). In addition, they recommended that the United States reach out to other countries to determine their best practices for

[65] http://cgvi.uscg.mil/media/main.php?g2_itemId=98775

preventing terrorist attacks via small vessels. Lastly, attendees backed developing a system to obtain information from foreign port facility directors so that it can be analyzed by U.S. authorities.

Employ technologies and develop effective operational procedures to detect radiological and nuclear threats

There was widespread consensus among stakeholders to use radiation detectors, but concerns were raised about device and operational effectiveness. Several stakeholders mentioned that the detection of radiological materials overseas and their interdiction is the single most important issue facing federal law enforcement agencies. To highlight the engagement, commitment, and patriotism of the stakeholders at the Summit, multiple stakeholders volunteered to place detectors on their vessels to help prevent a WMD attack.

Several attendees indicated that the key to preventing a cataclysmic WMD attack is to place the sensors on buoys as far out as practical to detect boats with radiation signatures, thus increasing available reaction time. One breakout group indicated that placing sensors as far as possible might cause the premature detonation of WMD by terrorists following detection. However, the detonation of a WMD several miles off the coast of the United States would be preferable to its detonation near a major U.S. population center, which could result in a massive loss of lives.

Some stakeholders also recommended that state and local law enforcement agencies and other first responders be provided with RAD/NUC devices for use while inspecting both vessels and cargo containers. As state and local law enforcement agencies have limited budgets to purchase portable or vessel mounted radiation detection devices, they suggested that the federal government provide funding for this equipment.

Despite widespread support for the use of nuclear detection devices, attendees from some ports were skeptical that RAD/NUC detectors would work in every port. They indicated that the layout of some ports would make it difficult to detect a nuclear device far enough out to make a real difference due to the inherently wide access to some ports. In addition, some port representatives indicated that their ports do not have natural choke points where detectors could be placed, further minimizing their effectiveness.

Reassess Security Zones

There were divergent views among stakeholders at the Summit as to whether or not security zones around vessels, ports, and other critical infrastructure should be publicized or if they should be expanded to allow authorities more time to take effective action after determining hostile intent. It was noted that resizing security zones may be impossible at certain ports where the main channel is near critical infrastructure or vessels.

According to several stakeholders, security zones should be charted, clearly marked with markers and buoys, and patrolled to make waterside targets less attractive to attack. Multiple members of the recreational boating community also supported the expansion of security zones as this is one area of security that recreational boaters are familiar with. In

addition, they suggested that expanding security zones would meet with little criticism from the recreational boating community as long as the areas are selected with some moderation.

Conversely, other attendees at the NSVSS disagreed with publicly disseminating security zone information to recreational boaters as providing such information to the general public might tip terrorists as to which targets are more important to attack than others.[66]

Other attendees countered this argument by stating that potential terrorists would be able to determine high priority targets regardless of whether or not security zones were publicized. Terrorists could acquire this information by other means (e.g., Internet, surveillance, word of mouth, media, etc.).

Regardless of the above mentioned stakeholder views on security zones, there was general consensus that any increase in security zones would also require a corresponding increase in security personnel to patrol the expanded areas. There was also widespread agreement that more must be done to bring about a "cultural change" among recreational boaters, since many boaters feel they can go wherever they want regardless of whether a security zone is marked or not.

Two stakeholders advocated additional measures to prevent boaters from violating security zones. The first proposal was is to make violations of maritime security zones not only a civil penalty, but a potential criminal penalty as well. The second measure proposed was to allow authorities to check boat registration, ownership and identification for any individual violating, closely approaching, or conducting surveillance of targets near security zones by identifying such activities in law as 'probable cause.'

Despite the general discussion, there was considerable confusion as to what security zones are and what they are intended to achieve, thus additional boater education and awareness is necessary.

Other Participant Views

Several attendees noted that implementing common sense security measures that protect against danger, loss, or theft will also deter terrorists from stealing vessels or trespassing at marina or port facilities. This could mean reducing "free access" to maritime vessels or marinas and port facilities to authorized personnel. Other dual purpose security measures included installing security devices such as lights, fences, locks and surveillance equipment to make small vessels less attractive to potential terrorists.

Several law enforcement participants also pointed out that the more a target is hardened, the less likely it is that the target will be attacked, as terrorists would most likely seek a softer target. Other stakeholder ideas to harden targets included: using fixed and floating barriers (booms or floats); installing sensors on barriers; and using long range cameras. Also, since critical infrastructure facilities on the shoreline are vulnerable to attack from

[66] It should be noted that Security and Safety Zones are enacted via regulation and are published in the Federal Register, making the issue of publication moot.

both land and sea, some attendees recommended deployment of security assets, not only at the front gate, but also out on the water.

Law enforcement participants also emphasized that "good police work" is more important than technology. In particular, a visible law enforcement presence serves as a strong deterrent. Terrorists should believe that "law enforcement is everywhere." This concept was widely held at the NSVSS as recreational and commercial stakeholders repeatedly mentioned that a robust USCG and state and local law enforcement presence on the water would do the most to improve maritime security.

Several stakeholders recommended that any proposed security initiatives must be viewed as part of a larger security system model for a particular port or geographic area. They suggested that the MTSA needs to be revised, as it does not view ports as a system. Marinas and public access areas currently do not fall under the current MTSA regulatory scheme. Therefore, each port needs to be required to have a security plan that incorporates all of the facilities in the port rather than just the MTSA regulated ones.

To increase overall preparedness, some attendees suggested that crewmembers of commercial vessels receive annual training and certification on MARSEC security levels; vessel and port facility security plans; recognition and detection of suspicious individuals, activities, substances and devices; search and screening procedures; response and reporting procedures; communications protocols; and security and navigation equipment use and maintenance.

