

PROFESSIONAL MARINERS AND THE SMALL VESSEL THREAT

Stephen L. Caldwell

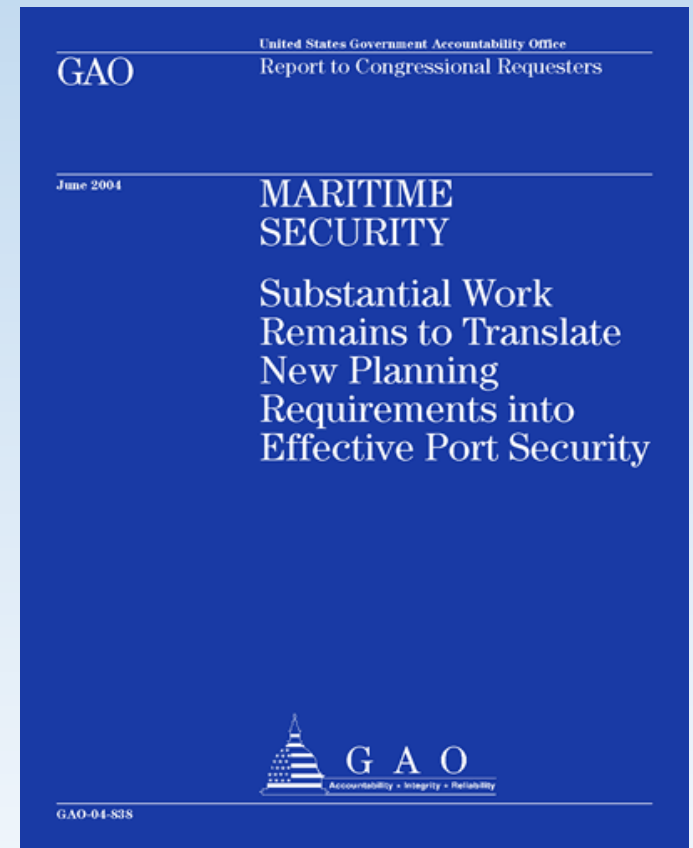
- Member, National Maritime Security Advisory Committee
- Former Director, Maritime and Supply Chain Security Issues at the U.S. Government Accountability Office

Chesapeake Area Professional Captains Association

27 June 2016, Annapolis, MD

AGENDA

- Background
- Maritime Domain Awareness
- Vessel Tracking Systems
- Small Vessel Threat
- Potential Solutions
- Questions & Contact Info



BACKGROUND

National Maritime Security Advisory Committee (NMSAC)

- NMSAC created by Maritime Transportation Security Act.
- NMSAC members are appointed by the Secretary of the Department of Homeland Security (DHS).
- NMSAC may advise, consult, and make recommendations to the Secretary on maritime security matters.
- NMSAC may also make such recommendations available to the Congress.
- NMSAC is intended to represent a broad array of maritime stakeholders such as ports, terminals, vessels, labor, state and local government, and academia.
- Stephen L. Caldwell was appointed to the NMSAC by DHS Secretary Jeh Johnson in June 2015 (for a 3 year term).



BACKGROUND

U.S. Government Accountability Office (GAO)

- GAO is an independent, nonpartisan agency that works for the U.S. Congress.
- The GAO mission is to support the Congress in meeting its oversight responsibilities and to help improve the performance and ensure the accountability of the federal government.
- GAO evaluates how the federal government manages programs and spends funds.
- Regarding maritime issues, since 9/11, GAO has issued about 100 reports on maritime and supply chain security.
- Stephen L. Caldwell was the director in charge of the maritime and supply chain security portfolio from 2006-2015.



BACKGROUND

Importance of U.S. Ports

- Ports contain many types/sectors of critical infrastructure.
- More than 95% of non-North American foreign trade arrives through U.S. ports, and more than 12 million containers enter the U.S. each year.
- Ports are major centers for chemical and petroleum-producing activities.
- 17 Strategic US seaports are necessary for major military deployments.
- Many ports feature important national symbols.
- Recreation is a central feature of many ports.



