DEPARTMENT OF HOMELAND SECURITY

SMALL VESSEL SECURITY STRATEGY

APRIL 2008

FOREWORD

Since the terrorist attacks of September 11, 2001, maritime security efforts have focused primarily on large commercial vessels, cargoes, and crew. Efforts to address the small vessel[1] environment have largely been limited to traditional safety and basic law enforcement concerns. Small vessels are, however, readily vulnerable to potential exploitation by terrorists, smugglers of weapons of mass destruction (WMDs), narcotics, aliens, and other contraband, and other criminals. Small vessels have also been successfully employed overseas by terrorists to deliver Waterborne Improvised Explosive Devices (WBIEDs).

Law enforcement agencies face the challenge of distinguishing between the vast number of legitimate vessel operators and the relatively few individuals engaged in illicit activities. The challenge is immense, as it involves nearly 13 million registered U.S. recreational vessels,[2] 82,000 fishing vessels, and 100,000 other commercial small vessels. On any given day, a considerable number of these boats share waterways with commercial and military traffic, operating at hundreds of U.S. ports and in the immediate vicinity of critical maritime infrastructure, including bridges and waterfront facilities such as petrochemical plants. More information concerning small vessels is needed to improve the proper assessment of the risk posed by these vessels. The challenge is to balance the collection of requisite information necessary for proper assessment of risk posed by these vessels, with the freedom of the seas expected by the small boating community.

Additionally, a significant number of these craft operate internationally, especially in regions such as the Great Lakes, the Gulf of Mexico, and the Caribbean Sea. During Fiscal Year 2006, only 70,000 boater foreign arrivals were recorded in the U.S. Customs and Border Protection (CBP) Pleasure Boat Reporting System (PBRS), based on boater self-reporting. Conservative estimates suggest that these reporting figures represent only a fraction of the actual international boater traffic, especially given the ease with which boaters operate in these waters.

Currently, the U.S. Government has an incomplete knowledge of the international recreational boating public, their travel patterns, and the facilities they use. Couple this with the limited information available regarding fishing fleets and the multitude of small commercial vessels operating in or near U.S. waters and the complexity of the issue becomes obvious.

Hence, there is a clear need to close security gaps and enhance the small vessel security environment. The *Small Vessel Security Strategy* (SVSS) addresses these concerns and provides a coherent framework to improve maritime security and safety. It envisions a coordinated effort of Federal, state, local, and Tribal authorities, together with international partners, private industry, and recreational users of the waterways.

[1] Small vessels are characterized as any watercraft regardless of method of propulsion, less than 300 gross tons. Small vessels can include commercial fishing vessels, recreational boats and yachts, towing vessels, uninspected passenger vessels, or any other commercial vessels involved in foreign or U.S. voyages.

[2] CG 2006 boater statistics compiled from state boater registration reports (does not include unregistered watercraft, which, when combined with registered boats, is estimated at 17 million total U.S. watercraft).

TABLE OF CONTENTS

FOREWORD i

TABLE OF CONTENTS iii

EXECUTIVE SUMMARY iv

INTRODUCTION 1

- PURPOSE OF THE STRATEGY 1
- SCOPE 1
- RELATIONSHIP TO OTHER STRATEGIES AND PLANS 1
- METHODOLOGY 2
- KEY DEFINITIONS 2

STRATEGIC ENVIRONMENT 4

- IMPORTANCE OF THE MARITIME DOMAIN 4
- MARITIME GOVERNANCE 5
- SMALL VESSEL COMMUNITY 5
- SMALL VESSEL RISK 6

STRATEGIC VISION 15

- GUIDING PRINCIPLES 15
- OVERARCHING VISION AND MAJOR GOALS 16

RISK MANAGEMENT 22

ORGANIZATIONAL ROLES, RESPONSIBILITIES, AND COORDINATION 24

THE WAY AHEAD 29

CONCLUSION 31

APPENDIX A—UNITED STATES FEDERAL GOVERNMENT RESPONSIBILITIES A-1

APPENDIX B—RELEVANT AUTHORITIES B-1

APPENDIX C—EXISTING INTERAGENCY INSTITUTIONS C-1

APPENDIX D—ACRONYMS D-1

EXECUTIVE SUMMARY

The Department of Homeland Security (DHS) *Small Vessel Security Strategy* (SVSS) exists within the framework of other security strategies. It does not replace any of the current strategies or relevant documents. Rather, this strategy harmonizes directions from related strategies into a multi-layered, unified approach for the component agencies within the DHS, and to lay the groundwork for DHS participation in coordination across all levels of government, as well as other public, private and international stakeholders in the maritime domain. This strategy's purpose is to address the risk that small vessels[1] might be used to smuggle terrorists or WMD into the United States or might be used as either a stand-off weapon platform or as a means of a direct attack with a WBIED. The resulting risks are difficult to manage because small vessels are not centrally registered, operators have not always demonstrated proficiency in small vessel operations, and the ability to screen or detect vessel-borne hazards is extremely limited. There is, moreover, a tradition and expectation among the large population of small vessel operators of largely unrestricted access to U.S. waterways.

This strategy also describes the small vessel community and the environment in which it operates. It discusses and identifies the threats, vulnerabilities, and consequences resulting from four key risk scenarios. Understanding the relationship of the threat, risk, vulnerability, and consequence of a small vessel terrorist attack on the United States will help to reduce the risk of such an attack. The guiding principles and overall goals of this strategy complement existing solutions for large vessels. These have

been effective in controlling risk in the operation of larger vessels that fall under the traditional oversight and regulations of commercial operations in international trade. These solutions provide direction, but each solution needs to be creatively adapted to suit the circumstances of small vessels, due to their difference in size, operation, and use compared to larger commercially operated vessels.

This strategy identifies specific goals where efforts can achieve the greatest risk reduction across the breadth of the maritime domain. Its guiding principles are that: solutions shall be risk-based; education and training are the key tools for enhancing security and safety; and economic and national security needs will not be compromised.

The overarching goals of the *Small Vessel Security Strategy* are to: enhance maritime security and safety based on a coherent framework with a layered, innovative approach; develop and leverage a strong partnership with the small vessel community and public and private sectors in order to enhance maritime domain awareness; leverage technology to enhance the ability to detect, infer intent, and when necessary, interdict small vessels that pose

[1] Small vessels are characterized as any watercraft regardless of method of propulsion, less than 300 gross tons. Although there is no exact correlation between a vessel's length and its gross tonnage, a vessel of 300 GT is approximately 100 ft in length.

a maritime security threat; and enhance cooperation among international, Federal, state, local, and Tribal partners and the private sector (e.g., marinas, shipyards, small vessel and facility operators), and, in coordination with the Department of State and other relevant federal departments and agencies, international partners. This strategy lays out the appropriate way forward in managing and controlling risks posed by the potential threat and possibly dire consequences of small vessel exploitation.

The private sector performs a central role in Homeland Security and can assist authorities in reducing each of the components of risk (threat, vulnerability, and consequence).

Small vessel operators can be effective partners in detecting threats in our ports and on our waterways. The large number of small vessel operators and their familiarity with the local area and patterns of waterway use make it possible that small vessel operators will be the first to recognize suspicious behavior. DHS must promote and strengthen their effectiveness through public dialogue regarding their role in homeland security and specialized programs such as America's Waterway Watch. Non-governmental organizations are key partners in keeping this dialogue going.

The private sector, through its efforts at securing private facilities from unauthorized entry and other intrusions, plays a key role in reducing our vulnerability to terrorist exploitation of small vessels. Small vessel operators can reduce vulnerability by ensuring their vessels are secure and protected against unauthorized use.

The private sector is the Nation's primary provider of goods and services and the owner and operator of approximately 85 percent of our critical infrastructure. It is an essential partner in ensuring structural and operational resilience that protects the American people, establishing security around critical infrastructure and key resources, and reporting suspicious activities at work sites that could uncover and ultimately help disrupt terrorist activity.

The private sector is also a critical partner in rebuilding critical infrastructure and key resources affected by a catastrophic incident as well as in fielding scientific and technological advancements that can help secure the United States. Due to the multiple and essential roles the private sector plays across all areas of homeland security, continued collaboration and engagement with the private sector to strengthen small vessel security is imperative.

It is understood that the vast size of the small vessel community makes the efforts to manage and reduce the overall risk in the maritime domain difficult. Yet, it is clear that an effective partnership through the layers of stakeholders and government authorities involved in security operations, and commercial and recreational pursuits, comprises one of the nation's greatest assets for reduction of small vessel related risks.

INTRODUCTION

PURPOSE OF THE STRATEGY

The intent of the *Small Vessel Security Strategy* (SVSS) is to reduce potential security and safety risks from small vessels[1] through the adoption and implementation of a coherent system of regimes, awareness, and security operations that strike the proper balance between fundamental freedoms, adequate security, and continued economic stability. Additionally, the strategy is intended to muster the help of the small vessel community in reducing risks in the maritime domain.

SCOPE

The SVSS is designed to guide efforts to mitigate the potential security risks arising from small vessels operating in the maritime domain. While guiding DHS efforts, this strategy acknowledges that to effectively reduce risk, all maritime security partners—Federal, state, local, and Tribal partners and the private sector as well as international partners—must work together to develop, implement, and undertake cooperative actions to reduce both security and safety risks from misuse of small vessels.

Much of the recent U.S. maritime security efforts have focused on regulating cargo containers and large vessels at official Ports of Entry (POE). Examples of such regulations include the 96hour Advance Notice of Arrival, cargo manifest/crew list transmittal within 24 hours of departure, and the carriage requirement for the Automatic Identification System (AIS). This strategy broadens the focus of federal interest, taking into

consideration small vessels regardless of type. The small vessel community includes a wide-range of vessels, from small commercial vessels, such as uninspected towing vessels and passenger vessels, to commercial fishing vessels and recreational boats, whether personal watercraft or large power and sail boats.

RELATIONSHIP TO OTHER STRATEGIES AND PLANS

The SVSS complements and is consistent with all applicable portions of the following legislations and strategies:

- 2002 Homeland Security Act
- 2002 Maritime Transportation Security Act
- 2004 Department of Homeland Security Strategic Plan
- 2005 National Defense Strategy
- 2005 National Intelligence Strategy
- 2005 National Strategy for Maritime Security
- 2006 National Security Strategy

[1] Small vessels are characterized as any watercraft regardless of method of propulsion, less than 300 gross tons. Although there is no exact correlation between a vessel's length and its gross tonnage, a vessel of 300 GT is approximately 100 ft in length.

- 2006 National Strategy for Combating Terrorism
- 2006 National Strategy to Combat Terrorist Travel
- 2007 National Strategy for Homeland Security

Specifically, SVSS incorporates the indicated guidance contained in the following:

- the use of risk-based decisions to prioritize DHS resource investments embodied in the *National Strategy for Homeland Security* and the *DHS Strategic Plan*
- the principles of the *National Security Presidential* Directive-*41/Homeland Security Presidential Directive-13* (NSPD-41/HSPD-13), which underscore the importance of securing the maritime domain
- identifying threats as early and as distant from U.S. shores as possible per the *National Plan to Achieve Maritime Domain Awareness*
- using existing capabilities to analyze and disseminate all available intelligence regarding potential threats to U.S. interests in the maritime domain according to the *Global Maritime Intelligence Integration Plan*
- coordinating the Federal Government's response to threats and delineating roles and responsibilities consistent with the *Maritime Operational Threat Response Plan*
- providing the framework coordinating all maritime security initiatives undertaken with foreign governments, international organizations, and private corporations overseas in keeping with the *International Outreach and Coordination Strategy*, and
- improving the security of the marine transportation system consistent with the *Maritime Transportation System Security Recommendations.*

METHODOLOGY

A DHS working group developed the SVSS and applied risk management principles to address four key risk scenarios from small vessels (enumerated in the *Strategic Environment* section). It built upon prior efforts such as the U.S. Coast Guard's (USCG) Small Vessel Information Gap Analysis,[2] the Small Vessel Risk Task Force Report, and the U.S. Customs and Border Protection (CBP)/USCG Joint Small Vessel Security Risk Strategic Principles. These documents and other precursor studies and analyses, along with the inputs from the June 2007 National Small Vessel Security Summit held in Arlington, Virginia, were critical in developing the SVSS.

KEY DEFINITIONS

The following definitions do not constitute, and are not intended to be, an exhaustive list of terms, nor is it to be understood to express a comprehensive, legally-binding view. These characterizations are provided to assist in understanding the application of risk assessment methodology to the small vessel security environment for the purpose of this strategy.

Small vessels are characterized for the purposes of this strategy as any watercraft—regardless of method of propulsion—less than 300 gross tons, and used for recreational or commercial purposes. Small vessels can include commercial fishing vessels, recreational boats and yachts, towing vessels, uninspected passenger vessels, and any other personal or commercial vessels involved in U.S. or foreign voyages.

[2] Conducted as part of the USCG's *Combating Maritime Terrorism* Campaign Plan.

Maritime Domain is all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime related activities, infrastructure, people, cargo, vessels, and other conveyances.

Risk is typically defined as a function of frequency and consequence of an undesirable event. When assessing the risk of terrorism, the frequency factor of risk is often broken down into the elements of threat and vulnerability. When assessing operational risk, frequency often includes the elements of probability (likelihood that an event will occur) and exposure (amount of time, people, or equipment involved).

Risk Management is a continuous process of assessing risks and implementing mitigating actions, with its primary goal being to reduce the potential that an adverse event will occur. Risk management addresses initial risk of an identified threat, and manages the residual risk after countermeasures are implemented. It has been used in the private sector (insurance, engineering, and banking and finance) and public sector (Food and Drug Administration, Environmental Protection Agency, and Department of Defense) for decades, but its application for Homeland Security and combating terrorism is relatively new without a precedent framework.

Threat is an indication of the likelihood that a specific type of attack will be initiated against a specific target or class of targets.[3] It is based on an understanding of an adversary's intentions, motivation, history of attacks, and capability to carry out an attack.

Vulnerability of an asset is an indication of the likelihood that a particular attempted attack will succeed against a particular target or class of targets.[4]

Consequence of an attack is the magnitude of the adverse impact of a successful attack. The outcome of an attack may include many forms, such as the loss of life, economic costs, and any adverse impacts on U.S. national security.