Finally, it was recommended that a select number of commercial vessel operators receive greater levels of training in observation and terrorist detection techniques and perhaps receive some level of clearance. This would allow for more trained "eyes and ears on the water" and provide focused reporting on security threats.

Participant view of the NSVSS

Stakeholder sentiment in regard to the NSVSS was overwhelmingly positive. By these measures, the NSVSS was a major success for DHS and the small vessel stakeholders.

A recurring theme among the survey respondents was that the NSVSS successfully brought together distinctive stakeholders, particularly the commercial and recreational boating communities, to focus their attention on important maritime security issues. Over 90 percent of the respondents to the post Summit survey indicated that the NSVSS was a valuable event for identifying issues important to small vessel security.

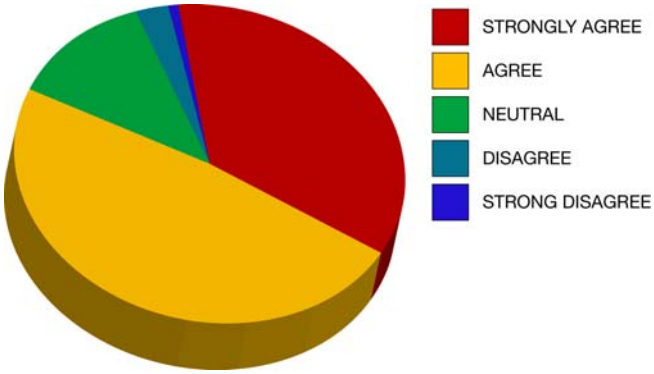
Another recurrent theme from attendees was that events similar to the NSVSS should be replicated in regional forums and DHS should consider conducting the NSVSS on an annual basis. As evidence of a highly engaged constituency with a desire to participate in future small vessel forums, nearly all of the respondents (99%) expressed their willingness to continue participating in national and regional small vessel security discussions. Most (86%) favored participating in face-to-face working groups. About one-half of the respondents also indicated that they would participate in a web-based collaborative activity such as virtual work groups, eConferences, web-based planning communities, or web-based Information Sharing and Analysis Centers (ISACs).

Furthermore, respondents suggested that future incarnations of the NSVSS should aim for even broader maritime stakeholder participation to include groups not well represented at the NSVSS such as marina operators, boat dealers, yacht clubs, and federal, state and local law makers. Beyond the NSVSS, stakeholders also recommended creating a website to offer and solicit information from stakeholders regarding issues of safety and security. Many respondents indicated their personal commitment to begin promoting greater security awareness based on their participation in the NSVSS.

Below are the results post-Summit surveys.

Overall Reaction

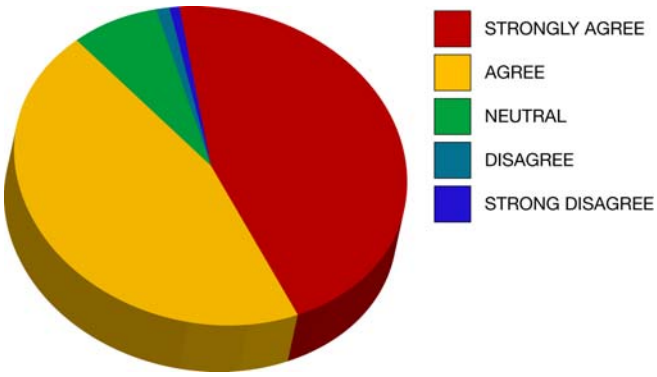
Overall the Summit provided a valuable opportunity to share my concerns, experience, and insights regarding small vessel security.



All Respondents *n = 174*

Strongly Agree	35.6 percent	(62)
Agree	48.3 percent	(84)
Neutral	12.6 percent	(22)
Disagree	2.9 percent	(5)
Strongly Disagree	0.6 percent	(1)

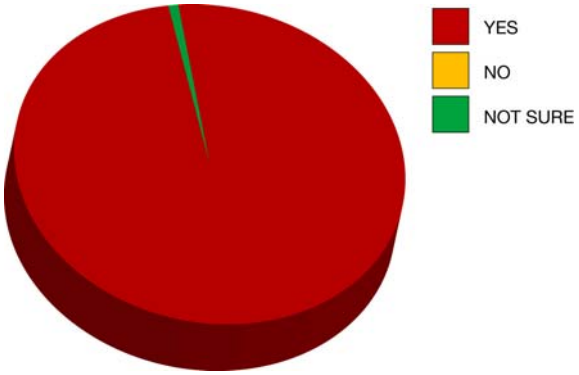
Overall the Summit was a valuable event for identifying issues related to small vessel security.



All Respondents *n = 174*

Strongly Agree	45.4 percent	(79)
Agree	45.4 percent	(79)
Neutral	7.5 percent	(13)
Disagree	1.1 percent	(2)
Strongly Disagree	0.6 percent	(1)

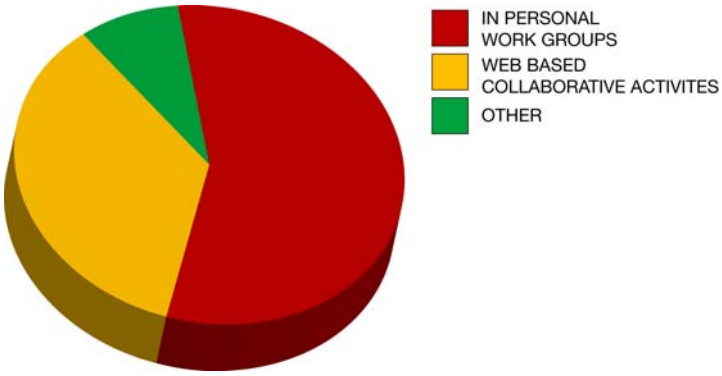
Would you or a representative from your organization like to continue to participate in national and regional small vessel security discussions?



