

Special section reprint from

The **COAST GUARD** Journal of Safety
& Security at Sea
PROCEEDINGS
of the Marine Safety & Security Council
Summer 2008



U.S. Department
of Homeland Security

United States
Coast Guard

Information Sharing

- *Future Forecast*
- *Cultural Change*
- *Successes in the Field*



INFORMATION



Information Sharing

We all "need to know."

Executive Perspective

by MR. JAMES F. SLOAN

U.S. Coast Guard Assistant Commandant for Intelligence and Criminal Investigations

By presidential declaration, information sharing has been an administration priority since the September 11th attacks. The "need to know" culture of the Cold War era is now a handicap that threatens our ability to uncover, respond, and protect against threats to our national security. Law enforcement organizations and intelligence agencies from the federal level to state, local, and tribal authorities have developed their own networks and data repositories, making it difficult to share data necessary to aggressively plan, communicate, and intercede to thwart a future terrorist attack in a timely manner.

In October 2007, President Bush signed the National Strategy for Information Sharing. This document describes the information sharing vision that has guided the administration for the past seven years. The strategy lays out a plan to establish more integrated information sharing to ensure that those who need information will receive it, and those who have access to information will share it.

Within the intelligence community, Director of National Intelligence Michael McConnell has made accelerating and improving information sharing one of his top priorities. He has called upon the intelligence community to transform its culture to one where the responsibility to provide information is a central tenet. Several major factors drive the need for change. These include the

ever-evolving threat environment of the 21st century, recently established national and homeland security customers, and emerging asymmetrical threats that require synthesizing intelligence from a greater variety of sources.

As a reader of *Proceedings*, you have a personal responsibility to follow information sharing protocols. Within the maritime domain, whether you are a government employee or an interested stakeholder, information sharing is a collective responsibility. We must balance our country's civil liberties with the timely exchange of information in order to protect our ports and maritime interests. I hope you find this special information sharing section informative and instructive.



About the author:

As the U.S. Coast Guard Assistant Commandant for Intelligence and Criminal Investigations, Mr. Sloan directs, coordinates, and oversees all intelligence and investigative operations and activities. His previous leadership experience comes from working with law enforcement, intelligence communities, foreign governments, and financial and regulatory sectors in such positions as the director of the Financial Crimes Enforcement Network and acting undersecretary of enforcement for the Department of the Treasury.

Additionally, Mr. Sloan served with the United States Secret Service for 21 years, most recently as the agency's deputy assistant director for protective operations, and was senior program manager of its antiterrorism programs. Prior to joining the Secret Service, he served as a police officer, investigator, and as a lieutenant in the U.S. Army.

Information Sharing in the 21st Century



Information Sharing Coordination Council Perspective

by CAPT CHRISTOPHER J. TOMNEY

Chief, U.S. Coast Guard Office of Intelligence Plans and Policy

Twenty-first-century problems require 21st-century solutions. This is especially true in the area of information sharing. Director of National Intelligence Michael McConnell has repeatedly stated that our federal agencies must evolve beyond the 20th century mentality of a “need to know” when it comes to information sharing. While this philosophy worked well during the Cold War when dealing with more traditional threats, today’s digital world, at risk from asymmetrical threats, requires a more timely exchange of information from those who possess it to those who require it for mission execution. No longer is “need to know” an acceptable principle. As Mr. McConnell stated, we must get beyond the old “need to know” norm to a new paradigm of the “responsibility to provide.”

As a law enforcement and regulatory agency that is also a military service and intelligence community member, the United States Coast Guard is in a unique position to acquire and disseminate information to Coast Guard decision makers and operational commanders, as well as to our interagency, industry, and international partners. Information sharing is a fundamental responsibility of every Coast Guard employee. Information stovepipes within the Coast Guard and the larger government community must be eliminated and replaced by enduring protocols, policies, and procedures that promote the sharing of information while protecting sources, respecting security requirements, and abiding by civil liberties protection.