State government, for the purposes of this strategy, means any state of the United States, the District of Columbia, the U.S. territories of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or the Trust Territory of the Pacific Islands.

Local government means any county, city, village, town, district, or other political subdivision of any state, and includes any rural community or unincorporated town or village or any other public entity for which an application for assistance is made by a state or political subdivision thereof.[5]

[3] *Risk Management*, GAO-06-91, December 2005, at p. 111.

[4] *Risk Management*, GAO-06-91, December 2005, at p. 112.

[5] Definitions of state and local governments from the *National Strategy for Homeland Security* (October 2007) p. 4.

STRATEGIC ENVIRONMENT

IMPORTANCE OF THE MARITIME DOMAIN

The United States is the world's leading maritime trading nation, accounting for nearly 20% of the annual world ocean-borne overseas trade. The global Maritime Transportation System (MTS)—a complex and interconnected system of waterways, ports, terminals, inter-modal connections, vessels, people, support service industries, and users spanning the domestic and international public and private sectors—is the economic lifeblood of the global economy and is critical to U.S. national security and interests.

The maritime domain serves as a critical highway for the global economy, but also presents unique security challenges, encompassing vast stretches of oceans, waterways and countless potential points of entry. The United States has over 95,000 miles of coastline, 361 ports (including eight of the world's 50 highest-volume ports), and 10,000 miles of navigable waterways. It enjoys the world's largest Exclusive Economic Zone (EEZ), spanning 3.4 million square miles of waters and containing some of the most valuable and productive natural resources on Earth. In 2005, offshore activities contributed over $120 billion and two million jobs to American economic prosperity. Approximately 30% of U.S. oil supplies and 25% of its natural gas supplies are produced in offshore areas.

Nearly 700 ships arrive in U.S. ports daily, and 8,000 foreign-flag ships, manned by 200,000 foreign mariners, enter U.S. ports every year. Annually, the nation's ports handle more than $700 billion in merchandise, while the cruise

industry and its passengers account for $35.7 billion in direct and indirect economic output.[9] All told, the U.S. MTS supports a global chain of economic activity that contributes more than $700 billion to America's economy each year.

In addition to the global maritime trade contributions, the economic role of ocean industries provides tremendous value to the domestic economy. The MTS supports the commercial fishing industry and its 110,000 fishing vessels. In 2006, it contributed approximately $35.1 billion[10] to the U.S. economy, while the recreational saltwater fishing industry was valued at $30.5 billion.[11]

The millions of recreational boaters, who use the MTS every year, also contribute considerably to the economy. Nationwide, retail expenditures on

---

[9] *The Contribution of the North American Cruise Industry to the U.S. Economy in 2006* (August 2007), prepared for Cruise Lines International Association by Business Research & Economic Advisors, p. 35.

[10] *Fisheries of the United States 2006*, National Marine Fisheries Service, p. v.

[11] *A Vision for Marine Recreational Fisheries, NOAA Recreational Fisheries Strategic Plan FY2005-2010*, p 2.

recreational boating exceeded $33 billion in 2004. Moreover, hundreds of millions of visitors spend billions of dollars annually to enjoy the nation's ocean, lakes, and river beaches.

MARITIME GOVERNANCE

Maritime security and safety initiatives are best understood when viewed or discussed in the context of Figure 1. Governance of security and safety issues are accomplished using regimes, awareness, and operations through a unified effort involving international organizations, government, and private stake holders across the global maritime domain. Effective maritime governance requires:

(1) Appropriate regimes, or rule sets, to describe the desired state of the domain;

(2) Awareness to inform decision makers as to the actual state of the domain; and

(3) Operations and operational capability/capacity to help shape the domain from its current state toward the state described by the regimes.

This strategy embodies and fosters the development of capabilities across all three areas of regimes, awareness, and operations and employs unity of effort.

SMALL VESSEL COMMUNITY

The small vessel community is not monolithic. It is a large and diverse group of operators with different backgrounds, professional and casual training, and operating characteristics. Each geographic area has its own unique operating patterns and mix of small vessels. There are thousands of professional mariners who make their living on the waters every day—a considerable number of whom do so operating small vessels. These professional mariners range from charter vessel operators to small ferry or freight vessel operations, and include the

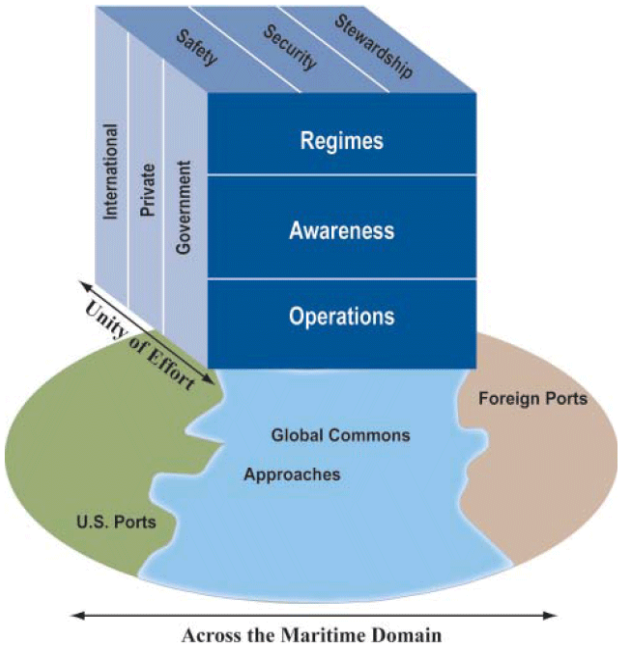


Figure 1, Maritime Governance

majority of the domestic commercial fishing and towing vessel industries. In addition to these professional mariners, as many as 80 million people participate in recreational boating in a given year. The level of experience within the small vessel community varies from experts down to occasional renters of a recreational boat who have little or no training and widely varying experience.

Additionally, there are generally low barriers to entry into the small vessel community. Small vessels are affordable to a broad range of boaters. Extensive skills and experience are often not necessary to minimally operate small vessels, and limited regulations in effect are primarily focused on safety. Another difference from large vessel operators is that the small vessel stakeholders generally have little direct involvement or face-to-face interaction with the international, Federal, state, local, and Tribal partners that govern the use of the waterways. This can lead to unnecessary misunderstandings and confusion. Finally, governance of the small vessel community is spread across multiple entities, with 18 Federal agencies and numerous state, local, Tribal, and port authorities, having roles ranging from vessel registration to

operational safety enforcement. Therefore, small vessel operators have different expectations than more regulated large vessel operators.

The following are some of the security concerns presented by small vessels:

- Small vessels operate (often routinely and with ease) in close proximity to critical infrastructure (CI) and key resources (KR), as well as major transportation channels and military ships, which may be potential high-profile targets.
- There is a lack of a centralized access to hull identification and vessel registration (owner) data.
- The ability to identify small vessel operators is limited because of uneven requirements for small vessel user certification and documentation.
- There are very limited Advance Notice of Arrival (ANOA) requirements for most recreational small vessels arriving from abroad.[12]
- There is limited awareness among small vessel operators of arrival reporting requirements and limited resources to enforce requirements, making enforceability of the small vessel arrival reporting process difficult.
- There is limited ability to screen for weapons of mass destruction (WMDs), especially chemical and biological agents.
- Among the large population of small vessel operators, there is a longstanding public expectation of totally unregulated access and use of U.S. waterways.

Offsetting these security concerns are the small vessel community's contributions to security:

- An abundance of geographically dispersed small vessels providing a large number of "eyes on the water" that would be impossible to replace using only government assets.
- An immense population of small vessel operators whose presence on U.S. waters can serve as a deterrent by identifying suspicious activities, given their adequate education and training.
- Willing volunteer partners to assist in providing the initial response capability for maritime incidents.
- A wealth of professional mariners and recreational boaters who understand the local waterways and are willing to assist in developing methods to reduce risk in the maritime domain.

SMALL VESSEL RISK

General Risk Framework

Most traffic on U.S. waterways and within ports involves legitimate boaters and commercial operators. But all too often it also involves those engaged in illegal activities, such as drug and, migrant smuggling, and theft. It is equally open to potential acts of terrorism. A key requirement for enhancing U.S. national security efforts is the ability to identify those who intend to do harm hiding within the sizable majority of people engaged in legitimate activities. The President has charged the Secretary of Homeland Security with coordinating homeland security programs through the application of intelligent risk

[12] CBP APIS requires all commercial vessels to provide advance manifests of crew and passengers. Within the USCG Seventh District (specifically in southeast Florida) there is a requirement for ANOA on recreational vessels.

management.[13] This effort requires identifying high-risk small vessels in priority and developing a layered system of regimes, awareness, and operational response capabilities to reduce risks.

In general terms, risk is defined as the product of the frequency (or likelihood) of an undesirable event and its consequence (or magnitude of the outcome) to persons, places, or property.

*Risk = **Frequency** x Consequence*

Frequency can further be broken down into separate components of threat (to address the likelihood of adverse actions based on anticipated capabilities and intent) and vulnerability (to address the potential strengths or weaknesses of facilities or assets that are targeted).

*Risk = **(Threat x Vulnerability)** x Consequence*

Relative to other fields such as insurance or finance, terrorism is a relatively new application for risk assessment. Unlike those fields which have extensive historical data that are used to assess risks, DHS lacks such data on terrorism against the U.S. homeland, thus limiting any detailed analysis in assessing risks. As a result, the threat, vulnerability, and consequence factors of a terrorist act are poorly understood and difficult to predict, requiring greater reliance on judgments from intelligence analysts, terrorist action modeling experts, and subject matter experts.

The Homeland Security Act of 2002 and other guidance such as *Homeland Security Presidential Directive 7* (HSPD-7) advocate the use of risk management to protect the nation's CIKR. HSPD-7, in particular, directed DHS to establish uniform policies, approaches, guidelines, and methodologies integrating Federal infrastructure protection and risk management activities. The Government Accountability Office (GAO) developed an overall risk management framework using a variety of industry, government, and academic sources of information. That framework outlines an iterative process that focuses on identifying the objective, assessing risk, identifying options for mitigating actions, selecting and managing the best options, and implementing those actions and monitoring the overall process. Figure 2 displays the framework graphically.

Small Vessel Risk Components

Threat

As defined, threat is an indication of the likelihood that a specific type of attack will be initiated against a particular target or class of targets. It may include any indication, circumstance, or event with the potential to cause the loss of or damage to an asset. Generally, the threat component of risk is determined by capability (resource implications), and intent (political or other motives). Intent is the most difficult variable to determine, the one most amenable to change, and the quickest way to increase threat and modify the risk assessment. Analysis of threat-related data is a critical part of risk assessment. Information for characterizing threat can be gained from a variety of sources, such as the intelligence and law enforcement communities, as well as from past activities of various enemy groups and entities. Understanding an underlying pattern of attacks on target types is useful in predicting future adverse events and planning mitigation strategies. However, threats not supported by historical data must also be considered. Ultimately, one purpose of assessing threats is to assign relative probabilities to various types of attacks.[14]

[13] *Critical Infrastructure Identification, Prioritization, and Protection (*Homeland Security Presidential Directive–7).

[14] *Risk Management*, GAO-06-91, December 2005, p. 25.

Overall Vulnerability

As stated, the vulnerability of an asset is an indication of the likelihood that a particular attempted attack will succeed against a particular target or class of targets. It is usually measured against some set of standards, such as availability/predictability, accessibility, and available countermeasures. Each of these elements can be evaluated based on a numerical assignment corresponding to the conditional probability of a successful attack. The probability that a particular vulnerability could be successfully exploited is, in part, a function of the effectiveness of countermeasures.[15]

The vast majority of small vessel operators are legitimate, law-abiding individuals. However, the large numbers of small vessels and the dearth of information regarding the user, owner, or operating patterns of those vessels make it extremely difficult to precisely identify the population and distinguish legitimate users from those with the intent to do harm. When evaluating and addressing the risks, law enforcement agencies are faced with sorting through thousands of small vessels, which can be closely intermingled with large commercial cargo vessels, cruise vessels, military warships, and critical infrastructure, at or near hundreds of seaports, along thousands of miles of U.S. coastline and navigable waterways, or originating from foreign waters.

[15] *Risk Management*, GAO-06-91, December 2005, p. 25.