All Respondents *n = 172*

Yes	99.4 percent	(171)
No	0.0 percent	(0)
Not Sure	0.6 percent	(1)

If you answered YES (to the previous question) to continue to participate in national and regional small vessel security discussions and planning, in which of the following would you be willing to participate? Please check all that apply.



All Respondents *n = 171*

In Personal Work Groups	85.8 percent
Web based collaborative activities	53.6 percent
Other	13.1 percent

VI. RECOMMENDATIONS

The following recommendations are not preconceived notions from the Homeland Security Institute (HSI) or the Department of Homeland Security (DHS) leading into the Summit. Rather, these recommendations were derived from stakeholder comments recorded at the Summit and from the post-Summit surveys that they completed. As there were multiple dozens of recommendations and suggestions taken from individual stakeholders at the Summit, HSI independently assessed these responses and grouped them into relevant categories.

- National Strategy: DHS needs to develop a coherent National Small Vessel Security Strategy based on a layered security approach. This strategy should not be separate from existing initiatives to improve the safety and security of larger vessels but should compliment such programs. Moreover, this strategy should not focus on deterring a specific type of terrorist attack but should enhance the overall safety and security of the maritime domain. Any national strategy must be flexible enough to meet the unique needs of any given port as a one size fits all strategy will ultimately prove to be ineffective and inefficient. The strategy should include actions for coordination with international partners where small vessel threats may emanate from.
- Personal Liberty and Economic Self-Determination: DHS should not impose overly restrictive regulatory constraints on small vessel operators or their boats in the areas of licensing, registration, or tracking. Such measures will likely be costly; increase safety and security minimally; alienate the small vessel operator; and damage the industry economically.
- Threat and Risk Assessments: DHS needs to conduct and convey threat and risk assessments on a continuing basis in the following areas: 1) defining the nature of the threat; 2) determining port specific security needs; and 3) clarifying the small vessel threat from foreign countries.
- Small Vessel Stakeholder Engagement: Given the commitment and interest of the small vessel community to actively participate in the security of the country, DHS needs to take immediate steps to keep this stakeholder group engaged. Regional meetings, continued feedback, public - private partnerships, and web-based initiatives were some of the major recommendations suggested to keep the small vessel community engaged and informed on this critical issue. Stakeholder outreach should be a part of the overall small vessel security strategy.
- Funding: Funding is needed to support state, local, tribal, and territorial maritime law enforcement entities as homeland security missions have become unfunded mandates that deplete these agencies of their budgets and negatively impact other public safety and security missions. As difficult decisions need to be made, any new federal funds should be used to build upon existing capabilities and capacities that have been successful in the past at addressing both maritime safety and homeland security operations.

- Training: Law enforcement training deficiencies need to be addressed, not just for terrorist attacks, but for a variety of security objectives. Increased interagency training for state, local, tribal, and territorial law enforcement agencies, with search and rescue, and other first responders is recommended to improve response to waterborne terrorist attacks. Such training would serve the dual purpose of improving preparedness and reducing the damage of non-terrorist catastrophic events like man-made accidents (e.g., oil spills) and natural disasters (e.g., hurricanes).
- Education and Outreach: More must be done to encourage citizen participation and disseminate information about safety and security concerns. The best and most efficient approach for DHS to accomplish this is to expand and reenergize the America's Waterway Watch program. To do this DHS needs to ensure adequate and sustained funding for AWW as well as provide continued and committed support by senior federal officials.
- Suspicious Activity Reporting: The small vessel community has a positive interest in participating in programs to identify and report suspicious activities. It is recommended that a universal hotline telephone number, similar to the National Response Center 1-800 number, be developed and widely communicated so that the boating community can report both suspicious activities and emergency situations. This number should be kept simple so that boaters will recall it easily; it should be prominently displayed on all boats. The call center should have the capability to route calls to the appropriate agencies.
- Domain Awareness: AIS technologies should not be required for vessels under 65 feet in length until the technology is perfected, the cost of such technology significantly reduced, and until law enforcement has the ability to track and respond to all vessels in the maritime domain. Until these problems are resolved, an interim step may be for small vessels to install some type of RFID technology or install relatively inexpensive vehicle recovery and monitoring systems similar to LoJack or OnStar. It is recommended that DHS initiate research, preferably in partnership with the small vessel community, to develop alternative technologies. In addition, unintrusive technology solutions that do not impact vessel operators such as radar and infrared/low light cameras should also be explored. Whatever tracking system is adopted it must be simple, effective, inexpensive, and multipurpose.
- Operator and Vessel Identification: It is necessary to streamline the number and variety of credentials and ensure that various jurisdictions accept the same standards. A simple solution would be for states to add a boat operator endorsement, similar to ones required to operate a tractor trailer or school bus, to their state driver licenses. At the Summit it was widely held that a national boat registry should be created so that it can be indexed and searched by federal, state local, tribal and territorial law enforcement agencies.
- International Cooperation: There was widespread agreement at the Summit that a strong regime of international agreements and cooperation is needed to identify and defeat possible small vessel threats before they reach U.S. waters. Attendees

recommended that the federal government enhance international cooperation and intelligence sharing with our foreign counterparts, especially with those countries in close proximity to the United States (i.e. Mexico, Canada, and nations in the Caribbean) as these nations are the most likely departure points for a small vessel terrorist attack from overseas.