BACKGROUND

Vulnerability of U.S. Ports

- Ports are extensive in size, and are accessible by water, land, and air.
- Many ports are intertwined with major urban areas.
- Ports process a large volume of cargo, passengers, and hazardous materials.
- Ports are a hub of activity for multiple transportation modes.
- Many small vessels move through ports with relative anonymity.
- Cargoes move quickly due to just-in-time delivery systems.



BACKGROUND

U.S. Presidential Directive, Strategies & Plans

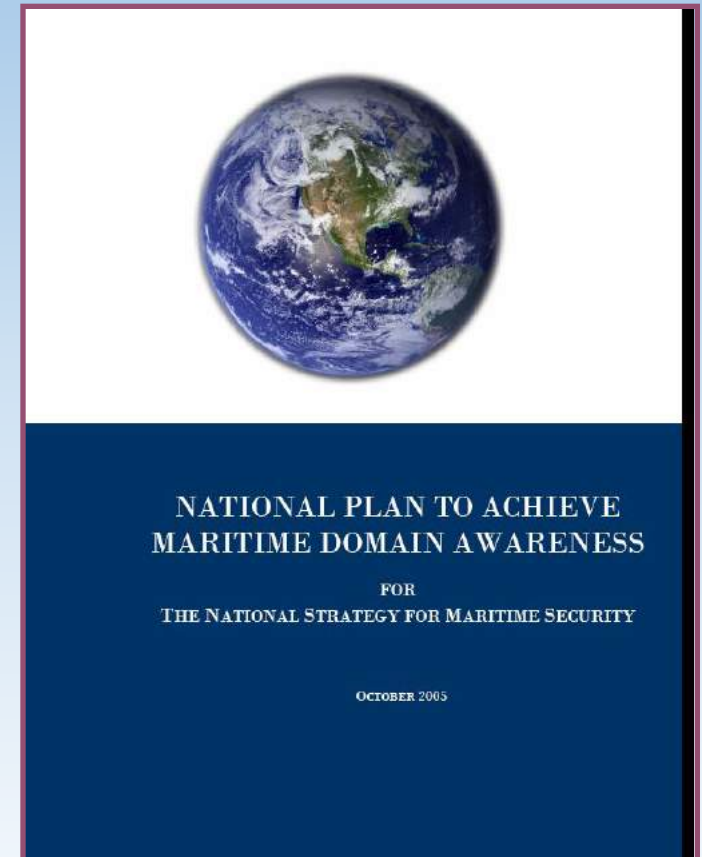
- HSPD-13 called for national system for coordinating response.
- National Strategy for Maritime Security with 8 sub-plans:
 - Maritime Domain Awareness,
 - Intelligence Integration,
 - Domestic Outreach,
 - International Coordination,
 - Threat Response,
 - Infrastructure Recovery,
 - Transportation Security, and
 - Commerce Security.
- Other action plans and strategies.



MARITIME DOMAIN AWARENESS

Definition and National Strategy

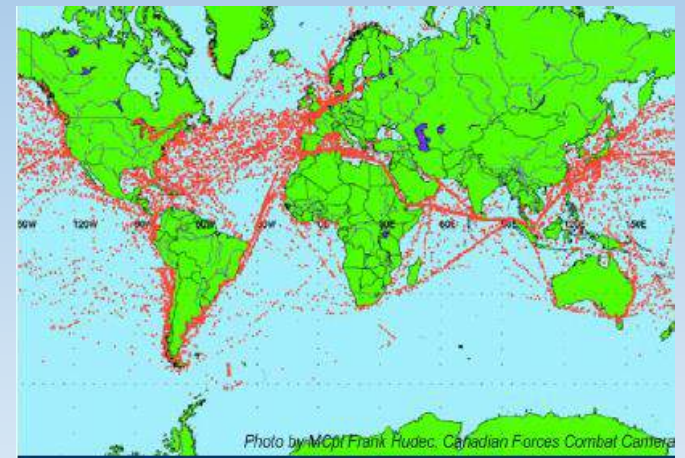
- Definition: “The effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States.”
- Strategic goals:
 - Enhance transparency in Maritime Domain.
 - Enable accurate responses to maritime threats.
 - Ensure freedom of navigation and efficient flow of commerce.