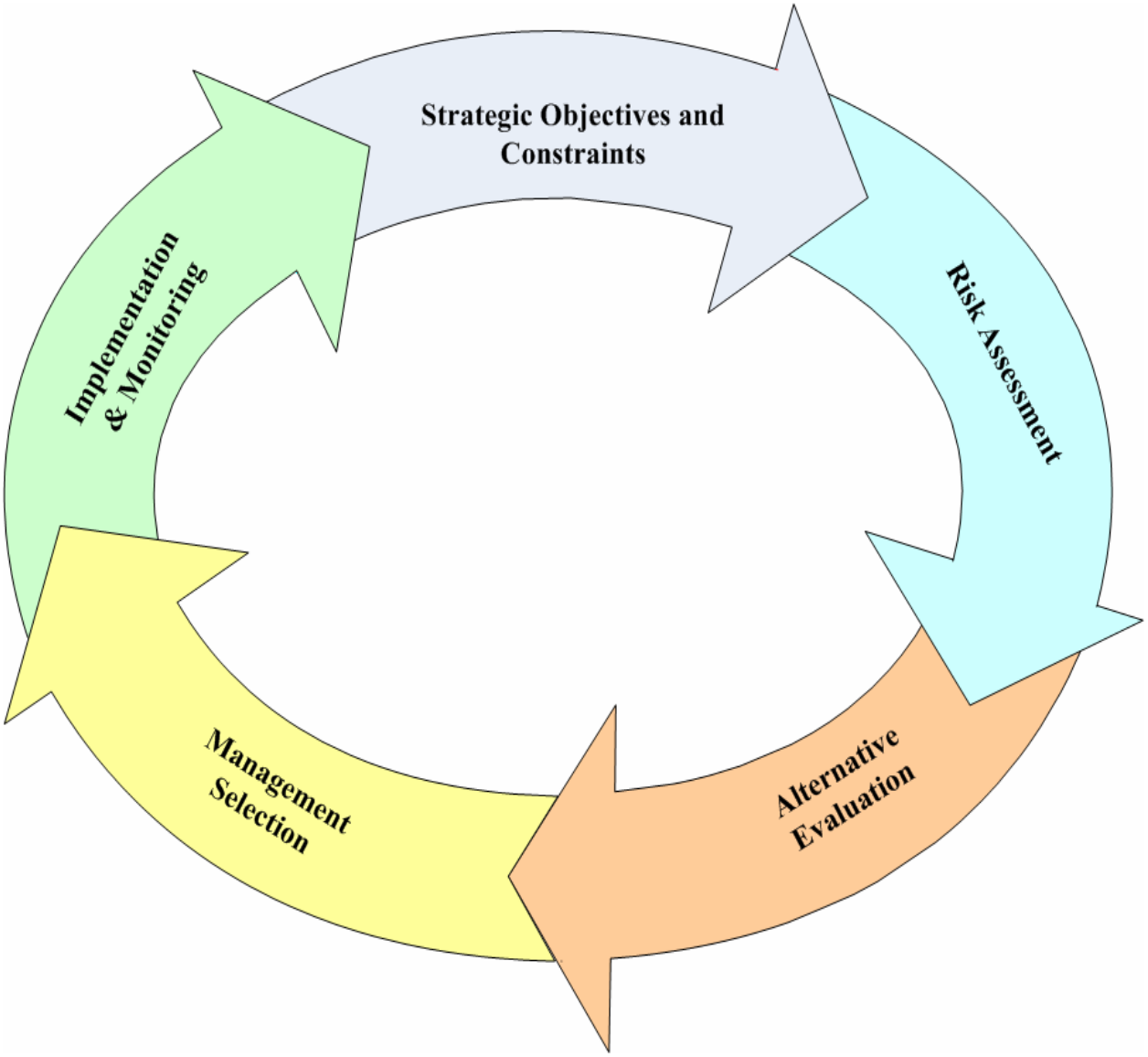


Figure 2, United States Government Accountability Office (GAO) Risk Management Framework

Small vessels possess complex characteristics, which also present unique challenges in assessing risks related to their presence in the maritime domain. The most obvious is simply the sheer number nationwide. There are 13 million registered recreational vessels throughout the country and perhaps an additional four million unregistered recreational boats. Further, there are 110,000 commercial fishing vessels as well as thousands of towing vessels and uninspected passenger vessels operating within the maritime domain. Each of these disparate types of small vessels have different operating patterns, economic factors, and interested stakeholder groups.

Many sites of CIKR in the maritime domain are vulnerable to small vessel attacks. Additionally, small vessels routinely operate within close proximity of high-profile targets such as

passenger craft, large commercial or cargo vessels, military warships, major bridges, critical waterfront industries, and other maritime infrastructure. The exact number of all small vessels operating in proximity of maritime infrastructure at any given time is also a key factor in CIKR vulnerability.

In 2007, the USCG Research and Development Center sponsored a study of nine U.S. ports and determined that there were approximately 3,000 small commercial vessels, 3,000 fishing vessels, and 400,000 recreational vessels that either must or are likely to operate in the vicinity of important maritime infrastructure within those ports.[16]

Overall Consequence

As defined earlier, consequence of a terrorist attack is the magnitude of the adverse impact of a successful attack. Depending on its magnitude, consequence can easily be a dominant driver in the overall risk calculation for many threats.

The primary consequence of a terrorist incident (as well as other Transportation Security Incident (TSI)[17]) arising from the use of a small vessel with conventional weapons could be devastating for the U.S. economy if it damaged CIKR or resulted in closure of the port. A 10-day labor dispute closed West Coast seaports in 2002. One estimate[18] placed the cost to the national economy for the first five days of this closure at $4.7 billion and increased exponentially after that. The consequences of a WMD release via small vessel would be worse.

Coastal waters and adjacent lands are some of the most productive and active areas of the United States. U.S. coastal communities are major population and economic centers, which generate over 60 millions jobs and about half of U.S. GDP—approximately $4.5 trillion. According to the 2000 U.S. Census, 53% of Americans live in coastal watershed counties. Additionally, 85% of Americans live within 100 miles of the nation's coasts. In 2004, close to 75 million Americans were directly involved in on-the-water activities and 90 percent of international trade by weight was carried by sea. Much of the U.S. critical infrastructure and key resources is located near the maritime domain. The great diversity and redundancy of the nation's CIKR provide for significant physical and economic resilience in the face of terrorist attacks, natural disasters, and other emergencies, and contribute to the strength of the nation's economy. However, this vast and diverse aggregation of highly interconnected assets, systems, and networks present an attractive array of targets to terrorists.

Any large-scale incident would also create other long-term, cascading, adverse effects. By way of example, following Hurricanes Katrina and Rita, large segments of the population moved away from the Gulf Coast — particularly in New Orleans — thereby causing a secondary consequence. The loss of population further harmed the Gulf Coast's economy as a tertiary consequence. The direct loss of power also disabled pumps in the petroleum pipelines across the southern United States. This negatively impacted gasoline stocks throughout the nation. One can imagine the multifold consequences of a terrorist attack using a weapon of mass

[16] *An Assessment of Small Vessel Populations in U.S. Waters*, prepared for the U.S. Coast Guard Research and Development Center by Potomac Management Group, Inc., June 2007.

[17] Section 70101(6) of Maritime Transportation Security Act of 2002

[18] Zeigert, Amy, et. al. "Port Security: Improving Emergency Response Capabilities at the Ports of Los Angeles and Long Beach." *California Policy Options 2005*. University of California Los Angeles, School of Public Affairs (Los Angeles, Calif. 2005).

destruction (WMD), including the mass casualties, devastation to infrastructure, and environmental fallout. A 2006 study[19] examined the potential effects of a 15-day port closure at Los Angeles-Long Beach due to a radiological bomb. It estimated the economic impact at $34 billion.

Specific Risk Scenarios

Small vessel risks have been assessed at the national level through various studies and have helped drive strategic decisions and planning efforts. The USCG's *National Maritime Security Risk Profile* (2003-2004) and *National Maritime Security Risk Assessment* (of 2004 and 2006) are two prominent examples. However, the security-sensitive or classified nature of the details of these studies and of the components that determined the overall risk levels precludes detailed discussion in this strategy.

The four scenarios of gravest concern in using small vessels in terrorist-related attacks have been identified as:

a. Domestic Use of Waterborne Improvised Explosive Devices (WBIEDs);

b. Conveyance for smuggling weapons (including WMDs) into the United States;

c. Conveyance for smuggling terrorists into the United States; and

d. Waterborne platform for conducting a stand-off attack (e.g. Man-Portable Air-Defense System (MANPADS) attacks).

[19] "The economic impact of a terrorist attack on the twin ports of Los-Angles-Long Beach" in *The Economic Impacts of Terrorist Attacks* (2006).

The USCG Intelligence Coordination Center provided information to this strategy regarding the viability of various threats from the exploitation of small vessel characteristics. Overseas terrorists have demonstrated the ability to combine the elements of capability, opportunity, and intent on several occasions, as noted in the list of attacks below on maritime assets and personnel.

a. Domestic Use of Waterborne Improvised Explosive Devices (WBIEDs)

There are numerous examples overseas of the use of small vessels as a waterborne improvised explosive device (WBIED) to attack maritime targets. These tactics could be applied against the United States and its interests to attack vessels, infrastructure, and industry (such as refineries and chemical plants) in the maritime domain. While not an exhaustive list, the following represents a range of high-profile tactics and targets that could be replicated in the United States.

- In August 2005, Turkish authorities arrested Louai Sakka, a senior al-Qaeda operative when a one-ton bomb he designed detonated prematurely. Sakka had intended to place the bomb on a yacht and ram a cruise ship carrying vacationing Israeli and U.S. soldiers on rest and recreation in Antalya, Turkey.
- In April 2004, terrorists using two fishing dhows packed with explosives attacked an Iraqi offshore oil terminal in the North Arabian Gulf, killing one U.S. Coast Guardsman and two U.S. Navy sailors protecting the terminal as they prepared to search one of the boats.
- In October 2002, Al-Qaeda directed an attack by an explosive-laden small boat against the French oil tanker M/V LIMBURG off the coast of Yemen. The attack resulted in fires on board the

tanker, a large oil spill, and killed one and injured four crew members.

- In October 2000, Al-Qaeda attacked the USS COLE and killed 17 U.S. Navy sailors by navigating an explosive-laden small boat alongside the destroyer as it was refueling pier side in Aden, Yemen.
- The Liberation Tigers of Tamil Eelam (LTTE) have conducted numerous successful suicide attacks using small boats against the Sri Lankan Government and its assets. Their attacks have destroyed or damaged several civilian and military vessels.

Significant naval assets, CI, and KR such as offshore oil platforms, merchant vessels (including oil and chemical tankers), and passenger vessels (such as ferries and cruise ships) operate in areas that are frequented by small vessels. Small vessels may easily blend or disappear into other vessel traffic in ports and the coastal maritime environment, and are usually subject to less scrutiny than larger vessels in these areas. They are often inconspicuous, fast, highly maneuverable, and able to quickly relocate via roads and surface transportation, making them particularly dangerous and lethal if used as WBIEDs. Additionally, operators do not require extensive training or large crews, and these vessels can be acquired relatively easily and inexpensively, thereby making them a very attractive and available mode of attack.

The use of a small vessel as a WBIED also has potential consequences that would exceed the immediate casualties or damage caused by the attack. For instance, the U.S. military relies heavily on the maritime transportation system (MTS) to deliver equipment and supplies to forces abroad, as most of American military power is transported by sea through Department of Defense (DOD) facilities at 15 key seaports. A successful WBIED attack, particularly at one of these military ports, has the potential to seriously disrupt movement of arms, ammunition, military supplies, and military units, depending on the intensity of the strike. As shut downs of certain West Coast ports during a labor dispute demonstrated, the impacts of even a temporary disruption of the maritime transportation system can be substantial.

b. Conveyance for smuggling weapons (including WMDs) into the United States

One of the gravest maritime risks facing the nation is the potential for a terrorist group to obtain a WMD and detonate it within the confines of a major U.S. port city, military installation, or industrial facility. Closely aligned with this is the potential for the maritime domain to be used as a transportation system for such a weapon, weapon materials, or its components, with an eventual target further inland.

The 2007 National Intelligence Estimate (NIE), "assesses that al-Qaeda will continue to try to acquire . . . radiological and nuclear material and would not hesitate to use them if it develops what it deems is sufficient capability." While there is no evidence that they possess WMDs at this time or that they intend to use small vessels as a means of transport to the United States, the use of small vessels to smuggle drugs and other contraband into the United States is instructive as to our vulnerability to the exploitation of small vessel characteristics to smuggle WMDs into the United States.

A nuclear weapon could be concealed on many vessels that meet the small vessel criteria. For instance, an improvised nuclear device (IND),[20] which might be smaller and less cumbersome than a nuclear weapon, presents an even more plausible scenario for transport via a small vessel. Furthermore, a terrorist organization would not necessarily have to transport a fully

[20] Improvised Nuclear Device (IND)—essentially a cruder version of a nuclear weapon fabricated by a terrorist organization or rogue nation.

assembled weapon. The parts and technology, required for assembling an IND could be well hidden on a small vessel. Additionally, the small vessel itself could readily serve as a platform from which to detonate a nuclear weapon, IND, or radioactive dispersal device (RDD)—commonly referred to as a "Dirty Bomb."

Fissile material is the most difficult component of a nuclear weapon to obtain. Because the material is better secured in U.S. facilities, it more probably would be acquired by a terrorist organization overseas where some of the larger and less well secured potential sources for nuclear weapons and materials exist. These weapons or materials would be more likely to be transported via maritime modes. Small vessels provide a clear opportunity for terrorists to retain control of the WMD and activate it at the optimum times.

The consequences of a WMD attack anywhere in the United States could be catastrophic, and potentially include millions of people killed and injured, billions of dollars in direct and indirect economic losses, and adverse environmental effects including the contamination of the impact area with subsequent loss of its use for decades.[21] While an RDD would likely result in far less casualties than a nuclear weapon/IND, it could also easily cause economic disruption in the billions of dollars coupled with a devastating psychological effect on the nation.

c. Conveyance for smuggling terrorists into the United States

In September 2007, 10 people dressed in black arrived in San Diego, California aboard a 20-foot skipjack, which they abandoned at Wipeout Beach. The boat was registered to a San Diego resident who sold it in 2002 and had not been registered since.[22]

Undocumented maritime migration and smuggling threatens the United States from all sides. Illegal landings have occurred along the entire Eastern and Western seaboards, as well as from every U.S. territory. Since 1980, the USCG, working with other Federal, state, and local law enforcement authorities, has interdicted over 320,000 illegal maritime migrants from 47 different countries. In 2004, there were approximately 5,000 successful arrivals of illegal maritime migrants.[23] These numbers are primarily from small vessel arrivals as opposed to absconders from large commercial vessels. Any one of these arrivals could potentially be a terrorist.

The number of people entering the country illegally between ports of entry, and the concomitant proliferation of human and drug smuggling networks, present clear risks to U.S. national security due to the ever-present threat of terrorism. Terrorists and terrorist organizations could leverage these illicit networks to smuggle operatives into the United States, while the large number of aliens attempting to enter the country illegally could potentially provide cover for the terrorists. A particular concern has been that terrorists may take advantage of numerous criminal networks and exploit small vessels as low-profile modes of transportation to smuggle dangerous people and materials into the United States, thereby circumventing more-stringent land border security measures. Additionally, the proceeds from these smuggling networks could potentially be used to finance terrorist activities.

[21] Abt, Clark C. "The Economic Impact of Nuclear Terrorist Attacks on Freight Systems in an Age of Seaport Vulnerability," (Cambridge, MA, 2003), pp. 3-4.

[22] Baker, Debbi Farr. *The San Diego Union Tribune*, September 5, 2007. http://www.signonsandiego.com/news/metro/20070905-0841-bn05boat.html

[23] GAO-05-364T Coast Guard Budget Priorities, p. 31.

d. Waterborne platform for conducting a stand-off attack (e.g., Man-Portable Air-Defense Systems (MANPADS) attacks).