- Intelligence, Analysis and Dissemination: A broad spectrum of stakeholders called for the development of fusion centers to better share, analyze and disseminate intelligence. Stakeholders recommended that these fusion centers be fully funded and staffed by personnel from the USCG, CPB, U.S. Navy, the Harbor Master and state and local law enforcement agencies. Stakeholders also recommended the use of a nationwide system to share information on stolen vessels in real-time, in a form that all law enforcement agencies could access (e.g., NCIS)
- Radiological and Nuclear Detection: Preventing a terrorist organization from acquiring and using a RAD/NUC device against a major U.S. population center is one of the nation's utmost security concerns. To prevent such an attack, it is recommended that federal, state, local, tribal, and territorial law enforcement agencies be provided with nuclear detection devices so they can detect radioactive signatures on small vessel and in cargo. The cost of such equipment requires federal guidance and oversight. In addition, the federal government should develop RAD/NUC detection devices with a stand-off capability in order to provide detection without directly impacting small vessel operators. The federal government should also consider placing nuclear detection devices on commercial vessels in a partnership to increase the chance of detecting a nuclear device or nuclear material before it reaches a major U.S. port or population center. Lastly, the federal government needs to strengthen counter-proliferation initiatives with our foreign counterparts to prevent shipments of WMD, their delivery systems, or related materials from reaching the U.S. maritime domain.[67]

[67] Counter-proliferation efforts that should be enhanced to the highest possible extent include the Cooperative Threat Reduction (CRT) Program, the Proliferation Security Initiative, the U.N. Security Council Resolution 1540, and other diplomatic and intelligence efforts.

VIII. CONCLUSIONS

The federal government needs to take immediate steps to develop a national small vessel strategy; improve intelligence sharing and coordination among federal, state and local law enforcement agencies; expand the development and use of radiological and nuclear detection devices; ensure adequate funding for maritime homeland security missions and other safety needs; and bolster international cooperation. DHS should make these initiatives a high priority as they are clearly a federal responsibility, will develop the needed layered security systems, will greatly increase the security of the U.S. maritime domain, and will be widely supported by the small vessel community.

Emphasis should be placed on streamlining and ensuring small vessel operator credentialing, to identify those operators who have received safe operation training of small vessels. There is a need for creating a uniform performance standard and ensuring that every small vessel operator carry a recognizable credential and provide it when requested. There is also a need for a national small vessel identification standard to include creating a national boat registry. As many of these issues are controversial, common sense solutions can be achieved so long as they respect the individual rights of boaters to enjoy their maritime heritage with minimal interference from the government.

Improving domain and situational awareness are also issues of critical importance. Upgrading suspicious activity reporting through universal hotline numbers and other reporting mechanisms are potentially effective ways to improve situational awareness. However, improving domain awareness is a much more delicate issue due to the expense and perceived intrusiveness of such systems. Whatever means are adopted to improve domain and situational awareness, these measures should be simple, effective, inexpensive, respect the rights of boaters, ensure the economic viability of the industry, and leverage existing successful methods and technologies.

Lastly, DHS needs to make a continued and concerted effort to actively engage the small vessel community on issues of small vessel safety and security. This is a dynamic and committed constituency that seeks a longstanding partnership with DHS and is ready to make major contributions to the safety and security of the country. Enhanced education and training combined with regional meetings, expanded feedback, public-private partnerships, and web-based initiatives are a few of the many ways the federal government can keep the small vessel community interested and informed on these vital issues.

IX. APPENDICES

Appendix A: NSVSS Agenda

Schedule of Events

Tuesday, 19 June 2007

7:30 – 8:45	Registration & Coffee
8:45 – 9:00	Introduction (*RDML Brian Salerno, USCG*)
9:00 – 9:30	Admiral Thad W. Allen, Commandant U.S. Coast Guard
9:30 – 10:00	W. Ralph Basham, Commissioner U.S. Customs and Border Protection
10:00 – 10:30	Break – Refreshments
10:30 – 11:00	Vayl Oxford, Director Domestic Nuclear Detection Office
11:00 – 11:30	Dr. Christopher Merritt U.S. Coast Guard Intelligence Coordination Center Small Vessel Threat Assessment
11:30 – 12:45	Hon. Michael Chertoff, Secretary Department of Homeland Security Luncheon & Keynote Speaker
12:45 – 1:45	Panel 1: *Recreational Vessel Interests*
1:45 – 2:45	Panel 2: *Commercial Vessel Interests*
2:45 – 3:00	Break
3:00 – 4:00	Panel 3: *State & Local Government Interests*
4:00 – 4:15	Moderators Direction (*Ms. Kristin Arnold*)
4:15 – 4:30	Break – Refreshments

4:30 – 6:00	Work Group Discussions

*****

Wednesday, 20 June 2007

7:00 – 7:30	Coffee
7:30 – 9:00	Work Groups: Scenario Threat – WBIED
9:00 – 9:30	Break – Refreshments
9:30 – 10:30	Work Group presentations on WBIED
10:30 – 10:45	Break
10:45 – 12:00	Work Groups: Scenario Threat – WMD
12:00 – 1:30	Michael Wermuth, RAND Corporation Luncheon & Speaker
1:30 – 3:00	Work Group presentations on WMD
3:00 – 3:15	Closing Remarks (*RDML Salerno, USCG*)

*****

Appendix B: Participating Agencies and Organizations

The following participant information from the post Summit surveys is garnered from the State and Local Government, Commercial Vessel Operators, Recreational Boating Industry, Recreational Boating Community, and Others categories. In some cases, there is replication between categories because some participants identified with multiple organization categories.