MARITIME DOMAIN AWARENESS

National Coordinating Organizations

- White House Maritime Security Interagency Policy Committee, and its Maritime Security Working Group.
- New Office of Global Maritime Situational Awareness (dual Navy USCG) created to catalog ongoing efforts, identify gaps, and coordinate efforts.
- New Assistant Deputy DNI for Global Maritime and Air Intelligence Integration (within ODNI) created to provide policy and direction to Intelligence Community elements to integrate activities and share information.



GLOBAL MARITIME INTELLIGENCE
INTEGRATION PLAN
FOR
THE NATIONAL STRATEGY FOR MARITIME SECURITY

JULY 2005

MARITIME DOMAIN AWARENESS

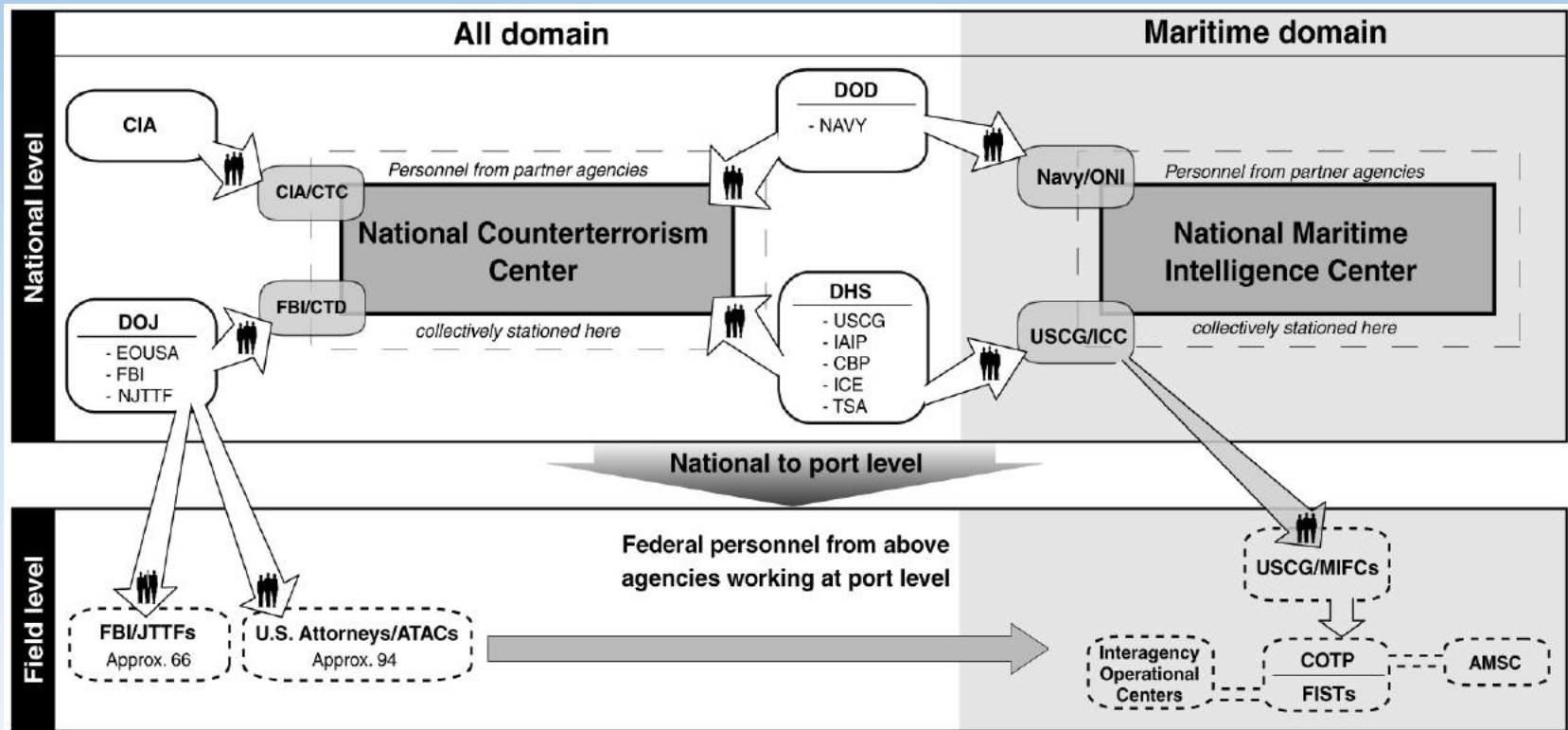
Regional / Port Level Monitoring and Analysis of Threats