The use of a small vessel as a platform for conducting a stand-off attack is viable. In November 2005, a cruise ship 100 miles off the coast of Somalia was attacked by two 25-foot rigid hull inflatable boats. The pirates used rocket-propelled grenades and automatic weapons at a distance of no more that 25 yards from the SEABOURNE SPIRIT. The pirates were ultimately repelled by the ship's crew using a device that generated disabling sonic blasts.

It is technically feasible to launch a ballistic missile from a ship as small as 200 tons against the United States. A substantial, cooperative effort between the ship's crew and missile launch personnel would be required to achieve a successful launch.[24]

The exploitation of a small vessel to provide a stand-off attack platform provides numerous benefits for terrorists. The use of a small vessel as a stand-off weapon platform provides greater operational security, improved access to targets (bypassing shore-side security measures), and a ready means of escape. It also increases difficulty for protecting assets due to the relative quickness and maneuverability of many small vessels in evasive situations.

The result of a successful stand-off attack could disrupt the nation's transportation system and economy. In several locations across the United States, citizens rely on ferry service for daily commuting, as well as for travel and recreation. The ferries that transport passengers and vehicles across bays and channels provide critical links within the marine transportation system, serving as an essential means of transportation for more than 64 million individuals annually. Cargo is also continuously transported on water by thousands of ships, vessels, and barges via the inland and coastal waterway systems and oceans. Key energy resources, such as coal for electrical power plants, petroleum products, and grain for export to global trading partners, move on the U.S. waterway system daily. We could see significant impacts on cargo and general transportation insurance rates, even after a minor but successful attack.

These four scenarios illustrate some terrorist groups' prior history of using small vessels in suicide operations overseas, a history which, combined with some groups' stated objective to attack the United States, supports a determination of significant potential risks to the United States. This strategy addresses those risks.

[24] Defense Intelligence Agency/Missile & Space Intelligence Center response to PR R205-08-0005-S dated 31 January 2008.

STRATEGIC VISION

GUIDING PRINCIPLES

In pursuing the strategic goals, DHS is guided by the following principles. These are underlying concepts that will inform and frame development and implementation across all goals, priorities, objectives, and action plans.

- Risk based decision making will be necessary to best channel actions and finite resources.
- Efforts to enhance security may improve small vessel safety and operator education, thus the security strategy builds on existing safety frameworks
- Risk mitigation efforts must be designed so as to strike the delicate balance and tradeoffs between personal freedom, national security, and commerce.
    - Small vessel risk reduction efforts should not impede the lawful use of the maritime domain or the free flow of legitimate commerce.
    - Small vessel risk reduction efforts will include ongoing engagement with the small vessel community, as well as other key stakeholders in order to ensure that potential solutions reflect their interests and to benefit from the collected wisdom of the small vessel community in crafting solutions.
    - Successful small vessel risk reduction will require close coordination and cooperation between Federal agencies, state, local, and Tribal governments, as well as private and international partners.
- A one-size-fits-all approach cannot adequately ensure U.S. maritime security and safety due to the diversity of the maritime domain and the heterogeneity of the small vessel community. These complexities require the implementation of a national framework, within the scope of international standards, which can be properly tailored to local situations.

- Maritime security and safety depends upon the successful implementation of an interlocking system of governance comprised of maritime regimes, domain awareness, and operational capabilities.
- Authorities at every level will be able to identify shore vulnerabilities and potential targets, and work with private entities to establish appropriate protection plans to ensure shore security.
- Technology will serve as an important, complementary component to enhance subsequent plans, initiatives, and actions (such as increasing MDA), but it is not the sole answer to ensure small vessel security. Additionally, leveraging technology will mitigate risks but should also minimize impacts to small vessel operators.

OVERARCHING VISION AND MAJOR GOALS

Overarching Vision

The SVSS aims at ensuring the maritime domain remains a secure environment, where small vessel operators are able to safely earn a living, travel, and recreate freely, without unduly burdensome government regulations and with the freedom to sail upon the navigable waters of the United States.

The institution of a system of effective regimes, awareness, and operational capabilities allows government agencies at the Federal, state, local, and Tribal levels to determine which of the millions of small vessels plying U.S. waters present an undue risk to homeland security.

Ultimately, we want to be able to easily identify the few threatening vessels from among the millions that legitimately use U.S. waterways. All government agencies, along with international partners, must work in a concerted effort to manage and reduce risks, and have sufficient awareness to clearly distinguish between legitimate and illegitimate uses.

Major Goals

A. Develop and leverage a strong partnership with the small vessel community and public and private sectors in order to enhance maritime domain awareness.

It is imperative that efforts focus on building partnerships and trust with recreational boaters and professional mariners who operate small vessels.

Again, the vast majority of professional and recreational operators are law-abiding and safe users of the maritime domain. It is imperative to enlist their aid as close allies in identifying threats and reporting suspicious activities emanating within the small vessel community. Hence, special care must be directed at providing opportunities and venues for a continuous dialogue the small vessel community to encourage the free and regular flow of information and ideas between the private sector and Federal, state, local and Tribal authorities and non-governmental organizations.

The small vessel community is the single largest asset in the efforts to mitigate small vessel-related security risks. As many as 80 million individuals participate in recreational boating activities each year. By formally educating small vessel operators with respect to the risks faced and suggesting methods to address those risks (reporting, security measure protocols, etc.), small vessel users become an effective agent for reducing risk and increasing security.

Two effective means for the public to report suspected terrorist activity are to telephone America's Waterway Watch (AWW) or the National Response Center (NRC).

A prime example of the value of AWW occurred in 2003 when a tour boat operator in Florida reported suspicious activity by one of the passengers. The call led to the investigation of the suspect and his apprehension in Brooklyn, New York.[25] Between 2002 and 2006, the NRC received 646 reports of suspected terrorist activity.

[25] During a series of several meetings with an undercover agent, the suspect attempted to buy five bulletproof vests, night vision goggles, a camera for the front of his car, 50 sleeping pills, 100 Valium pills and a half-case of C-4 for $10,000. *N.Y. Man Arrested for Allegedly Trying to Buy Explosives*, CNN.com, May 22, 2003 accessed at http://edition.cnn.com/2003/US/Northeast/05/22/explosives.arrest/index.html on September 26, 2007.

Goal A—Specific Objectives

Develop and leverage a strong partnership with the small vessel community and public and private sectors in order to enhance maritime domain awareness.

i. Provide opportunities and adequate venues for an ongoing dialogue with the small vessel community to encourage the free flow of information and ideas between the private sector, the Federal Government, and state, local, Tribal, and territorial authorities.

ii. Expand local-level constituent relationships with other maritime organizations such as paddle sports, sport fishing associations, and port authorities.

iii. Move towards a knowledgeable small vessel community through a common, efficient, accessible, and easy to use lessons-learned system from exercises, real life events, peer review, and formal—but simple and inexpensive—instruction.

iv. Leverage existing education and outreach programs, such as those provided to the small vessel community by the USCG Boating Safety Division, USCG Auxiliary and partnerships with the U.S. Power Squadrons to provide both security and safety training.

v. Increase public awareness of how to report suspected terrorist activity via America's Waterway Watch (AWW).

B. Enhance maritime security and safety based on a coherent plan with a layered, innovative approach.

Small vessels will be screened according to the realistic risk they pose, the surrounding operating environment, and all available intelligence. To improve the overall small vessel security enforcement posture, it is important to identify which operators present a low-risk profile, and develop appropriate risk targeting systems to distinguish high-risk users. DHS agencies with jurisdictions that include the maritime domain should utilize data gathered from multiple sources, such as the Pleasure Boat Reporting System (PBRS), the Vessel Identification System (VIS), the Marine Information for Safety and Law Enforcement (MISLE), available intelligence, and in coordination with the Department of State, foreign governments, and trusted traveler programs. In doing so, they will develop and improve methods to appropriately analyze and target high-risk small vessels, while developing a more concrete understanding of the small vessel landscape.

The Department of Commerce's National Oceanic and Atmospheric Administration (NOAA)'s Office of Law Enforcement maintains a Vessel Monitoring System (VMS) that currently tracks over 5,900 small vessels with an anticipated expansion of another 2,500 vessels this calendar year. In addition, NOAA maintains law enforcement information on small vessels through its Law Enforcement Accessible Database System (LEADS) that tracks investigations, incidents, activities, and outreach.

The analysis of a broad set of information will not only allow enforcing authorities to identify specific threats, but also enable the development

of trends and fusing of potential intelligence related to the small vessel operator population and related security risks. Improving information analysis and sharing—especially between the law enforcement and intelligence communities and, in coordination with the Department of State, with foreign governments—will enable authorities to specifically target threats related to WMDs or WBIEDs. Overall, this will improve capabilities at the operational and tactical levels and allow better allocation of resources, particularly in emergency situations.

Additionally, improving reporting procedures is essential to increasing reporting compliance and gathering data for risk-based efforts. As such, obtaining advance data for international traffic, such as the 96-hour Notice of Arrival rule, will allow the USCG and CBP to conduct the necessary risk-based analysis, gain situational awareness of small vessels, and improve the overall MDA. The submission of basic—but essential—information on recreational vessel operators in advance of U.S. arrival and departure will enable consistent enforcement prioritizations and responses. These simple reporting requirements will also improve the effectiveness of risk assessment efforts.

A layered innovative approach does not necessarily mean all risk-mitigation actions will be technologically based. Many times, the simple expedient of installing effective barriers around critical infrastructure and key resources will eliminate most vulnerability to terrorist use of small vessels as a WBIED. In order to develop and maintain effective layered security, Federal, state, local, and Tribal officials must work in conjunction with their international counterparts and private sector representatives to provide adequate security for CIKR.

Goal B—Specific Objectives

Enhance maritime security and safety based on a coherent plan with a layered, innovative approach.

i. Improve detection and tracking capabilities to better identify small vessels operating in or near U.S. waters.
ii. Develop a robust layered defense by expanding and enhancing maritime radiological/nuclear detection capabilities to international, Federal, state, local, Tribal, and private stakeholders.
iii. Implement basic procedures on advanced data submission and increase reporting compliance to improve situational and maritime domain awareness.
iv. Improve efforts to gather and share data on small vessels and their operators.
v. Improve data analysis capabilities to target high-risk small vessels.
vi. Assess, develop, and improve layered security for critical infrastructure and key resources.

C. Leverage technology to enhance the ability to detect, determine intent, and when necessary, interdict small vessels.

Surveillance of the entire maritime domain and the tracking of all small vessels are not contemplated by this strategy. Consistent with applicable privacy laws, increased surveillance and tracking may be appropriate, though, along the maritime border and in high risk, high traffic areas. Technology improvements will be central to those efforts. Security technology is continuously evolving in terms of compatibility, standardization, and integration with information systems. Yet, technology is not the single solution that can realize complete security for the small vessel environment. Instead, it is part of a larger layered security approach that can mitigate small vessel risks. Technology applications may improve the ability to identify threats early—through proper identification protocols—and may improve the effectiveness of response operations.

As technology matures, new tools will be constantly evaluated in order to adapt new systems to small vessels—taking into account security requirements and operator preferences. Hence, efforts should be directed to the implementation of effective security solutions that increase MDA, clearly identify dangerous small vessels, and ensure an appropriate level of privacy for law-abiding operators.

New detection capability will need to be developed to address the vulnerabilities and risks due to the exploitation of small vessel characteristics, such as advanced human portable radiation detection systems and mobile standoff radiation detectors. The existing and new detection capability should be deployed to Federal, state, local, and Tribal agencies operating on or near the water to improve the nation's layered defense against terrorists exploiting small vessels.

Research and development play an important role in fulfilling this objective, since applicable technologies must operate within critical areas of the maritime domain. To be useful, information obtained must be processed efficiently and rapidly, and incorporated into the normal screening procedures and daily operations of local authorities and law enforcement agencies. Ultimately, preventive measures, such as providing the necessary, timely, and critical information to key decision makers, will reduce the security risks of small vessels operating in the maritime domain.

Goal C—Specific Objectives

Leverage technology to enhance the ability to detect, determine intent, and when necessary interdict small vessels.

i. Expand research into and invest in prototyping low-cost, non-intrusive, small vessel identification systems, such as Radio-Frequency Identification (RFID) tags, adaptable miniature transponders, portable Global Positioning System (GPS) devices, or cell-phone based recognition systems.

ii. Expand research into and invest in anomaly detection instruments and other decision aids such as automated scene understanding tools.

iii. Expand research into methods of protecting critical infrastructure and key resources, especially at shorelines, through means such as small boat barriers, unambiguous warning devices, and non-lethal deterrents such as sonic canons.

iv. Improve maritime domain awareness capabilities to adequately distinguish between and respond to intentional and innocent intrusions into security and safety zones.

v. Expand research into and invest in advanced maritime radiation/nuclear detection technology for human portable radiation detection equipment, mobile standoff radiation detectors, and fixed detectors that could be deployed on or near the waters in the vicinity of small vessels.

D. Enhance coordination, cooperation, and communications between Federal, state, local, and Tribal partners and the private sector as well as international partners.

The size and the scope of the maritime domain, and the number of small vessels actively engaged in its use, make it virtually impossible for any single government entity at any level to have sufficient information, resources, expertise, or statutory authority to address the spectrum of potential risks related to small vessels. Only through concerted coordination, continuous cooperation, and diligent communications between Federal, state, local, and Tribal agencies can the potential risks from small vessels be adequately addressed without adversely impacting the legitimate use of the maritime domain.

Federal Agencies, where appropriate, will use the Maritime Operational Threat Response (MOTR) Plan in accordance with current directives to optimize employment of all appropriate resources in order to interdict threats as far from U.S. shores as practicable. The MOTR Plan sets forth lead and supporting Federal agency roles and responsibilities for MOTR based on a number of criteria including: existing law; desired U.S. Government outcome; greatest potential magnitude of the threat; the response capabilities required; asset availability; and authority to act. The MOTR plan directs clear coordination relationships and operational coordination requirements among the lead and supporting MOTR agencies, enabling the U.S. Government to act quickly and decisively to counter maritime threats. The plan also sets forth protocols for interagency coordination, consultation, and assessment throughout MOTR execution.