State and Local Government

- Alameda County Sheriff's Office – Marine Patrol, CA.
- Boston Police – Harbor Patrol, MA.
- California Department of Boating and Waterways
- Charlotte County, FL.
- Golden Gate Bridge, Highway and Transportation District, Ferry Division
- Los Angeles County Sheriff, CA.
- Marina Del Rey, CA.
- Marine Patrol, St. Claire County, MI.
- National Association of State Boating Law Administrators (NASBLA)
- North Carolina Ferry Division
- New York City Police Department
- Orange County Sheriffs Department, CA.
- Port of Long Beach, CA.
- Port of Los Angeles, CA.
- Puerto Rico Maritime Transportation Authority, P.R.
- Richmond Police Department, VA.
- San Francisco Police Department – Marine Patrol, CA
- San Francisco Fire Department – Homeland Security Division, CA.
- Seattle, Fire Department, WA.
- State of Alabama, Department of Natural Resources
- State of California, Office of Homeland Security
- State of California, Department of Boating and Waterways
- State of Delaware, DNR and Environmental Control
- State of Florida, Fish and Wildlife Conservation Commission

- State of Maine, Marine Patrol
- State of New York, State Police
- State of Ohio, Department of Natural Resources
- State of Tennessee Wildlife Resources Agency – Boating Division
- State of Virginia, Department of Game and Inland Fisheries
- State Organization for Boating Access

Commercial Vessel Operators

- American Waterways Operators (AWO)
- Atlantic Intracoastal Waterway Association
- Captree Boatmen Charter Boats
- Chesapeake Area Professional Captains Association
- Commercial Fishermen of America (CFA)
- Commercial Fishing Industry Vessel Safety Advisory Committee (CFIVSAC)
- C-PORT
- Crowley Marine Corporation
- Cruise Lines International Association (CLIA)
- DONJON-SMIT, LLC
- Edison Chouest – Offshore and U.S.
- Fire Island Ferries, Inc.
- Furlough Marine Management, L.L.C.
- G & H Towing Company
- Gloucester Fishermen's Wives Association
- Great Lakes Sport Fishing Charter Groups Council
- Inlandboatman's Union of the Pacific
- Moran Towing Corporation
- McAllister Towing
- Massachusetts Bay Line
- Mississippi Charter Boat Captains Association
- National Association of Charter Boat Operators (NACO)
- Offshore Marine Service Association (OMSA)
- Passenger Vessel Association (PVA)

- Potomac River Pilot Association
- Riverstreet Riverboats
- S.T.A.M. Marine Enterprises, Inc.
- Sandy Hook Pilots
- Seabulk Towing Inc.
- South Ferry, Inc.
- St. Lawrence Seaway Pilots' Association
- Sun Cruz Casinos
- Trident Seafoods Corporation
- Wendella Sightseeing Boats
- Wilmington Tug, Inc.
- Woods Hole Steamship Authority

Recreational Boating Industry

- American Boat & Yacht Council (ABYC)
- Ancon Marine Consultants, Inc.
- Association of Marina Industries
- Bombardier Recreational Products
- Browning's Marine Inc.
- Dawson Marine Group/Boating Writers International
- Forever Resorts
- Fraser Yachts Worldwide
- Indmar Products
- Lake Erie Marine Trade Association
- Marine Retailers Association of America (MRAA)
- National Marine Manufacturers Association (NMMA)
- Paddlesports Industry Association
- Personal Watercraft Industry Association
- Recreational Boating Committee of the Maritime Law Associations of the U.S.
- Seacor Marine Inc.
- Sea Tow Services International, Inc
- Soundings Magazine

- Southern Boating and Marine Business Journal
- Sunset Marine, LLC.
- Zodiac of North America

Recreational Boating Community

- American Canoe Association
- American Watercraft Association
- Boat Owners Association of the United States (Boat U.S.)
- Greater Cleveland Boating Association
- Mt. Vernon Yacht Club, VA.
- National Boating Federation (NBF)
- National Boating Safety Advisory Council (NBSAC)
- National Safe Boating Council
- National Water Safety Congress
- United Safe Boating Institute
- U.S. Power Squadron
- U.S. Sailing Association

Other

- ADM Corporate Security (ARTCO)
- Applied Research Associates, Inc.
- Archer Daniels, Midland Corp.
- American Salvage Association
- B. & J. Martin, Inc.
- Canada Border Services Agency (CBSA)
- Canadian Power and Sail Squadron
- Commercial Fisherman Magazine
- Department for Transport, United Kingdom
- Dawson Marine Group/Boating Writers International
- EADS, North America
- EG&G Technical Services
- EnviroCare Solutions International and Marine University
- General Dynamics, IT

- Gilbert and Associates Inc.
- Great Lakes Sport Fishing Council
- Homeland Security Council
- Info-link Technologies
- Inland Marine Services
- Inland Rivers, Ports and Terminals, Inc.
- International Association of Marine Investigators
- Investigative Security Services
- Jones Walker LLP
- Leland Limited Inc.
- Looney and Grossman
- Marine Exchange of Alaska
- Marine Security Policy and Operations, Transport Canada
- Maritime Authority of the Cayman Islands
- Maritime Security Council
- New Bedford Seafood Consulting
- Ontario Provincial Police, Canada
- Royal Canadian Mounted Police (RCMP), Canada
- SAIC, Homeland and Maritime Security Systems
- Savannah River, National Labs
- Secure Waters LLC
- Telemus Solutions
- Terminal Operations, Hovensa LLC
- The Cayman Islands Shipping Registry
- The Triton
- The Vane Brothers Co.
- TranSystem / SeaSecure
- University of Findlay, Ohio
- U.S. Federal Government:
  - DHS – CBP
  - DHS – DNDO