- USCG Maritime Intelligence Fusion Centers supporting commands on East and West Coasts.
- Sector Command Centers are located at individual ports supported by sector intelligence staff.
- Interagency Operational Centers at selected ports representing USCG, Navy, CBP and some state and local law enforcement.
- SAFE Port Act called for Coast Guard to create additional Interagency Operational Centers, but a lack of prevented full implementation.



MARITIME DOMAIN AWARENESS

Integrating National and Port Level Intelligence



Source: GAO.

MARITIME DOMAIN AWARENESS

Vessel Tracking

- Tracking vessels supports the purpose of MDA -- to facilitate decision-making based on accurate information regarding vessel type, people, and cargo as far from shore as possible.
- Incoming commercial vessels must provide USCG with 96 Hour Advanced Notice of Visit.
- Linked to the Port State Control program – where USCG will board and examine incoming vessels for compliance with security and other requirements.



VESSEL TRACKING SYSTEMS

National Technical Means

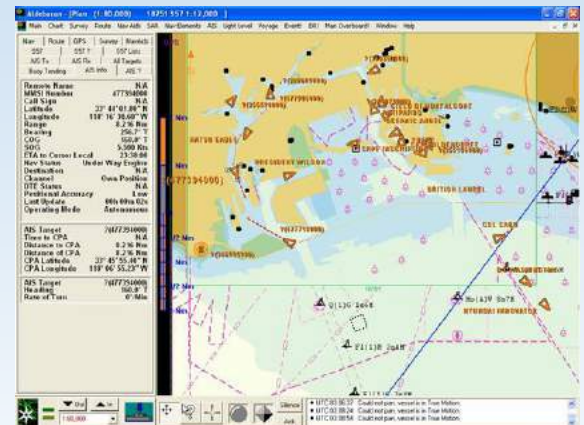
- National technical means were developed by the United States during the Cold War to track Soviet warships.
- Now such means are used to track a wide variety of vessels, not necessarily limited by size.
- Further details on national technical means are classified.
- This limits the usefulness of such means, their information can not be shared with other government agencies and port partners, which may complicate a multi-agency response to a potential threat.



VESSEL TRACKING SYSTEMS

Automated Identification System

- SOLAS and USCG regulations require AIS on certain larger vessels and the technology is widely available and proven.
- USCG currently uses land-based AIS as the primary means to track larger vessels in and around port areas.
- USCG expanded to National Automated Identification System (NAIS) to cover most of US coastline. USCG expanded range through commercially available satellite AIS.
- Limitations, initially many vessels within US waters do not need AIS (except in VTS ports), but the requirement was expanded to smaller vessels. However, vessel operators can turn off their AIS.