Non-governmental organizations (recreational boating, maritime exchanges, manufacturing associations, pilot associations, and commercial

operator associations, etc.) as well as private entities share many of the same concerns and responsibility for protecting CIKR and the MTS. These private actors have intimate knowledge of their own facilities and sphere of influence. Working with the various non-governmental organizations is more effective than trying to work with individual small vessel community members. The various non-governmental organizations provide a centralized point of contact on behalf of their members and have the ability to efficiently communicate with them.

DHS agencies will work with Canadian, Mexican, Caribbean, and other foreign counterparts to develop coordinated enforcement operations targeting high-risk small vessels. This will ensure maritime assets and response capabilities are properly distributed to provide appropriate coverage of the maritime border, consistent with current intelligence and the maritime threat. DHS agencies should cross-train, conduct personnel exchange programs, and develop clear standards of performance to best coordinate information sharing and appropriate enforcement actions.

In addition, DHS will continue to work with our foreign counterparts to coordinate enforcement operations, and will continue to work with international maritime organizations such as the International Maritime Organization (IMO) and World Customs Organization (WCO) to develop international standards applicable to small vessels.

Goal D—Specific Objectives

Enhance coordination, cooperation, and communications between Federal, state, local, Tribal, and territorial agencies, the private sector, and non governmental organizations as well as international partners.

i. Improve coordinated small vessel interdiction capabilities and operations.

ii. Leverage the capabilities of domestic partners and foreign governments through sharing of information.

iii. Where appropriate, establish programs where law enforcement authorities from different nations combine efforts in cooperative patrol and enforcement.

iv. Make it a priority, consistent with available funding and in accordance with agency resourcing plans, to integrate officers and intelligence analysts from the USCG, CBP, and Immigration and Customs Enforcement (ICE) into participating state, local, and regional fusion centers located in jurisdictions along maritime borders of the U.S.

v. Update Area Maritime Security (AMS) processes to insure that small vessels are addressed when conducting AMS assessments and developing AMS Plans (AMSPs).

RISK MANAGEMENT

Given the size and complexity of the maritime domain, risk-based decision making is the only feasible approach to prevention, protection, response and recovery related to small vessel threats. This risk-based SVSS will be applied across the maritime domain, the high seas, and foreign ports. The success of this strategy will hinge upon the informed and effective employment of risk management, which will also inform decisions about resources and investments in risk-mitigation actions.

Maritime security partners will mitigate a risk posed by terrorist use of small vessels by conforming to the following five phases of the GAO risk management framework:

1. Strategic Objectives and Constraints
   - Ensure all actions are firmly aligned with articulated goals and objectives, keeping a clear focus on the desired "end state."
   - Identify high-risk scenarios and/or locations.
2. Risk Assessment
   - Assess current and forecast threats, vulnerabilities, and consequences.
3. Alternative Evaluation
   - Develop various risk mitigation actions, coordinating efforts, where prudent.
   - Develop quantifiable performance objectives for each risk-mitigation action under consideration.
4. Management Selection
   - Select appropriate risk mitigation actions and coordinate funding.
5. Implementation and Monitoring
   - Implement risk mitigation actions.
   - Assess attainment of each performance objective.

   - Make adjustments in DHS resources and investments to better attain performance objectives.
   - Consider new risk mitigation actions.

Within this construct, maritime security partners should continue to undertake activities and initiatives aimed at mitigating risks associated with small vessels. Coordinating and achieving synergy among these efforts will reap benefits and should include:

Maritime Regimes

- Update Area Maritime Security Plans (AMSP), and Vessel and Facility Security Plans as required by the Maritime Transportation Security Act of 2002 (MTSA) to reflect small vessel security issues.
- Assess the benefits and costs of legislative and regulatory options pertaining to enhanced registration and reporting of small vessels.
- Tailor domestic and international outreach programs to small vessel security.
- Identify and evaluate alternative law enforcement and defense operations/legislative initiatives.

Maritime Domain Awareness

- Review MDA initiatives and programs and, when appropriate, expand to include small vessels.
- Support the AWW program to provide enhanced public outreach and education programs and evaluate potential expansion.
- Review and where possible improve the Domestic Nuclear Detection Office (DNDO) *Maritime Program Strategy* to support initiatives that will reduce the risk of small vessels smuggling illicit nuclear and radiological weapons and material into the United States.

Maritime Operational Capabilities

- Coordinate operational security activities closely through interagency operations centers.
- Use DHS adaptable capabilities packages to augment the security of the maritime domain. Adaptable capability packages do not replace statutory missions, existing contingency plans, or other established processes, but they facilitate DHS-wide planning, support, prevention, detection, disruption and mitigation activities associated with threats against and incidents affecting security interests through the integration of internal agency operational assets.
- Employ law enforcement resources as appropriate to augment response and prevention activities within the maritime domain of the United States.
- Employ Research and Development (R&D) capabilities undertaken within DHS Science and Technology (S&T) Directorate to support expanded small vessel security.

Maritime security partners and the American public are encouraged to recommend additional approaches to further mitigate small vessel risks through Area Maritime Security Committees (AMSC) and other public forums. Such improvements and recommendations will be promptly evaluated by the appropriate entities and implemented where prudent.

Relative Risk Reduction from Various Activity Groups

The risk reduction analyses conducted as part of the USCG's *Combating Maritime Terrorism* (CMT) Campaign Plan have identified key groups of activities that contribute to risk reduction. The activity groups that resulted in the greatest reduction in evaluated risk areas were:

Maritime Regimes

- Control Port Access
- Vessel and Facility Security Compliance

Maritime Domain Awareness

- Surveillance of high risk areas and activities
- Information collection and sharing

Maritime Operations

- Boarding of Suspect Vessels
- Use of Specialized Forces

(*Adapted from CMT Campaign Plan Table 4: Activity and Relative Risk Reduction*)

Figure 3, Key Activity Groups

Organizational Roles, Responsibilities, and Coordination

The movement of small vessels from origin to destination can be either a domestic or international evolution. In many cases, domestic jurisdictions overlap. For instance, both the USCG and CBP have specific jurisdictions within a port. Further complicating this maze of jurisdictions are cases where a foreign-flagged small vessel engages in innocent passage through U.S. territorial waters. Furthermore, every nation addresses its commerce, transportation, customs, and maritime systems differently.

While coordinating Federal and international roles and responsibilities is complicated; even more difficult is the coordination of roles and responsibilities between the Federal, state, and local governments and the private entities responsible for providing security from small vessel threats in our maritime domain. Given the number of state and local jurisdictions, the number of private entities involved, and the range of authorities and capabilities these groups have makes the development of a single national pre-established protocol for responding to incidents problematic. The implementation of local plans developed under the guidance of this Strategy will likely be more effective and allow consideration of local requirements.

Strictly from a U.S. perspective, the following descriptions are the primary functional responsibilities of U.S. entities with responsibilities involving small vessel regulation, customs, maritime security and safety; including prevention of activities that would result in a disruption of the maritime transportation system. Coordination of involved agencies in a disaster response scenario will be in accordance with the National Response Framework (NRF).

United States Federal Government Functional Responsibilities

The Federal agencies with regulatory, statutory and management responsibilities that impact small vessels are as diverse as the small vessel community. No single agency has sole or complete authority to act in all matters related to small vessel construction, registration, and operation. In order to effectively mitigate risks resulting from the misuse of small vessels, Federal agencies should coordinate in the development of regimes, awareness, and operational capabilities. Unity of effort is necessary to effectively reduce risk. This unity of effort must encompass state, Tribal, and local authorities as well. DHS will take the lead in identifying and coordinating organizational roles and responsibilities. In addition, DHS has a key role in the development and implementation of guidance or standards, as appropriate. Appendix A lists selected Federal agencies and departments with authorities and responsibilities in the maritime domain.

STATE, LOCAL, AND TRIBAL GOVERNMENTS

To enhance deterrence and improve preparedness, state, local, and Tribal governments must address prevention, response and recovery. Under the National Incident Management System (NIMS), these governmental entities have responsibility for incident management response and recovery efforts immediately after an incident. In dealing with the vulnerability and threat aspects of small vessel security risk, any planning initiatives should align with AMSPs through participation in AMSCs.

As responsibilities, capabilities, and organizational structures vary from agency to agency, specific functional responsibilities are not delineated in this strategy. State, local, and Tribal governments may each provide some assistance in the development of regimes, awareness and operational capability. However, to coordinate the Federal, state, local, and Tribal government relationships, the following generic list of functional responsibilities that state, local, and Tribal governmental agencies may perform was developed.

State Governments

- Coordinate state resources.
- Make, amend, and rescind orders and regulations under certain threat conditions in support of detection and prevention efforts as appropriate.
- Communicate to the public aspects of an emergency within state jurisdiction.
- Assist people, businesses, and organizations of the state or territory to cope with the consequences of terrorist activity.
- Encourage participation in mutual aid and implement authorities for the state or territory to enter into mutual aid agreements with other states, tribes, and territories to facilitate resource-sharing.
- Coordinate requests for Federal assistance when it becomes clear that state capabilities will be insufficient or have been exceeded or exhausted.
- Exchange information with other Federal, state, local, and Tribal government agencies.
- Participate in various advisory committees and task forces regarding maritime security.
- State boating law administrators develop, implement, and enforce safe boating standards and operator qualifications.
- Assist in the assessment of the economic impact caused by a TSI.
- Assist in the identification of response and prevention resources and assets.
- Provide resources as requested and as appropriate.
- Assist in assessment, implementation and improvement of security for critical infrastructure and key resources.

Local Governments

- Craft, manage, and maintain small vessel risk and threat mitigation and prevention plans.
- Perform emergency first-responder activities as appropriate.
- Coordinate local resources.
- Communicate to the public any type of local threat or declared emergency within the local jurisdiction.
- Assist people, businesses, and organizations in the local area with the prevention and possible consequences of any type of local threat or declared

emergency and its recovery considerations.

- Negotiate and enter into mutual aid agreements with other jurisdictions to facilitate resource-sharing.
- Request state and, if necessary, Federal assistance through the governor of the state when the jurisdiction's capabilities have been exceeded or exhausted, or otherwise as appropriate.
- Exchange information with other Federal, state, and Tribal government agencies.
- Participate in various advisory committees and task forces regarding security incident prevention and recovery management.
- Assist in the assessment of the economic impact created by a security incident.
- Assist in the identification of resources and assets.
- Provide resources as requested and as appropriate.
- Assist in assessment, implementation and improvement of security for critical infrastructure and key resources.

Tribal Governments

- Coordinate local resources.
- Communicate any type of declared emergency within Tribal jurisdiction.
- Assist people, businesses, and organizations to cope with the consequences of any type of security incident or declared emergency.
- Negotiate and enter into mutual aid agreements with other tribes/jurisdictions to facilitate resource-sharing.
- Request state and Federal assistance through the governor of the state when the tribe's capabilities have been exceeded or exhausted.
- Deal directly with the Federal government (although a state Governor must request a Presidential disaster declaration on behalf of a tribe under the Stafford Act, Federal agencies can work directly with tribes within existing authorities and resources).
- Engage in exchange of information with Federal, state, local, and other Tribal government agencies.
- Participate in various advisory committees and task forces regarding maritime security.
- Assist in the assessment of the economic impact created by a national TSI.
- Assist in the identification of resources and assets.
- Provide resources as requested and as appropriate.
- Assist in assessment, implementation and improvement of security for critical infrastructure and key resources.

PRIVATE SECTOR

As the principal providers of goods and services, and the owners or operators of approximately 85 percent of the Nation's critical infrastructure[26], the private sector plays the most important role in ensuring its overall security.

As a component of their business, private sector entities have responsibility for planning, operations, and advisory aspects relating to the safety and security of vessels, critical infrastructure and key resources.

[26] *National Strategy for Homeland Security* (October 2007) p. 4.

To assist the private sector in preparing for this role, DHS advocates, in accordance with the *Maritime Infrastructure Recovery Plan* the following:

- Private sector owners and operators of vessels and facilities subject to United States Government regulation are encouraged to expand their business continuity plans to include security incident prevention, detection and recovery operations as part of required planning pursuant to Federal regulations.
- Owners and operators of vessels and facilities not subject to United States Government regulation are encouraged to establish security incident prevention, detection and recovery operations and business continuity plans, in coordination with appropriate trade partners.
- All private sector security incident prevention, detection and recovery operation plans should include notification of appropriate local, state, and Federal government agencies. Plans should be industry specific and include: (1) a plan for reducing vulnerability to attacks; (2) a plan for evacuation or remaining, (3) adequate communications capabilities, and (4) a plan for business continuity, and any other area or industry specific concerns.

It is anticipated that the private sector will implement business continuity plans/operations plans on their own accord, based on information provided by the Federal Government. Information that may influence the decision to implement contingency plans and divert or redirect cargo and/or the conveyances include: national priorities; military requirements; MTS restrictions; and the expected duration of those restrictions.

To facilitate continued flow of commerce, the following list of functional responsibilities that the private sector may perform was developed as part of the *Maritime Infrastructure Recovery Plan*, and is applicable within the framework of this strategy:

- Participate in various maritime industry stakeholder professional organizations and advisory committees such as the AMSCs.
- Engage in exchange of information about recovery operations plans with other potentially affected private sector entities and the Federal Government to mitigate potential congestion at non-incident site ports following the diversion of vessel traffic.
- Assist in the assessment of economic impact.
- Assist in the identification of prevention and recovery resources and assets.
- Provide resources to assist in security and safety activities, as appropriate.
- Participate in pilot programs to test the effectiveness of the Federal Government to communicate security activities to the private sector.
- Using existing information-sharing mechanisms such as the National Infrastructure Coordinating Center (NICC), AMSCs, Transportation Sector Coordinating Councils and Information Sharing and Analysis Centers (ISAC), communicate situational and operational information as well as physical asset capabilities for mitigation management.
- In conjunction with Federal, state, local and Tribal authorities, assist in providing security for critical infrastructure and key resources.

INTERNATIONAL PARTNERS

Securing the maritime domain from the threats posed by small vessels is a global issue and will involve partnering with Canada, Mexico, Caribbean states, as well as other foreign governments. Additionally, combating terrorist exploitation of small vessels will require assistance from and close collaboration with all U.S. international partners.