- DHS – FLETC
- DHS – ICAO
- DHS – ICE
- DHS – Policy Office
- DHS - TSA
- DHS – U.S. Coast Guard and Auxiliary
- FBI
- U.S. House of Representatives, Committee on Homeland Security
- NORTHCOM
- U.S. Army Corps of Engineers
- U.S. Navy
- U.S. Small Business Administration

Appendix C: Post-Summit Survey

DHS National Small Vessel Security Summit Survey Form

Your participation in the National Small Vessel Security Summit was greatly appreciated. The Homeland Security Institute collected your inputs throughout the summit, but in addition would like to get your reaction to the summit and any additional ideas directly. If you provided your input during the summit, you may still provide additional input here.

By responding to the following questions, your input will assist us in developing a post-Summit report, and assist DHS in the development and implementation of small vessel security programs, protocols and practices.

1

The Speakers

The speaker sessions addressed issues important to me.

○ Strongly Agree ○ Agree ○ Neutral ○ Disagree ○ Strongly Disagree

1

The speakers provided valuable information regarding small vessel security.

○ Strongly Agree ○ Agree ○ Neutral ○ Disagree ○ Strongly Disagree

1

Please note any speakers or speaking sessions that were particularly helpful, and/or recommend any improvements or possible future speaker topics.

1

The Panels

The panels stimulated important discussion regarding small vessel security.

○ Strongly Agree ○ Agree ○ Neutral ○ Disagree ○ Strongly Disagree

1

The panel discussions provided insight important to small vessel security issues.

Strongly Agree Agree Neutral Disagree Strongly Disagree

1

Please provide any suggestions or comments regarding improvements in the p discussions.

1

The Scenario Discussion Sessions

The purpose of the Scenario Discussion Sessions was clearly explained.

Strongly Agree Agree Neutral Disagree Strongly Disagree

1

The direction provided by the facilitators for the Scenario Discussion Sessions was clear and understandable.

Strongly Agree Agree Neutral Disagree Strongly Disagree

1

The Scenario Discussion Sessions identified valuable information regarding small vessel security.

Strongly Agree Agree Neutral Disagree Strongly Disagree

1

The Scenario Discussion Session process was well managed.

Strongly Agree Agree Neutral Disagree Strongly Disagree

1

I had the opportunity during the Scenario Discussion Sessions to share my concerns.

Strongly Agree Agree Neutral Disagree Strongly Disagree

1

Please recommend any changes that would improve the process or the Scenario Discussion Session output.

1

Networking Opportunities

There were adequate opportunities to network during the conference.

Strongly Agree Agree Neutral Disagree Strongly Disagree

1

What additional networking opportunities should DHS consider in the future, to have further discussions regarding small vessel security?

1

Overall Reaction

Overall the summit provided a valuable opportunity to share my concerns, experience, and insights regarding small vessel security.

Strongly Agree Agree Neutral Disagree Strongly Disagree

1

Overall the summit was a valuable event for identifying issues related to small vessel security.

Strongly Agree Agree Neutral Disagree Strongly Disagree

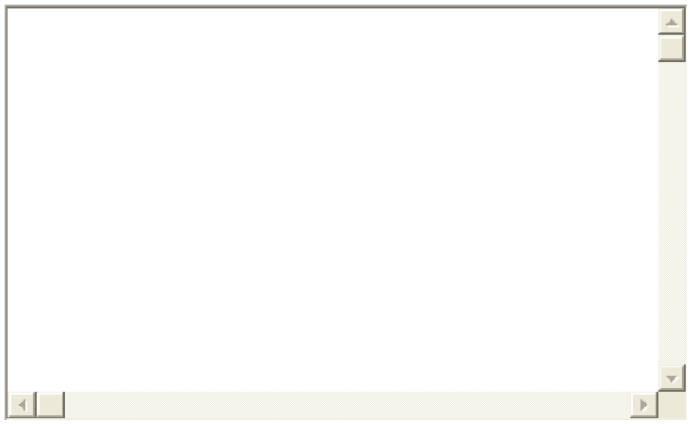
1 **Please indicate which stakeholder group you represent.**

State or Local Government Recreational Boating Industry Other (please specify)
Commercial Vessel Operators Recreational Boating Community

If you selected other please specify:

Your Ideas, Issues, Recommended Solutions

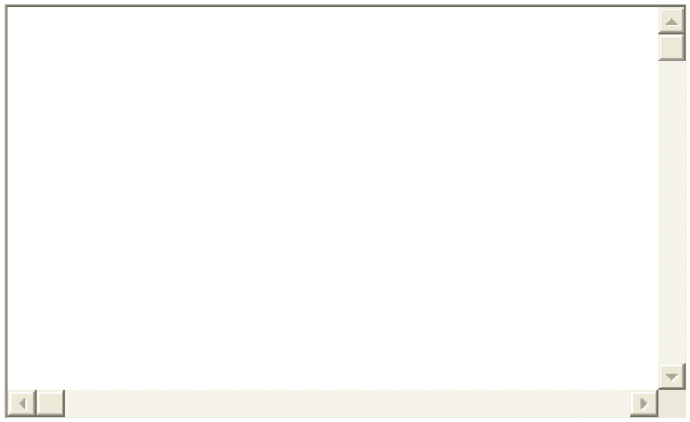
Please tell us what you consider to be the most important issues, ideas and recommended solutions to improve small vessel security and why you feel that way.