True information sharing ensures that consumers have the information they need when they need it. Users must be able to discover the existence of information and retrieve relevant information when needed. Intelligence analysts must have access to the most sensitive information when creating a product. This information must be accessible through an infrastructure that supports information discovery, retrieval, and collaboration.

This section of *Proceedings* highlights ongoing efforts to establish a culture of information sharing within the Coast Guard. I hope the following articles will stimulate organizational dialogue on additional actions our service can undertake to achieve the spirit and intent of national information sharing initiatives.



About the author:

CAPT Christopher J. Tomney has served in various afloat assignments aboard USCGC Diligence and USCGC Confidence. He served as commanding officer, USCGC Point Monroe and USCGC Ocracoke. For two years CAPT Tomney was dual-hatted as the Coast Guard Group Key West law enforcement division officer and officer-in-charge of Law Enforcement Detachment Two.

CAPT Tomney headed the Coast Guard's Operational Intelligence School in Yorktown, Va. Following this, he was dual-hatted as USCG Pacific Area Intelligence Division deputy division chief and director of intelligence operations. He was then deputy director of the Coast Guard's Counterintelligence Service at USCG headquarters. He is presently chief of the Office of Intelligence Plans and Policy within the USCG Directorate of Intelligence and Criminal Investigations.

CAPT Tomney holds a bachelor of science degree in marine science from the U.S. Coast Guard Academy and a master of science degree in strategic intelligence from the Defense Intelligence College.



INFORMATION



Creating a Culture of Information Sharing

Information Sharing Executive Agent's Perspective

by Ms. SUSAN HENRY

U.S. Coast Guard Information Sharing Executive Agent

At long last, more than three years after publication of the 9/11 Commission Report¹ and many executive branch memoranda later, Congress passed the Implementing Recommendations of the 9/11 Commission Act of 2007. It was signed into law on August 3, 2007,² bringing assessment of federal information sharing practices and performance into sharper focus. Though annual assessment of federal information sharing had already been mandated under the Intelligence Reform and Terrorism Prevention Act of 2004,³ the ownership and scope of the process were uncertain, and the reorganization of the intelligence community was still in progress.

The interpretation of information sharing within the Department of Homeland Security (DHS) has also been

evolving since 2004. Under the current DHS executive leadership, federal information sharing mandates are no longer applied specifically to counter-terrorist intelligence. Within DHS, the vision of our responsibility to share stretches across all threats, all hazards, and all missions under the department's purview. The Coast Guard is accountable for our information sharing performance across all maritime regimes and all missions, with a huge number and variety of partners.

New Annual Performance Measures

A few months after the 9/11 Commission Act was passed, the program manager for the information sharing environment of the Office of the Director of National Intelligence (ODNI) began working closely with DHS and other federal departments and agencies to

| SAFETY <i>Saving Lives & Protecting Property</i> | SECURITY <i>Establishing & Maintaining a Secure Maritime System while Facilitating its Use for the National Good</i> | STEWARDSHIP <i>Managing the Sustainable & Effective Use of Its Inland, Coastal and Ocean Waters & Resources for the Future</i> |
|--|---|--|
| Search and Rescue Marine Safety | Ports, Waterways & Coastal Security Illegal Drug Interdiction Undocumented Migrant Interdiction Defense Readiness Other Law Enforcement | Marine Environmental Protection Living Marine Resources Aids to Navigation Ice Operations |

Coast Guard missions, excerpted from the "2008 Budget in Brief and Performance Summary," Feb. 2007.



identify specific, achievable measures of information sharing performance. The baseline measures focus on several key improvement categories, including:

- establishing integrated policy and practices, such as international agreements, privacy policy, and interagency reporting of suspicious activities;
- establishing agency-level information sharing governance;
- implementing joint federal/state/local fusion centers and “common terrorism information sharing” standards;
- cultural transformation (including personnel incentives and disincentives) and training.

This summer ODNI used an overall list of 14 key measures to create and present the first annual report to Congress.

How Do We Measure Up?