VESSEL TRACKING SYSTEMS

Other Sensors In Port Areas

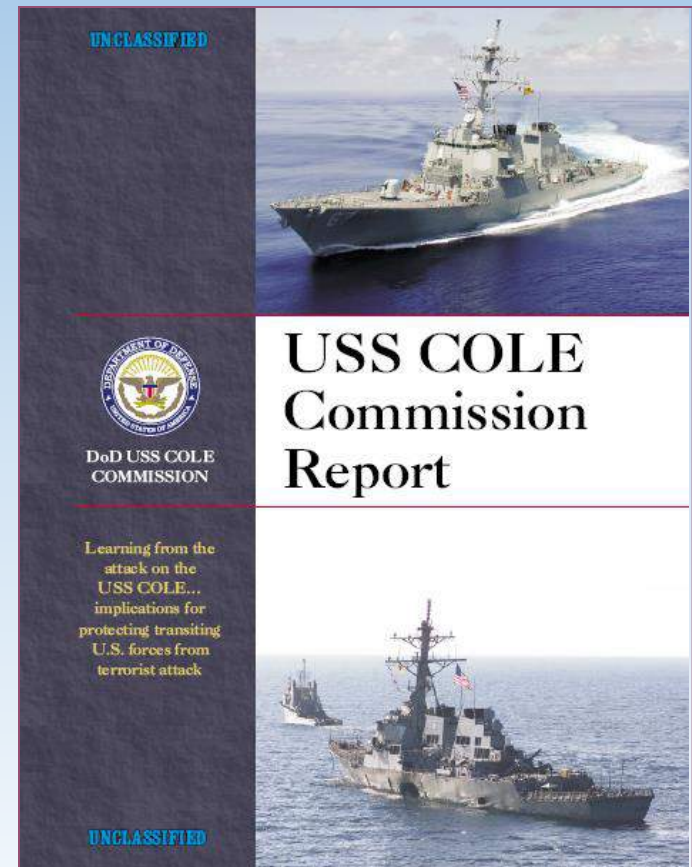
- USCG uses additional sensors at many ports and sectors.
- Video cameras (installed by USCG, Navy, and other stakeholders) can monitor port conditions, but some are fixed and can not follow vessels or zoom in, or are affected by low light or weather conditions.
- Radars can be used to track vessels, but have difficulty tracking smaller vessels, those that are between larger vessels, and (unlike AIS) they can not identify a vessel.



VESSEL TRACKING SYSTEMS

Limitations of These Other Sensors

- Thwarting an attack by a smaller vessel without advance knowledge of the threat may prove challenging even if all the available sensor systems are in place and working well.
- USCG is developing software programs for tracking the expected activity of a port over time and warning USCG when unexpected activities occur, but such programs will take years to be fully operational.



SMALL VESSEL THREAT

Small Vessel Threats and Scenarios

- Currently there is no known, credible threats to U.S. ports, but the situation can change quickly and several possible scenarios exist.
- Small vessels are very numerous and relatively anonymous as they move about.
- Small vessels could be used to illegally transport dangerous people and contraband.
- Small vessels pose a greater threat for nuclear smuggling than cargo container ships (per USCG Commandant Thad Allen).
- Small vessels could attack a number of targets: waterside facilities, port infrastructure, cruise ships, passenger ferries, and military ships (USS Cole and French supertanker Limburg).



SMALL VESSEL THREAT

Small Vessels and Main Shipping Channels

- USCG local regulations and NAVICs often establish general restrictions so small vessels avoid main shipping channels.
- However, small vessels can and often do violate these rules to traverse or even congregate in main shipping channels.
- USCG officials state they do not have the vessels and crews to continually enforce such restrictions.



SMALL VESSEL THREAT

Small Vessels and Restricted Areas

- Due to the configuration of many ports and waterways, there are restricted areas where navigation is constrained by a narrow channel, a canal or lock, or other chokepoint.
- In such locations, large commercial vessels may have to navigate in close proximity to small vessels.
- At such areas, port commerce is particularly vulnerable to small vessel attacks that might block passage of all ship traffic.