1

Next Steps

How do you think the process and content of this summit will change how you approach your role as a small vessel security stakeholder as it relates to homeland security and protecting the Nation?



1 **Would you or representatives from your organization like to continue to participate in national and regional small vessel security discussions?**

- Yes
- No
- Not Sure

1 **If you answered YES to continue to participate in national and regional small vessel security discussions and planning, in which of the following would you be willing to participate? Please check all that apply.**

☐ In Person Work groups

☐ Web-based collaborative activities, such as virtual work groups, eConferences, web-based planning communities, or web-based Information Sharing and Analysis Centers (ISACs)

☐ Other (please specify)

If you selected other please specify:

1 **Please tell us anything else about how to best involve stakeholders from your part of the small vessel community as DHS develops its programs in this important area of national security.**

1 **This survey is ANONYMOUS; however if you would like to share your name and organization with us, please feel free to do so. Also, if you would like to have someone contact you, please provide your email as well.**

Name

Organization

email

Thank you for taking the time to provide your input. The post-Summit after action report will be released approximately November 2007. When it is released by DHS, you will be notified by email where it is posted to read and download, or where you can contact us to have a copy sent to you. Additionally, here is the link to the America's Waterway Watch video http://www.youtube.com/watch?v=YCCKQjEqiJw

Please enter your email address:

Submit Survey

Appendix D: Small Vessel Security Means and Methods

Restricted Access Areas. A demarcated area to prevent damage or injury to any vessel or waterfront activity; to safeguard ports, harbors or U.S. waters. Used to control access or movement of persons, vessels and objects within the zone. Such zones allow for ready identification of potential threat vessels, enable possible intercept and neutralization of such vessels and, in turn, provide a degree of deterrence.

- Safety or Security Zones – around critical infrastructure, e.g., nuclear plant
- Protection Zones – around maritime critical infrastructure/key resources
- Prohibited Areas – exclude recreational vessels from maritime industry areas
- Regulated Navigation Areas – areas in which only certain vessels types of may navigate/enter, and from which other types are excluded.

Vessel Tracking. A means for port/waterway authorities to follow the movement of vessels to monitor vessel/waterway safety and detect any anomalous activities and, in turn, offer a degree of deterrence. As an example, the Vessel Traffic Services (VTS)

Vessel Registration. A means for port/waterway authorities to associate a particular vessel with its ownership, intended use, homeport, and any previous activities of law enforcement (LE) or intelligence significance and, in turn, offer a degree of deterrence. Each state has its own vessel registration system of varying degrees of sophistication. In combination with other methods, vessel registration offers a means to ascertain a level of risk.

Public Awareness. A means to allow the small vessel stakeholder community recognition of potential threats, anomalous activities and appearances indicating potential illicit activities; the means and channels to share that information with local authorities; and, in turn offer a degree of deterrence. Elements of public awareness are:

- Observation
- Education
- Information sharing (private to public sector; public to private sector)
- Reporting – relationships and communications channels
- America's Waterway Watch Program

Certification/Identification. A means for port/waterway authorities to identify a vessel operator, determine the qualifications of that person to operate that vessel, ascertain any previous operator activities of law enforcement of intelligence significance and, in turn, offer a degree of deterrence. It also allows for boater education regimens and provides a general awareness of the make-up of the boater community.

Identification Systems. A technological means for port/waterway authorities to readily identify a vessel and correlate that vessel with its ownership, registration, and reporting

activities in order to detect any anomalies, recognize threats and, in turn, offer a degree of deterrence.

Law Enforcement Intelligence/Data Fusion. The capability to gather and analyze information from and among multiple law enforcement authorities and other sources to provide for a common operating picture with which to detect and act on illicit and/or anomalous activities. EPIC (El Paso Intelligence Center) is an example of federal interagency border and drug-enforcement intelligence collection and fusion among DEA, CBP, USCG and other federal law enforcement partners. See http://www.usdoj.gov/dea/programs/epic.htm.

Directed Standards. Common procedures and practices applied at all ports and waterways to enhance security and, as such, offer a degree of deterrence. One example would be the vessel Notice of Arrival prescribed for vessels weighing over 300 gross tons.

Performance Standards. Common procedures and practices applied at specific ports and waterways to enhance security and, as such, offer a degree of deterrence.

Vessel of Interest. A thorough assessment of risk factors to determine if a vessel presents a potential threat and, if so, identify the "target" as a "vessel of interest" for further investigation and potential boarding. The USCG applies various matrices of risk factors to determine vessels of interest. This process represents a cultural change in the boating community.

Technical Detection Capabilities. Technical or scientific means to detect the presence of a weapon of mass destruction, WMD materials, or explosives, commonly applied to radiological/nuclear (RAD/NUC) devices.

International Cooperation. Collaboration with other states and international organizations to detect, deter and defeat terrorists and associated conspiracies.

Layered Defense. A combination of methods which, in the aggregate, allow for increased security. While each method may not be effective in every case, an combination of methods – varying from the tactical to the strategic – may provide the necessary defense in depth.

XIII. BIBLIOGRAPHY

Anderson, Patrick L. and Ilhan K. Geckil. "Flash Estimate: Impact of West Coast Shutdown." Anderson Economic Group LLC (October 15, 2002).

"Border Security: Infrastructure, Technology, and the Human Element, Statement of RADM David P. Pekoske, Assistant Commandant for Operations, Before the Committee on Homeland Security, Subcommittee on Border, Maritime, and Global Counterterrorism, U.S. House of Representatives." Department of Homeland Security—U.S. Coast Guard (February 13, 2007).