International standards and cooperation can be developed in traditional international maritime organizations such as the IMO and WCO. Geographic proximity in areas such as the Great Lakes region and Caribbean will call for a strong regional approach. The easy transit of small vessels between the United States and various regional ports in the Western Hemisphere requires robust multinational agreements and support.

In addition to international organizations and regional compacts, bilateral cooperation with countries, which share our borders both in information sharing and joint-operations will allow us to expand our reach and provide a more effective deterrent.

AUTHORITIES

The maritime domain, given its complex set of interlocking jurisdictions and authorities, is subject to a vast collection of laws and regulations at the Federal, state, local, and Tribal levels. Appendix B contains some of the primary laws which provide the Federal government and its agencies with authority to act in the maritime domain.

EXISTING INTERAGENCY INSTITUTIONS

Interagency cooperation has long been a cornerstone of effective governance. Multiple interagency groups provide for effective communications and cooperation. Interagency institutions provide a means for all levels of government to combine their existing authorities and operational capabilities ensuring unity of effort and building the relationships necessary to foster cooperation and commitment to common goals. A number of interagency efforts already exist. Rather than creating new entities, existing frameworks will be utilized as mechanisms to coordinate efforts to reduce small vessel risks. Appendix C lists several interagency efforts that may be leveraged in the effort to reduce risks.

THE WAY AHEAD

Numerous prevention and response solutions have been developed in building a layered security system that is currently operating in the maritime domain. Many of these prior initiatives have focused on larger commercial vessels. Maritime security initiatives appropriate for larger vessels do not systematically transfer well to small vessels because of differences between the two communities.

In addition to the obvious difference of vessel size, two important characteristics of the small vessel community are the number and diversity of stakeholders involved. Thus, there is no unique representation of small vessel stakeholder issues that would address the disparate viewpoints in the community. Another difference is the little direct involvement or face-to-face interaction between small vessel stakeholders and international, Federal, state, local, and Tribal authorities, or commercial industry managers, that govern the use of the waterways in the maritime domain.

Challenges

The way ahead includes substantial challenges. The diversity and size of the small vessel community impedes efforts to develop unity of effort as the various stakeholders have diverse goals, experience levels, capabilities, resources, and expectations concerning use of U.S. waterways. Many stakeholders are inexperienced with respect to risk management and may have never interacted with the various layers of government. The lack of a common viewpoint leads to misunderstandings and confusion on all sides of the risk management effort.

In addition to cultural challenges, there are technical challenges to overcome. The development of reliable and cost-effective technology to detect, deter, and prevent terrorist

use of small vessels faces several hurdles. Any technology must be effective and complementary in a wide-range of applications, in a large geographic area, and be able to address a broad set of requirements. The expanded use of technology will require the integration of a diverse set of currently stove-piped capabilities.

Next Steps

The foundation of small vessel security efforts is a continued dialog with involved stakeholders. It is vital that we continue the discussion begun at the June 2007 DHS National Small Vessel Security Summit held in Arlington, Virginia. The summit was a solid starting point to hear from stakeholders and collect their input. It was the first national step, but there has to be an ongoing local interaction and discussion to ensure that local ideas, strategies, and concerns are addressed as implementation of the national strategy occurs in the local ports, coastal and inland waterways.

DHS officials must continue to reach out to counterparts in state, local, and Tribal governments. In coordination with the Department of State, DHS will communicate with international partners, as well as private sector entities. DHS will also continue to build

partnerships and cooperation across the entire small vessel community so that a coordinated system of regimes, awareness, and operations can effectively reduce risk in the maritime domain.

DHS will develop an implementation plan to provide detailed direction to DHS agencies on how to achieve the major goals outlined in this strategy. The implementation plan will include specific actions in support of each objective in this strategy and identify lead agencies and target completion dates. The implementation plan will make provisions for support of ongoing efforts with international partners, as well as linkages to all domestic stakeholders.

CONCLUSION

I will guarantee you one thing—the enemy is not wasting time. … Remind yourself about The Sullivans. Remind yourself about the Cole. Remind yourself about that French tanker, the Limburg. This attack technique … is one they have used before. It is one that they will likely use again. Let us work together to make our protections against this as robust as they can be in a way that preserves the traditional freedom of the seas, our economic mobility and our continued pleasure and boating on our oceans and in our waterways.

DHS Secretary Michael Chertoff
National Small Vessel Security Summit
June 19, 2007

This strategy is the initial step in identifying overriding goals and objectives in order to implement a coordinated and unified strategy for securing the small vessel environment. An in-depth, risk-based security program must be coordinated in a multi-layered system that includes international, national, state, local, Tribal, and industry partners.

Yet, no single strategy can possibly address all areas of a topic as complex as small vessel related risk. This strategy and its implementation plan constitute the basis of the ongoing effort to reduce risk from illicit use of small vessels. While this strategy identifies four key risk scenarios, it is important to not let solutions be so focused on these four situations that they are not flexible enough to prevent other threats. National plans and strategies must be as adaptable as those who aspire to do harm.

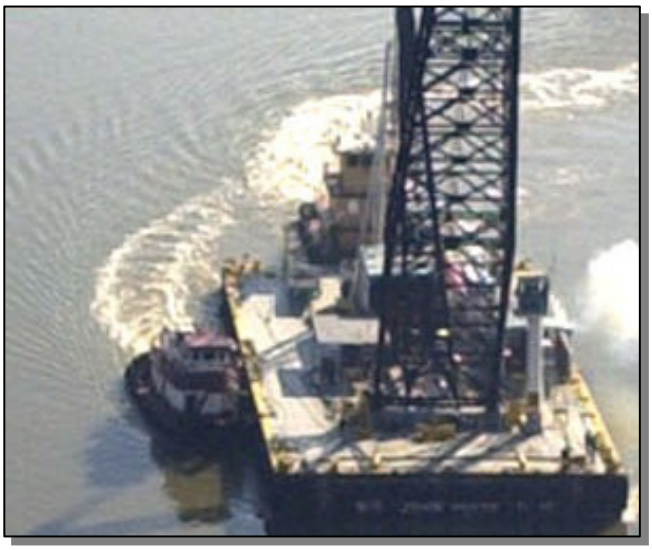
First and foremost solutions need to be risk-based, logical, and forward-looking, with a focus on the education, communication, and coordination of all stakeholders within the maritime domain.

Reducing risk from small vessels is a tremendous challenge because of the sheer number of boats, the variety of uses and types, their geographic range and frequent proximity to large vessels and critical infrastructure/key resources. This diversity precludes a single, one-size-fits-all solution, but requires a range of actions that can be undertaken to minimize risk. Separate stand-alone solutions may not make a significant contribution to risk reduction, but when taken together, will result in a greater overall reduction in small vessel risk.

Fortunately, the great size of the small vessel community also constitutes one of the greatest assets for risk reduction efforts. Everyday, millions of recreational boaters and thousands of professional mariners traverse our waters and stand ready, willing, and able to report suspicious activities. It is imperative that Federal, state, local, and Tribal governments work together, to develop, and nurture these relationships to address small vessel risk.

APPENDIX A—UNITED STATES FEDERAL GOVERNMENT RESPONSIBILITIES

This appendix summarizes, at a very high level, some of the relevant Federal government responsibilities in the maritime domain. It does not purport to confer additional responsibilities on these agencies, but is merely a concise summary of those responsibilities and authorities that already exist.



DEPARTMENT OF HOMELAND SECURITY (DHS)

DHS is a Cabinet level department of the United States Federal Government with the responsibility of protecting the territory or homeland of the United States from terrorist attacks and responding to natural disasters. The Department works to protect the United States within, at, and outside its borders. Its goal is to prepare for, prevent and respond to domestic emergencies, particularly terrorism.

DHS Office of Policy

DHS Policy is the primary policy formulation and coordination component for DHS. It provides a centralized, coordinated focus to the development of DHS-wide, long-range planning to protect the United States.

DHS Office of Intelligence and Analysis (I&A)

I&A is the office in DHS which identifies and assesses a broad range of intelligence information concerning current and future threats against the United States. The office is responsible for issuing timely warnings and advisories for the full spectrum of terrorist threats against the homeland, including physical and cyber events. In responding to disruption within the maritime domain, I&A reviews threats to the Marine Transportation System and marine CIKR, and provides intelligence to key decision makers within the Department.

DHS Office of Operations Coordination

The Office of Operations Coordination conducts joint operations across all organizational elements, coordinating activities related to incident management. It employs all Department resources to translate intelligence and policy into action and oversees the National Operations Center (NOC) which collects and fuses information from more than 35 Federal, state, Tribal, local, and private sector agencies.

DHS Directorate for Science and Technology (S&T)

The Directorate for Science and Technology (S&T) is the primary research and development arm of DHS. The S&T Directorate, in partnership with the private sector, national laboratories, universities, and other government agencies (domestic and foreign), helps push the innovation envelope and drive development and the use of high technology in support of homeland security. DHS S&T plays a critical role in the development of cost-effective technologies that will provide real world capabilities to support the reduction of risk from the exploitation of small vessels by terrorists.

United States Coast Guard (USCG)

The USCG is a multi-mission, maritime service within DHS and one of the five Services of the Nation's Armed Forces. Its core roles are to protect the public, the environment, and U.S. economic and security interests in any maritime region in which those interests may be at risk, including international waters and America's coasts, ports, and inland waterways.

The USCG provides unique benefits to the Nation because of its distinctive blend of military, humanitarian, and civilian law-enforcement capabilities.

The USCG routinely inspects and assesses the security of U.S. ports in accordance with the MTSA of 2002, the Ports and Waterways Safety Act, and other pertinent legislation. Every regulated U.S. port facility is required to establish and implement a comprehensive security plan that outlines procedures for controlling access to the facility, verifying credentials of port workers, implementing the Transportation Worker Identification Credential (TWIC), inspecting cargo for tampering, designating security responsibilities, training, and reporting of all breaches of security or suspicious activity, among other security measures. Working closely with local port authorities and law enforcement agencies, the USCG regularly reviews, approves, assesses, and inspects these plans and facilities to ensure full compliance. In addition, also as required by the MTSA, the USCG assesses the effectiveness of anti-terrorism measures at foreign ports.

The USCG:

- Leads development of maritime regimes
  - Participates in planning efforts by developing Area Maritime Security Plans (AMSP) and collaborating with maritime stakeholders, especially Area Maritime Security Committees (AMSC) and other local groups such as local harbor safety committees.
  - Controls vessel traffic, movement, and anchorage.
  - Establishes and enforces security and safety zones.

  - Controls access to the operations of facilities under, in, or adjacent to waters subject to the jurisdiction of the United States.

- Facilitates efforts to enhance maritime domain awareness
  - Tracks Notice of Arrival (NOA) information from ships entering U.S. waters and ensures changes to NOAs are provided to the appropriate USCG and CBP officials at alternate ports of entry.
  - As part of AMSCs, and in coordination with appropriate stakeholders and other government agencies, monitors all vessels and other inter-modal operations within the respective area of responsibility.
  - Collects, integrates, and analyzes maritime intelligence concerning threats to vessels, ports and maritime infrastructure.
  - Coordinates post-incident assessments and the reporting of maritime CIKR status and intermodal linkages.

- Provides operational capabilities to deter, respond to, and mitigate small vessel related attacks.
  - Actively manages risks to ports by directing the movement of vessels, as necessary.
  - Furnishes available personnel, equipment or other resource support as requested, consistent with overriding mission responsibilities and within the capabilities of assigned resources.
  - Provides port security measures to reduce potential threats and to ensure integrity of the existing infrastructure system, including boarding of certain high-risk vessels prior to port entry.
  - Ensures the safety of navigation and security of an Area of Responsibility (AOR).

United States Customs and Border Protection (CBP)

U.S. Customs and Border Protection's top priority is to keep terrorists and their weapons from entering the United States. While welcoming all legitimate travelers and trade, CBP officers and agents enforce all applicable U.S. laws. CBP employs over 33,000 sworn law enforcement officers, agents and agricultural specialists stationed at over 326 official ports of entry, at 142 Border Patrol stations and 35 checkpoints along 7,000 miles of land border with Canada and Mexico and along 95,000 miles of U.S. coastline, at 58 foreign seaports as part of the Container Security Initiative (CSI), and at U.S. embassies around the world.

CBP is the only agency authorized to make final admissibility determinations regarding cargo and persons arriving from a foreign port or place. With regard to small vessel operations, CBP enforces applicable requirements for commercial vessel operations without regard to the size of the vessel. Therefore, commercial vessel operators must comply with CBP requirements to provide inbound and outbound cargo declarations and passenger manifests, and provide entry and clearance notifications.

Pursuant to 19 CFR 4.2, operators of small pleasure vessels, arriving in the United States from a foreign port or place to include any vessel which has visited a hovering vessel or received merchandise outside the territorial sea, are required to report their arrival to CBP immediately

upon arrival. CBP also requires a face-to-face inspection unless the operator and passengers qualify for one of four alternate inspection systems.

In addition to enforcing reporting requirements, CBP searches for narcotics and other contraband, and undocumented migrants. CBP enforcement of small vessel requirements includes officers assigned to stationary designated inspection sites and agents on patrol using an array of over 260 fixed, rotary wing and unmanned aircraft, and nearly 200 marine enforcement vessels of all types.

CBP:

- Employs all available resources to identify and interdict terrorists and terrorist's weapons (WMD) as far from the U.S. shores as possible
- Coordinates with Federal, state, local, Tribal and international law enforcement partners to stop illegal migrants, drugs, and other criminals from entering the U.S. via the maritime domain
- Employs the widest possible information sharing practices with other law enforcement agencies and other partners
- Employs risk management practices when analyzing information and targeting possible high-risk persons, vessels, and cargo for enforcement actions
- Continues to leverage the latest state-of-the-art technology solutions for situational awareness and non-intrusive screening and inspection, whenever possible
- Ensures enforcement actions do not unnecessarily impede the legitimate flow of commercial maritime trade and the freedom of recreational boaters operating in the maritime domain

Domestic Nuclear Detection Office (DNDO)

The DNDO is a jointly-staffed, national office established 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.