Coast Guard missions have always required information sharing with international, federal, state, local, tribal, industry, public, and private partners. As a result of our tradition of information sharing, our entering position against the new baseline measures is strong. Coast Guard sector commanders have actively pursued new collaborative planning, prevention, and response partnerships at the local level. Regional alliances promoted by federal law, policy, sponsorship, and grants, such as area maritime security committees, have been added to existing area contingency plan-based and Incident Command System-oriented partnerships.

Since 2006, field surveys of selected critical ports indicate that each Coast Guard sector command typically engages more than 100 active port partners in a multitude of partnerships and forums.⁴ These surveys also identified a wealth of best practices, along with many practical recommendations for improving information sharing. Frustrations reported in recent surveys most often related to shortfalls of personnel, lack of shared networked capabilities, and insufficient funds for the joint training needed to sustain and expand collaborative partnerships. Nevertheless, working within our resource constraints, the culture of information sharing called for in the 9/11 Commission Report is already an everyday reality for Coast Guard field units.

Information sharing partnerships are also a high priority in Washington, D.C. The Commandant of the Coast

Guard and the Commissioner of Customs and Border Protection initiated a senior guidance team in 2006. In 2008, the Assistant Secretary, Immigrations and Customs Enforcement joined this strategic alliance, which is intended to strengthen collaboration in the field by directing and overseeing specific near-term actions.



CAPT Patrick Trapp, commander, Sector Hampton Roads, reviews each partner's role during a preparedness for response exercise. USCG photo.

DHS is forming several focused shared mission communities, beginning with the Law Enforcement Shared Mission Community, officially launched in January 2008. This group, which includes active Coast Guard members, has been working to identify and clear away information sharing obstructions among DHS and agency members, and to improve understanding of valid legal constraints on information sharing. The group has produced an information sharing strategy document,⁵ has begun to develop a shared data architecture, and is supporting an interagency information sharing pilot activity in Los Angeles. Future outreach beyond DHS is planned later this year, expanding the collaboration to other federal, state, and local partners.

New shared mission communities will focus on other aspects of the “all threats, all hazards” DHS realm, establishing policy-level collaboration in critical infrastructure, incident response, and other concerns crucial to safety and security. These will cut across all Coast Guard missions, and all will require Coast Guard representation.

What Do We Still Need to Do?

The new annual federal performance measures require us to take some additional steps forward to account for the information sharing we already do. We need to establish enterprise information sharing governance, an ef-

fort that is part of the ongoing Coast Guard re-organization. We need to develop an agency-level information sharing strategy that publicly articulates the improvements we intend to support and invest in for the future, based on the U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship, and in concert with DHS and national strategies.⁶ We need to continue to develop an information sharing segment architecture to ensure that our essential exchanges of information with our partners become part of our capability requirements. We also clearly need better collaborative, networked capabilities to work efficiently and effectively with our partners at local and regional levels.

Consistent with the 9/11 Commission Report's call to "unity of effort" in information sharing, the new federal annual performance measures also call us to create a culture of information sharing. To facilitate this, we must include measurable improvements to our personnel evaluation and appraisal standards and institute incentives and rewards for excellence in information sharing, as well as disincentives for obstructing information sharing with our partners. We are also now required to institute and report completion percentages on information sharing training to emphasize the importance of the responsibility to share, in balance to the traditional "need to know" information security rule. We must train Coast Guard personnel to be able to foresee the severe consequences of not sharing mission-essential information with our legitimate partners.

As a whole, our monitoring of Coast Guard field units' information sharing practices shows a multi-mission federal agency stretching to the limits of its resources to share information in order to increase operational effectiveness. The new federal information sharing performance measures give us additional opportunities to showcase successful partnering, better document our constraints, and continue to improve the safety and security of the U.S. maritime domain.

About the author:

Ms. Henry is a career information architect and system engineer who specializes in operational requirements analysis. She is a retired naval officer (cryptologist). She has served the Coast Guard since 1994, following assignments with the Navy, the Marine Corps, the U.S. Pacific Command, and the national intelligence community. She completed her undergraduate and graduate studies in information systems, applied mathematics, and organizational communications at the University of Hawaii.