SMALL VESSEL THREAT

Small Vessels and Transit Security Zones

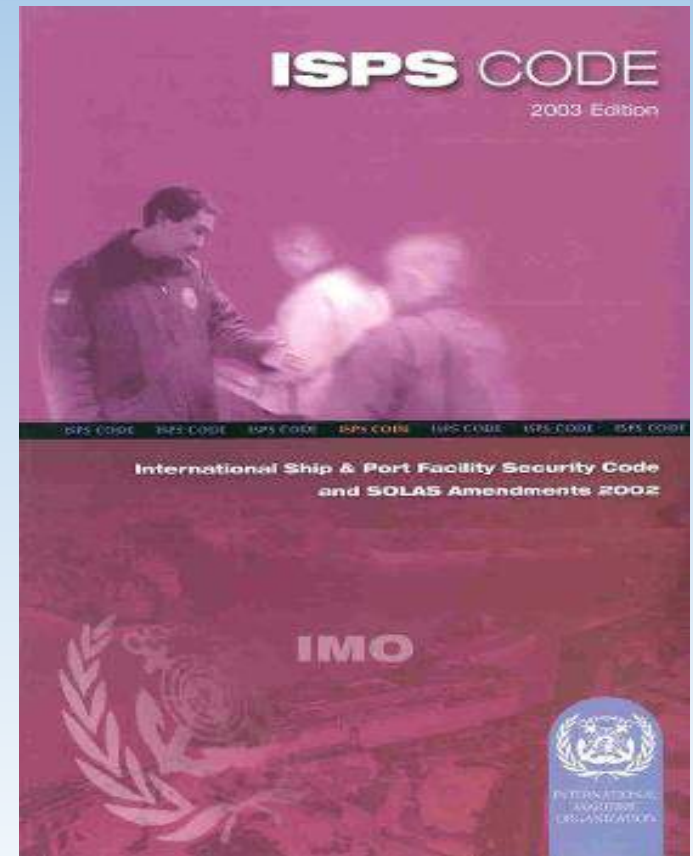
- USCG local regulations also establish security zones around certain transiting vessels.
- However, small vessels can and often ignore these.



POTENTIAL SOLUTIONS

IMO Small Vessel Circular

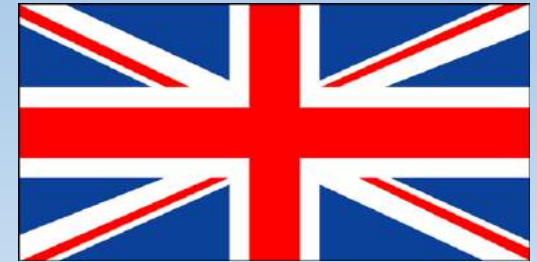
- ISPS Code supplemented by IMO Circular MSC.1/Circ.1283.
- Non-Mandatory Guidelines on Security Aspects of Non-SOLAS vessels.
- Includes commercial, special purpose, fishing, and pleasure vessels.
- Information on (among others):
 - Risk Assessment,
 - Security Awareness,
 - Personnel and Training,
 - International Voyages, and
 - Vessel Identification.



POTENTIAL SOLUTIONS

IMO Cited International Best Practices

- Security Awareness: the United Kingdom's Project Kraken and the United States' America's Waterway Watch program (discussed later).
- International Voyages by non-SOLAS vessels: Singapore's required declaration of arrival.
- Vessel Identification: Finland's pleasure craft registration and the United Kingdom's Small Ships Register.



POTENTIAL SOLUTIONS

Extend Tracking Systems to Small Vessels

- Singapore has Harbour Craft Transponder System (HARTS).
- Almost 3,000 licensed small vessels are required to carry transponders, which transmit identity, position, course and speed to the authorities.
- HARTS transponders can be fixed (larger vessels) or portable (for speed boats), with controls to confirm identity of each unique vessel.
- This solution not considered politically or economically viable in United States.