DNDO:

- Develops the global nuclear detection and reporting architecture;
- Develops, acquires, and supports the domestic nuclear detection and reporting system;
- Fully characterizes nuclear detector system performance before deployment;
- Establishes situational awareness through information sharing and analysis;
- Establishes operation protocols to ensure that nuclear detection leads to effective response;
- Conducts a transformational research and development program in nuclear detection; and

- Establishes the National Technical Nuclear Forensics Center to provide centralized planning and integration of USG nuclear forensics programs.

Immigration and Customs Enforcement (ICE)

The mission of ICE is to protect and uphold public safety by identifying criminal activities and eliminating vulnerabilities that pose a threat to the U.S. borders, as well as enforcing economic, transportation, and infrastructure security. By protecting national and border security, ICE seeks to eliminate the potential threat of terrorist acts against the United States. ICE hosts the largest international investigative component in DHS, interacting with the international community on behalf of multiple agencies through investigations of immigration and customs violations, representation with international organizations, conducting international training, and guiding repatriation efforts.

ICE Attachés work within U.S. Embassies to implement and support multiple maritime security initiatives in foreign countries.

- Cooperates with foreign governments in the coordination of DHS foreign investigations, and provides homeland security intelligence to the DHS Office of Intelligence and Analysis (I&A), other government entities, and our state, local, and private sector partners.
- Works with foreign counterparts to combat transnational crimes involving national security by conducting investigations of entities that pose a risk of terrorism and/or criminal activities before they arrive at U.S. ports of entry.
- Participates in Border Enforcement Security Task Forces (BESTs) and Integrated Border Enforcement Teams (IBETS), with foreign government counterparts to increase capability to detect and interdict harmful goods and materials.
- Serves as a point of contact in Canada and Mexico in the Security and Prosperity Partnership (SPP) and the Secure Border Initiative (SBI).

Transportation Security Administration (TSA)

TSA’s Office of the Transportation Sector Network Management (TSNM) is dedicated to leading the unified national effort to protect and secure our Nation’s intermodal transportation systems. TSNM ensures the safe movement of passengers and promote the free flow of commerce by building a resilient, robust, and sustainable network with our public and private sector partners. TSA's Maritime Security Division is engaged in this unified national effort primarily by providing expertise in credentialing as well as passenger and vehicle screening techniques and procedures. TSA supports specific programs for ferry and passenger vessel security, the Transportation Workers Identification Card (TWIC) program and The Port Security Exercise Training Program (PortSTEP), which brings together Federal, state, and local governments and private institutions to test responses to specific security events.

DEPARTMENT OF COMMERCE (DOC)

National Oceanic and Atmospheric Administration (NOAA)

NOAA has a number of responsibilities that regulate and monitor activities of vessels and ensure safe maritime navigation.

The NOAA Office of Law Enforcement is dedicated to the enforcement of laws that protect and conserve our Nation's living marine resources and their natural habitat. NOAA Fisheries currently has 131 special agents and 19 enforcement officers located at 53 duty stations throughout the United States. These agents and officers have specified authority to enforce over 37 statutes, as well as numerous treaties related to the conservation and protection of marine resources and other matters of concern to NOAA. This includes law enforcement activities and boarding vessels in port and at sea.

NOAA also provides accurate, reliable, and up to date information for safe, efficient, and environmentally sound transportation to our Nation's commerce communities. The NOAA Office of Coast Survey manages NOAA's nautical chart data collection and information program and provides navigation services to support this strategic goal.

DEPARTMENT OF DEFENSE (DOD)

The Department of Defense is responsible for defending the United States while helping to promote American interests globally. During a security incident, DOD may, at the direction of the President or the Secretary of Defense, provide Defense Support of Civil Authorities (DSCA), in accordance with applicable laws, regulations, and agreements, to Federal, state, local, and Tribal response and recovery activities. In addition, local military commanders and responsible officials of other DOD components are authorized to take necessary action to response to requests of civil authorities to save lives, prevent human suffering, or mitigate great property damage. All such necessary action is referred to as "immediate response."

DEPARTMENT OF TRANSPORTATION (DOT)

The mission of the Department of Transportation is to serve the United States by ensuring a fast, safe, efficient, accessible, and convenient transportation system that meets U.S. vital national interests and enhances the quality of life of the American people, today and into the future. This includes the development and coordination of security requirements within those modes

Maritime Administration (MARAD)

MARAD offers security training programs that can certify individuals as vessel security officers regarding the implementation of MTSA related requirements.

St. Lawrence Seaway Development Corporation (SLSDC)

SLSDC is a wholly owned government corporation created by statute in 1954, to construct, operate, and maintain that part of the St. Lawrence Seaway between the Port of Montreal and Lake Erie, within the territorial limits of the United States. It works closely with the Saint Lawrence Seaway Management Corporation of Canada to ensure safe and secure management of seaway transportation into and out of the Great Lakes on the Seaways.

DEPARTMENT OF ENERGY (DOE)

The DOE, through the National Nuclear Security Administration (NNSA) has four missions relevant to this strategy:

- Protecting or eliminating weapons and weapons-useable nuclear material or infrastructure, and redirecting excess foreign weapons expertise to civilian enterprises;
- Preventing and reversing the proliferation of weapons of mass destruction;
- Reducing the risk of accidents in nuclear fuel cycle facilities worldwide; and
- Enhancing the capability to detect weapons of mass destruction, including nuclear, chemical and biological systems.

DEPARTMENT OF THE INTERIOR

Minerals Management Service

The Minerals Management Service (MMS), a bureau in the U.S. Department of the Interior, is the federal agency that manages the nation's natural gas, oil and other mineral resources on the outer continental shelf (OCS). The OCS is a significant source of oil and gas for the Nation’s energy supply. The approximately 43 million leased OCS acres generally accounts for about 20 percent of America’s domestic natural gas production and about 30 percent of America’s domestic oil production. The MMS’s oversight and regulatory frameworks ensure production and drilling are done in an environmentally responsible manner, and done safely.

DEPARTMENT OF JUSTICE (DOJ)

DOJ, through the Federal Bureau of Investigation (FBI), is the lead agency for investigations of terrorist acts or terrorist threats by individuals or groups inside of the United States, or directed at U.S. citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States. Accordingly, DOJ, through the FBI, is responsible for coordinating the activities of other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States. DOJ, through the FBI, is the lead agency for intelligence collection in the United States.

DOJ controls all criminal prosecutions and civil suits in which the United States has an interest. Under the direction of the Attorney General, 93 United States Attorneys serve as the nation's

principal litigators, conducting most of the trial work in which the United States is a party, including the prosecution of criminal cases brought by the Federal government; the prosecution and defense of civil cases in which the United States is a party; and the collection of debts owed the Federal government which are administratively uncollectible.

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) is a principal law enforcement agency within the DOJ dedicated to preventing terrorism, reducing violent crime, and protecting our Nation. The men and women of ATF perform the dual responsibilities of enforcing Federal criminal laws and regulating the firearms and explosives industries.

APPENDIX B—RELEVANT AUTHORITIES

Various laws, presidential directives, national strategies, international conventions and agreements, and DHS goals and priorities shaped this strategy.

STATUTES/ACTS

Homeland Security Act of 2002[27]

This Act established a cabinet-level department headed by a Secretary of Homeland Security with the mandate and legal authority to protect the American people from the continuing threat of terrorism. Congress assigned DHS the primary missions to:

- Prevent terrorist attacks within the United States.
- Reduce the vulnerability of the United States to terrorism at home.
- Minimize the damage and assist in the recovery from terrorist attacks that occur.
- Ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland.

The Homeland Security Act of 2002 is an important legal element in the role of sharing information as it established the Department of Homeland Security (DHS) within the Executive Branch. The DHS was developed to aid in the prevention of and "reduce the vulnerability" of the U.S. to acts of terrorism. While the DHS is not tasked with the power to investigate and prosecute acts of terrorism, the Act requires the Department to monitor coordination between agencies and subdivisions to ensure that even the most tangential piece of information is analyzed to help secure the homeland.

Ports and Waterways Safety Act (PWSA) of 1972[28]

The PWSA grants the USCG broad authority to take action in response to safety and security issues within the port. For example, the USCG is authorized to establish safety or security zones both on land and water. Only authorized persons, vehicles, or vessels may enter a safety or

---

[27] Public Law 107–296, 116 Stat. 2135 (Nov. 25, 2002) as codified at 6 U.S.C. §101 et seq.

[28] Public Law 92–340, §2, formerly Title I, § 101, 86 Stat. 424 (Jul. 10, 1972), renumbered and amended Public Law 95–474, § 2, 92 Stat. 1471 (Oct. 17, 1978); Public Law 107–295, Title IV, § 443(1), 116 Stat. 2132 (Nov. 25, 2002), as codified at 33 U.S.C. § 1221 et seq.

security zone. Persons within a zone must obey the lawful orders of the Captain of the Port (COTP). Further the PWSA implementing regulations authorize the COTP to control vessels and facility operations to ensure the safety and security of vessels and waterfront facilities, as well as to protect navigable waters and the resources therein.

International Maritime and Port Security Act[29]

This act amended the Ports and Waterways Safety Act, adding a new section—Port, Harbor and Coastal Facility Security. This section authorizes the Secretary to carry out measures to prevent or respond to an act of terrorism against an individual, vessel, or public or commercial structure that is subject to the jurisdiction of the U.S. and located within or adjacent to the marine environment, or a vessel of the U.S. or an individual on board that vessel.

Port and Tanker Safety Act (PTSA) Of 1978[30]

The Port and Tanker Safety Act of 1978 amended the PWSA, and provides the Coast Guard with broader, more extensive, and explicitly stated authority. The Act addresses improvements in the supervision and control over all types of vessels, foreign and domestic, operating in the U.S. navigable waters, and in the safety of all tank vessels, foreign and domestic, which transport and transfer oil or other hazardous cargoes in U.S. ports. Additionally, the Act addresses improvements in the control and monitoring of vessels operating in offshore waters near our coastline, and vessel manning and pilotage standards.

The Magnuson Act of 1950[31]

This Act provides the USCG with the authority to ensure the protection and security of vessels, harbors, and waterfront facilities against sabotage or other subversive activities. It authorizes the USCG to establish security zones to prevent damage or injury to any vessel or waterfront facility and to safeguard ports, harbors, territories, or waters of the United States.

Maritime Transportation Security Act of 2002[32]

The Maritime Transportation Security Act of 2002 (MTSA) is designed to protect the nation's ports and waterways from a terrorist attack. This Act directs initial and continuing assessments of maritime facilities and vessels that may be involved in a TSI. It requires vessels and port facilities to conduct vulnerability assessments and develop security plans that may include passenger, vehicle and baggage screening procedures; security patrols; establishing restricted

---

[29] Public Law 99–399, title IX, 100 Stat. 889 (Aug. 27, 1986), as codified in 33 U.S.C. 1226.

[30] Public Law 95–474, 92 Stat. 1471 (Oct. 17, 1978)

[31] 50 U.S.C. §191.

[32] Public Law 107–295, codified at 46 U.S.C. Subtitle VI, Chapter 701.

areas; personnel identification procedures; access control measures; and/or installation of surveillance equipment.

Developed using risk-based methodology, the MTSA security regulations focus on those sectors of maritime industry that have a higher risk of involvement in a TSI, including various tank vessels, barges, large passenger vessels, cargo vessels, towing vessels, offshore oil and gas platforms, and port facilities that handle certain kinds of dangerous cargo or service the vessels listed above.

MTSA also required the establishment committees in all the nation's ports to coordinate the activities of all port stakeholders, including other Federal, local and state agencies, industry and the boating public. These groups, called Area Maritime Security Committees, are tasked with collaborating on plans to secure their ports so that the resources of an area can be best used to deter, prevent and respond to terror threats.

Security and Accountability for Every Port Act of 2006 (SAFE Port Act)[33]

In an effort to further the progress made through the Maritime Transportation Security Act of 2002, the Security and Accountability for Every Port Act (SAFE Port Act) was passed and became effective in October 2006. The SAFE Port Act created and codified new programs and initiatives, and amended some of the original provisions of MTSA. The SAFE Port Act includes provisions that:

- Codified the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT);
- Established port security interagency operational centers at all high-risk ports;
- Set an implementation schedule and fee restrictions for TWIC;
- Required that all containers entering high volume U.S. ports be scanned for radiation sources by December 31, 2007;
- Required additional data be made available to CBP for targeting cargo containers for inspection; and
- During a TSI on or adjacent to waters subject to the jurisdiction of the United States, the Coast Guard Captain of the Port acts as the incident commander, unless otherwise directed by the President.

[33] Public Law 109–347, 120 Stat. 1884 (Oct. 13, 2006), as codified at 6 U.S.C. §901, et seq.

Critical Infrastructure Information Act of 2002[34]

Enacted as part of the Homeland Security Act, this Act creates a framework that enables members of the private sector to voluntarily submit sensitive information regarding the Nation's Critical Infrastructure/Key Resources to DHS with the assurance that the information, if it satisfies certain requirements, will be protected from public disclosure.

Aviation and Transportation Security Act of 2001[35] *(ATSA)*

ATSA provides broad Federal authority for security in all modes of transportation. The authorities of ATSA are delegated by the Secretary of Homeland Security to the Administrator of the TSA. The Administrator "shall be responsible for security in all modes of transportation" including civil aviation security and all "security responsibilities over other modes of transportation that are exercised by the Department of Transportation." The Administrator is given an array of specific authorities which carry out this broad responsibility.

The Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act)[36]

The Stafford Act provides comprehensive authority for response to emergencies and major disasters—natural disasters, accidents, and intentionally perpetrated events. It provides specific authority for the Federal government to provide assistance to state and local entities for disaster preparedness and mitigation, and major disaster and emergency assistance.

Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism Act of 2001 (USA Patriot Act)[37]

The Patriot Act outlines the domestic policy related to deterring and punishing terrorists, and the United States policy for Critical Infrastructure/Key Resource protection. It also provides for the establishment of a national competence for National Infrastructure Simulation and Analysis Center and outlines the Federal government's commitment to understanding and protecting the interdependencies among critical infrastructure.