Butz, E., D. Steinmetz, W. Johnson, G. Williams, M. Thayer, and K. Knutson. "D13 Small Boat Threat Analysis/Mitigation." Group Port Angeles AOR (September 30, 2006).

Carafano, James J. "Small Boats, Big Worries: Thwarting Terrorist Attacks from the Sea." Backgrounder. Washington, DC: The Heritage Foundation, June 11, 2007.

Chalk, Peter, "Maritime Terrorism in the Contemporary Era: Threat and Potential Future Contingencies," The MIPT Terrorism Annual 2006.

"Coastal Zone Small Boat Threat Issue Paper: D14 Coastal Zone Small Boat Threat Analysis/Mitigation." Small Boat Threat Working Group.

Cohen, Steven S. "Economic Impact of a West Coast Dock Shutdown." University of California at Berkeley (January 2002).

"The Columbia-Willamette River Systems: River-borne Improvised Explosive Device Analysis." Sector Portland Work Group (September 2006).

"Comments of Admiral Thad Allen at the National Conference of State Legislatures." (December 6, 2006).

"Comments of Admiral Thad Allen at the 47th Annual Conference of the National Association of State Boating Law Administrators." (September 24, 2006).

"District 13 Waterborne Improvised Explosive Device (WBIED) Study Group." (October 27, 2006).

Downs, Brady. "Safely Securing U.S. Ports." Proceedings (Spring 2006): 19-21.

The Economic Costs of Disruptions in Container Shipments. Washington, DC: Congressional Budget Office, March 29, 2006.

"The Economic Impacts of the Port of Baltimore." Martin Associates (November 10, 2003).

Falk, Ophir and Yaron Schwartz. "The Maritime Threat." (April 25, 2005).

Frittelli, John F. Port and Maritime Security: Background and Issues for Congress. Washington, DC: Congressional Research Service, December 5, 2003.

Greenberg, Michael, et. al., Maritime Terrorism: Risk and Liability. Santa Monica, CA: RAND Corporation, 2006.

"Homeland Security: Applying Risk Management Principles to Guide Federal Investments, Statement of William O. Jenkins, Jr., Director, Homeland Security and Justice Issues, Testimony Before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives." Government Accountability Office (February 7, 2007).

"Improvised Nuclear Device (IND) Exercise Scenario." Domestic Nuclear Detection Office (DNDO) Department of Homeland Security (September 25, 2006).

Lugar, Richard G. "The Lugar Survey on Proliferation Threats and Responses." (June 2005).

"Maritime Operational Threat Response for the National Strategy for Maritime Security." (October 2006)

Medalia, Jonathan. Terrorist Nuclear Attacks on Seaports: Threat and Response. Washington, DC: Congressional Research Service, January 24, 2005.

Michaelis, Matthew. "Defending Against a Small Vessel WMD Attack." (December 12, 2006).

Moran, Jim. "The Dominance of 'Nuclear Device Transfer Scenarios' in PWCS/CMT Risk Assessments and Implications on Small Boat Risk." Coast Guard Office of Mission Analysis.

Moteff, John. Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. Washington, DC: Congressional Research Service, February 4, 2005.

National Plan to Achieve Maritime Domain Awareness, Washington, DC, 2005.

"New Threats, New Challenges, New Strategy." George Schultz Lecture Series.

Parfomak, Paul W. and John Frittelli. Maritime Security: Potential Terrorist Attacks and Protection Priorities. Washington, DC: Congressional Research Service, January 9, 2007.

"Radiological Dispersal Device (RDD) Exercise Scenario." Domestic Nuclear Detection Office (DNDO) Department of Homeland Security (September 25, 2006).

Report of the Defense Science Board Task Force on Critical Homeland Infrastructure Protection. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, January 2007.

"The Role of the Coast Guard in Border Security, Statement of VADM Thad Allen, Chief of Staff, Before the Committee on Appropriations, Subcommittee on Homeland Security, U.S. Senate." Department of Homeland Security—U.S. Coast Guard (April 6, 2006).

The U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship, United States Coast Guard, (January 19, 2007)

"Security in Maritime Transport: Risk Factors and Economic Impact." Maritime Transport Committee of the Organisation for Economic Co-operation and Development (July 2003).

"Small Boat Threat Information Paper." Sector Seattle Boat Attack Working Group (September 15, 2006).

"State of the Coast Guard Address." Washington, DC (February 13, 2007).

"Strategic Budgeting: Risk Management Principles Can Help DHS Allocate Resources to Highest Priorities, Statement of David M. Walker, Comptroller General of the United States, Testimony Before the Subcommittee on Management, Integration, and Oversight, Committee on Homeland Security, House of Representatives." Government Accountability Office (June 29, 2005).

U.S. Commission on Ocean Policy, An Ocean Blueprint for the 21st Century, Washington, DC: 2004.

"Use of Scenarios and 'Event Families': 2006 National Maritime Strategic Risk Assessment (NMSRA) & Combating Maritime Terrorism (CMT) Risk-Informed Planning Process." United States Coast Guard (April 14, 2007).

"The Water is Different." U.S. Naval Institute (USNI) Port Security Conference (June 7, 2006).

"WBIED Attack Study—List of All Recommendations."

White, Ronald D. "A System to Keep Tabs on Ships." Los Angeles Times (March 31, 2007). Accessed from http://www.latimes.com/business/la-fi-shiptrackers31mar31,1,359088,full.story?ctrack=2&cset=true on April 4, 2007.