A TYPICAL INSTALLATION OF FIXED HARTS TRANSPONDER ONBOARD HARBOUR CRAFT



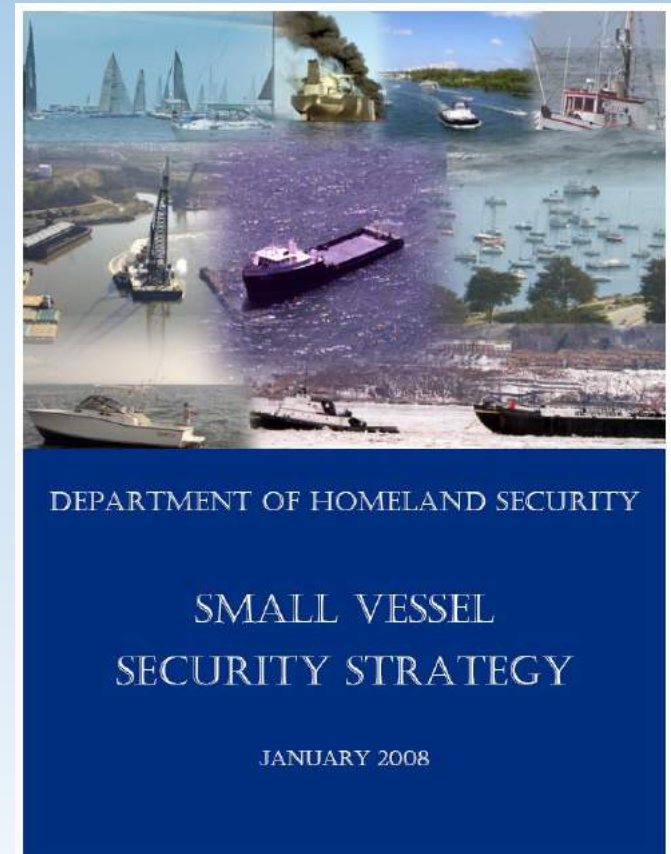
A TYPICAL INSTALLATION OF PORTABLE HARTS TRANSPONDER ONBOARD HARBOUR CRAFT



POTENTIAL SOLUTIONS

DHS Small Vessel Strategy

- DHS issued strategy in 2009.
- Develop & leverage partnership with small vessel community & public & private sectors.
- Develop risk-based plan with layered, innovative approach.
- Leverage technology to detect, determine intent, and interdict small vessels.
- Enhance coordination between all levels of government, private sector & international partners.
- DHS issued a more detailed implementation Plan issued in 2011 (not available to the general public).



POTENTIAL SOLUTIONS

Maritime Patrols, Escorts and Boardings

- USCG has internal requirements for security activities to include vessel escorts.
- However, USCG lacks resources to meet these requirements in many ports.
- Growing hazardous traffic (e.g., LNG and chemical tankers) requires more resources for escorts.
- USCG developed formal mutual assistance agreements with state and local law enforcement in many port locations.
- Increasing traffic, and the complexity of vessels, also requires more resources for boarding activities.



POTENTIAL SOLUTIONS

Security Zones and Closing Channels

- USCG can declare security zones and close channels near sensitive vessels and facilities.
- If present, waterborne patrols can intercept intruders and “shoulder” them away.
- Small vessel operators are not always cognizant of closures, and some closed areas are still in close proximity to port areas with small vessel traffic.