---

[34] Public Law 107–296, Title II, §212, 116 Stat. 2150 (Nov. 25, 2002), as codified at 6 U.S.C. 131 et seq. Presented as Subtitle B of Title II of the Homeland Security Act (sections 211-215).

[35] Public Law 107–71, 115 Stat 597 (Nov. 19, 2001), as codified at 49 U.S.C. §40101, et seq.

[36] Public Law 93–288, 88 Stat. 143 (May 22, 1974), as amended, codified at 42 U.S.C. §5121 et seq.

[37] Public Law 107–56, 115 Stat. 272 (Oct. 26, 2001), as codified at 18 U.S.C. §1, et seq.

Outer Continental Shelf (OCS) Lands Act of 1953

The OCS Lands Act, and subsequent amendments, outlines the Federal responsibility over the submerged lands of the Outer Continental Shelf. Additionally, it authorizes the Secretary of the Interior to lease those lands for mineral development. It is the role of DOI to ensure that the U.S. government receives fair market value for acreage made available for leasing and that any oil and gas activities conserve resources, operate safely, and take maximum steps to protect the environment.

PRESIDENTIAL DIRECTIVES

- Domestic Incident Management (HSPD-5)
- Critical Infrastructure Identification, Prioritization, and Protection (HSPD 7)
- National Preparedness (HSPD 8)
- Maritime Security Policy (HSPD 13/NSPD 41)
- Domestic Nuclear Detection (HSPD 14/NSPD 43)

NATIONAL STRATEGIES

- *National Security Strategy* (March 2006)
  - Prevent enemies from threatening the Nation, U.S. allies, and friends with WMD.
- *National Strategy for Homeland Security* (October 2007)
- *National Strategy for Maritime Security* (NSMS) (September 2005)
  - Prevent Terrorist Attacks and Criminal or Hostile Acts—Detect, deter, interdict, and defeat terrorist attacks, criminal acts, or hostile acts in the maritime domain, and prevent its unlawful exploitation for those purposes.
  - Protect Maritime-Related Population Centers and Critical Infrastructure—Protect maritime-related population centers, critical infrastructure, key resources, transportation systems, borders, harbors, ports, and coastal approaches in the maritime domain.
- *National Strategy for Combating Terrorism* (September 2006)
  - Deny WMD to rogue states and terrorist allies who seek to use them.
- *National Plan to Achieve Maritime Domain Awareness for NSMS* (October 2005)
  - Enhance transparency in the maritime domain to detect, deter and defeat threats as early and distant from U.S. interests as possible;
  - Enable accurate, dynamic, and confident decisions and responses to the full spectrum of maritime threats
- *International Outreach and Coordination Strategy for NSMS* (November 2005)

  - A coordinated policy for United States government maritime security activities with foreign governments, international and regional organizations, and the private sector.
  - Enhanced outreach to foreign governments, international and regional organizations, private sector partners, and the public to solicit support for improved maritime security.
- *National Military Strategy to Combat Weapons of Mass Destruction* (February 2006)
  - Prevent, dissuade, or deny WMD proliferation or possession.
- *National Military Strategic Plan for the War on Terrorism* (February 2006)
  - Deny terrorist networks the possession or use of WMD
  - Establish conditions that allow partner nations to govern their territory effectively and defeat terrorists
- *Civil Support*, DoD Joint Publication 3-28 (September 2007)
  - DOD contributes to homeland security by conducting homeland defense operations overseas and in the approaches to the US, and by providing civil support for disasters and declared emergencies, to designated law enforcement agencies.

INTERNATIONAL AGREEMENTS/INITIATIVES

- United Nations Convention on the Law of the Sea
- Convention for the Safety of Life at Sea, including the International Ship and Port Facility Security Code
- Proliferation Security Initiative
- Security and Prosperity Partnership of North America
- Global Initiative to Combat Nuclear Terrorism

APPENDIX C—EXISTING INTERAGENCY INSTITUTIONS

Interagency cooperation at all levels of government and including members of the private sector is vital to the success of efforts to reduce small vessel risk. Leveraging already existing interagency forums will allow more partnerships to develop quickly and be more effective than creating entirely new entities.

Homeland Security Advisory Council

At the upper levels of the Department of Homeland Security, the Homeland Security Advisory Council (HSAC) provides advice and recommendations to the Secretary on matters related to homeland security. The Council is comprised of leaders from state and local government, first responder communities, the private sector, and academia.

Area Maritime Security Committees (AMSC)

The USCG has developed 59 AMSCs covering 361 ports, the Great Lakes, Inland and Western Rivers, and the Outer Continental Shelf region. The USCG COTP, designated as the Federal Maritime Security Coordinator (FMSC) by the National Maritime Transportation Security Plan (NMTSP) under the MTSA of 2002,[38] have facilitated and coordinated the development of these plans through Area Committees.

Each FMSC has formed an AMSC, comprised of Federal, state, and local agencies, as well as members of the local maritime industry, in their areas of responsibility. The Committee process enhances the exchange of communications between the USCG, local agencies, and maritime stakeholders. This cooperative spirit facilitates the creation and maintenance of comprehensive, coordinated AMSPs which provide for coordinated community-wide measures and support for

[38] As implemented in 33 C.F.R. Part 103.200.

incident management. The AMSPs and Committees serve as the cornerstone for developing and maintaining the first lines of defense at our Nation's ports.

During a response to an incident, the AMSCs may also serve as advisory groups, providing the COTP/FMSC with critical information relating to the port, including recommendations and guidance on prioritization of response operations and resumption/restoration activities.

Joint Terrorism Task Force (JTTF)/National Joint Terrorism Task Force

A JTTF is the Federal Bureau of Investigation's task force concept that promotes interagency cooperation, coordination, and communication in addressing a wide variety of terrorism matters. JTTF members include other Federal agencies (notably DHS components such as CBP, ICE, the TSA, USCG, and the United States Secret Service (USSS)), state, and local law enforcement, and specialized agencies, such as railroad, harbor, and port police. JTTFs are established in all 56 FBI field offices.

In addition, a National JTTF exists in Washington, DC that is composed of representatives from many other government agencies. The NJTTF supports the JTTFs throughout the United States and enhances communication, coordination, and cooperation between Federal, state, and local government agencies representing the intelligence, law enforcement, defense, diplomatic, public safety, and homeland security community by providing a point of fusion for terrorism intelligence.

Integrated Border Enforcement Teams (IBETS)

To effectively combat cross-border criminal activity, American and Canadian law enforcement agencies take an international and integrated approach to their investigations.

Integrated Border Enforcement Teams (IBETs) core agencies are: the Royal Canadian Mounted Police (RCMP), the Canada Border Services Agency (CBSA), CBP, ICE, and the USCG.

IBET agencies share information and work together daily with other local, state and provincial law enforcement agencies on issues relating to national security, organized crime and other criminality transiting the Canada/U.S. border between the official Ports of Entry (POE).

Maritime Domain Awareness Coordination

Maritime Domain Awareness Stakeholder Board

The Maritime Domain Awareness Stakeholder Board will be responsible for policy coordination, alignment, synergy and issue resolution between the Global Maritime Intelligence Integration (GMII) Enterprise and the Global Maritime Situational Awareness (GMSA) Enterprise. The Stakeholder Board, through the co-chairs, will serve as a conduit to the Maritime Security Policy Coordinating Committee (MSPCC). The Stakeholder Board's efforts will focus on optimizing and guiding information sharing and the development of capabilities related to the key functional

aspects of Maritime Domain Awareness; collection, fusion, analysis and dissemination of data, information, and intelligence.

Global Maritime Community of Interest Intelligence Enterprise

National Security Presidential Directive-41/Homeland Security Presidential Directive-13 underscores the importance of securing the Maritime Domain. The Global Maritime Intelligence Integration Plan is one of the eight supporting plans to the *National Strategy for Maritime Security*. The GMII Plan defined the GMII Enterprise Director's roles and responsibilities in using existing capabilities to integrate all available intelligence regarding potential threats to U.S. interests in the Maritime Domain.

Director Global Maritime Situational Awareness Enterprise

The Director GMSA Enterprise is responsible for effective access to maritime information and data critical to building the situational awareness component of Global MDA. The Director will develop and recommend policy guidance for coordinated collection, fusion, analysis and dissemination of GMSA information and products, as well as information integration policies, protocols and standards across the GMSA Enterprise that are consistent with those established under GMII Enterprise.

Maritime Domain Awareness Enterprise Hubs

MDA Enterprise Hubs will be developed from within existing organizations with capabilities that already make substantial contributions to MDA in one or more of the following subject areas:

- Vessels;
- Cargo;
- People;
- Infrastructure; and
- Architecture Management.

Enterprise Hubs are intended to leverage their experience and expertise to provide leadership for the community in a particular area, not to be the exclusive Federal provider of information and products for that subject area.

Critical Infrastructure Sector Partnership

Critical infrastructure protection is a shared responsibility among Federal, state, local, and Tribal governments and the owners and operators of the Nation's CIKR. Partnerships between the public and private sectors are essential, in part because the private sector owns and operates approximately 85% of the Nation's critical infrastructure. Government agencies have access to critical threat information, and each controls security programs, research and development, and

other resources that may be more effective if discussed and shared, as appropriate, in a partnership setting.

Sector Partnership Structure

Homeland Security Presidential Directive 7 (HSPD-7) and the NIPP provide the overarching framework for a structured partnership between government and the private sector for protection of CIKR. This sector partnership structure details the formation of Sector Coordinating Councils and Government Coordinating Councils as described below.

Sector Coordinating Councils (SCC)

SCCs foster and facilitate the coordination of sector-wide activities and initiatives designed to improve the security of the Nation's critical infrastructure. They are self-organized, self-led, broadly representative of owners and operators (and their associations) within the sector, and are focused on homeland security and critical infrastructure protection.

Government Coordinating Councils (GCC)

Each GCC brings together diverse Federal, state, local, and Tribal interests to identify and develop collaborative strategies that advance critical infrastructure protection. GCCs serve as a counterpart to the SCC for each CIKR sector. They provide interagency coordination around CIKR strategies and activities, policy and communication across government, and between government and the sector to support the Nation's homeland security mission.

Critical Infrastructure Partnership Advisory Council (CIPAC)

The Critical Infrastructure Partnership Advisory Council (CIPAC) provides the operational mechanism for carrying out the sector partnership structure. The CIPAC provides the framework for owner and operator members of Sector Coordinating Councils (SCC) and members of Government Coordinating Councils (GCC) to engage in intra-government and public-private cooperation, information sharing, and engagement across the entire range of critical infrastructure protection activities.

APPENDIX D—ACRONYMS

AIS—Automatic Identification System

AMSC—Area Maritime Security Committee

AMSP—Area Maritime Security Plan

AOR—Area of Responsibility

ATSA—Aviation and Transportation Security Act of 2001

AWW—America's Waterway Watch

BEST—Border Enforcement Security Task Force

CBP—Customs and Border Protection

CBSA—Canada Border Services Agency

CI—Critical Infrastructure

CIKR—Critical Infrastructure and Key Resources

CIPAC—Critical Infrastructure Partnership Advisory Council

COTP—Captain of the Port

CSI—Container Security Initiative

C-TPAT—Custom-Trade Partnership Against Terrorism

DHS—U.S. Department of Homeland Security

DNDO—Domestic Nuclear Detection Office

DOD—U.S. Department of Defense

DOE—U.S. Department of Energy

DOJ—U.S. Department of Justice

DOT—U.S. Department of Transportation

EEZ—Exclusive Economic Zone

EPA—Environmental Protection Agency

FACA—Federal Advisory Committee Act

FBI—Federal Bureau of Investigation

FDA—Food and Drug Administration

FMSC—Federal Maritime Security Coordinator

FYHSP—Future Years Homeland Security Program

GAO—Government Accountability Office

GCC—Government Coordinating Council

GDP—Gross Domestic Product

GMII—Global Maritime Intelligence Integration

GMSA—Global Maritime Situational Awareness

GPRA—Government Performance and Results Act of 1993

GPS—Global Position System

IACM—Interagency Assessment of Cocaine Movement

IBETS—Integrated Border Enforcement Teams

ICE—Immigration and Customs Enforcement

ICS—Incident Command System

IIMG—Interagency Incident Management Group

IMO—International Maritime Organization

IND—Improvised Nuclear Device

ISAC—Information Sharing and Analysis Center

JTTF—Joint Terrorism Task Force

KR—Key Resources

LTTE—Liberation Tigers of Tamil Eelam

MANPADS—Man-Portable Air-Defense System

MARAD—Maritime Administration

MDA—Maritime Domain Awareness

MMS—Minerals Management Service

MISLE—Marine Information for Safety and Law Enforcement

MOTR—Maritime Operational Threat Response

MTSA—Maritime Transportation Security Act

MTS—Maritime Transportation System

NGO—Non-governmental Organization

NICC—National Infrastructure Coordinating Center

NIE—National Intelligence Estimate

NIMS—National Incident Management System

NIPP—National Infrastructure Protection Plan

NIRU—National Incident Response Unit

NMTSP—National Maritime Transportation Security Plan

NNSA—National Nuclear Security Administration

NOA—Notice of Arrival

NOC—National Operations Center

NRC—National Response Center

NRF—National Response Framework

NSMS—National Strategy for Maritime Security

OMB—Office of Management and Budget

OCS—Outer Continental Shelf

PART—Program Assessment Rating Tool

PBRS—Pleasure Boat Reporting System

POE—Port of Entry

PWSA—Ports and Waterways Safety Act

RCMP—Royal Canadian Mounted Police

RDD—Radioactive Dispersal Device

RFID—Radio-Frequency Identification

SBI—Secure Border Initiative

SCC—Sector Coordinating Council

SFO—Senior Federal Official

SLSDC—St. Lawrence Seaway Development Corporation

SPP—Security and Prosperity Partnership

SSA—Sector Specific Agency

TSA—Transportation Security Administration

TSI—Transportation Security Incident

TSNM—Office of the Transportation Sector Network Management

TWIC—Transportation Worker Identification Credential

USACE—United States Army Corps of Engineers

USCG—U.S. Coast Guard

USSS—U.S. Secret Service

VIS—Vessel Identification System

WBIED—Waterborne Improvised Explosive Device

WCO—World Customs Organization

WMD—Weapon of Mass Destruction