POTENTIAL SOLUTIONS

Radiation Monitoring Pilot Programs

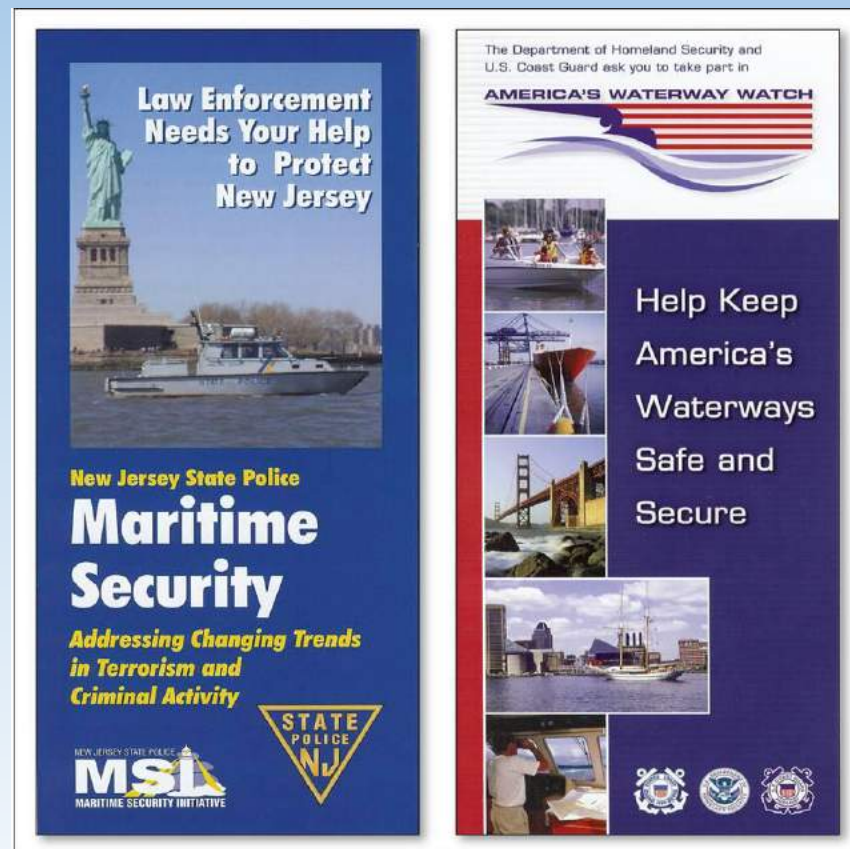
- The Department of Energy (DOE) and DHS's Domestic Nuclear Detection Office (DNDO) have various programs in place to monitor radiation in seaports.
- DNDO conducted pilot programs (in Puget Sound and San Diego) to test the feasibility of detecting radiological materials on small vessels.
- Pilot programs used Radiation Portal Monitors and Radio Isotope Identification Devices in various maritime applications.
- Challenges included training local personnel, the maritime environment (adapting technology, background radiation and water proofing), and sustainability (long term funding).



POTENTIAL SOLUTIONS

Waterway Watch Programs

- USCG program related to the small vessel threat, the limited abilities to track small vessels, and to improve MDA generally.
- USCG “America’s Waterway Watch” is an outreach effort with the port and mariner community to get them to report suspicious activity.
- Some state governments have similar programs (e.g., New Jersey State Police “Maritime Security Initiative” which includes regular visits to marinas, boat ramps, etc.
- Per Small Vessel Security Strategy, the small vessel and mariner community itself is the single largest asset in addressing the threat from small vessel attacks.



Source: New Jersey State Police; U.S.Coast Guard.

CONCLUSIONS

- Maritime Domain Awareness has been advanced through detailed planning, new organizations, and new technologies.
- Widely deployed longer-range tracking systems (AIS) are geared toward tracking larger ships, and depend on their cooperation. They cannot track small vessels.
- Newer in-port tracking systems (radars & cameras) can track small vessels in normal circumstances, but they are not widely deployed, and can not recognize threatening actions.
- Even if newer in-port systems are in place and working, they could not prevent a terrorist attack unless the plot was known in advance and/or response assets were on scene.
- The small boat and mariner community is both the problem and the solution to the small vessel threat.

QUESTIONS AND CONTACT INFO

Questions?

Stephen Caldwell, (301) 602-0794, email: stephencaldwell1000@gmail.com

For access to GAO reports, see GAO website: www.gao.gov



The image shows a screenshot of the U.S. Government Accountability Office (GAO) website as viewed in Internet Explorer. The browser's address bar shows the URL <http://www.gao.gov/>. The website header includes the GAO logo and navigation links such as "About GAO", "GAO", "E-mail Updates", and "Share/Save page". A search bar is visible with the text "GAO-10-12" and a "Search" button. Below the header, there are several menu items: "Reports & Testimonies", "Legal Decisions", "Comptroller General", "Topic Collections", "Careers", "FraudNet/Reporting Fraud", and "Multimedia". The main content area features a "Welcome to GAO" message, a "Recently Issued Products" section with links to "Reports & Testimonies", "Legal Decisions & Opinions", and "Comptroller General Presentations", and a "Featured Content" section titled "GAO High Risk" with a sub-heading "Following the Money: GAO's Oversight of the Recovery Act". A yellow arrow points from the text above to the search bar on the website.