Endnotes:

- ¹ The 9/11 Commission Report, July 22, 2004, identified information sharing failures and barriers impeding homeland security; Chapter 13 focuses on information sharing.
- ² Public Law 110-53, "Implementing Recommendations of the 9/11 Commission Act of 2007," Aug. 3, 2007.
- ³ Public Law 108-458, "Intelligence Reform and Terrorism Prevention Act of 2004," Dec. 17, 2004, section 1016.
- ⁴ "Port Inter-Agency Information Sharing Requirements Annual Assessment," Apr. 2008, and related survey data collected by the Coast Guard Research and Development Center from 2006 to present.
- ⁵ "Law Enforcement Information Sharing Strategy," Apr. 2008, DHS Intelligence & Analysis, approval pending.
- ⁶ "National Strategy for Information Sharing," White House, Oct. 2007. A companion DHS "Information Sharing Strategy" is in progress.



Capt. Philip Kenul, commanding officer of NOAA Aircraft Operations Center at McDill Air Force Base in Tampa, Fla., along with Rear Adm. David Kunkel, commander of the Seventh Coast Guard District talk about partnership response efforts during potential hurricanes and the importance of preparedness prior to the arrival of a hurricane. Government agencies have a responsibility to alert citizens and respond to those in distress. U.S. Coast Guard photo by PA1 Dana Warr.

Integrated Border Enforcement Teams

New measures to combat cross-border crime.

by CDR SLOAN TYLER
*Development Officer, Border Security Program
U.S. Coast Guard Office of Law Enforcement*

When talk turns to illegal immigration, drugs, and crime, there is a propensity to focus on the southern border of the U.S. as the greatest homeland security challenge. Migrant interdictions and drug seizures along the Mexican border and Florida coast routinely attract attention and media interest. Although our southern border is approximately 2,000 miles long, its length comes in a distant second when compared with the border of more than 5,500 miles dividing the United States and Canada.

This international boundary is a multifaceted line of demarcation spanning three oceans, the Great Lakes, and 14 states. It includes 1,500 miles separating British Columbia and the Yukon Territory from Alaska and is the most expansive, unguarded border in the world.

While travel in and out of the country is generally done through a United States port of entry, a vast portion of our shared border is protected primarily by isolation and inaccessibility. Some geographic areas that are accessible but isolated, such as open fields or farmland, have wide-ranging border security measures. Some areas are “self-reporting,” while others monitor individuals who bypass the designated port of entry with hidden sensors along back roads and trails.

Not on Our Water—Introducing Integrated Border Enforcement Teams

These areas may also be used to further criminal activity. In the maritime regions of these remote areas, the U.S. Coast Guard, U.S. Customs and Border Protection,

the Office of Border Patrol, U.S. Immigration and Customs Enforcement, and our law enforcement partners in Canada are working together to deny criminals the use of our nations’ waterways for illicit activity.

Border security and smuggling are systemic issues, dating back hundreds of years. Despite the ruggedness and inaccessibility of the terrain, the region had become a profitable, safe haven for organized criminal smuggling networks. In the mid-1990s the Canadians expanded the scope of integrated border enforcement teams (IBETs), which were originally implemented to address cross-border crime in a specific region between British Columbia and Washington state.

For years the illegal movement of people and contraband through this remote segment of the international border was investigated by the first law enforcement agency to respond. U.S. and Canadian law enforcement personnel used traditional investigative methods on a case-by-case basis. The integrated border enforcement teams combine the efforts of more than 50 federal,

INFORMATION



This vessel was specifically designed to smuggle cigarettes into Canada. USCG District 9 photo.



provincial, state, county, and municipal agencies. Their use was a significant change for law enforcement operations in that area.

Since September 11, 2001, border security along the U.S./Canadian border has been dramatically tightened as both nations strive to coordinate and cooperate to improve tactical and strategic information sharing. Today IBETs operate in strategic locations all along this border. Of these, several are focused on marine areas, including the Great Lakes/St. Lawrence Seaway region.

Top Official Buy-In

In December 2001, Homeland Security Advisor Tom Ridge and Canada's Deputy Prime Minister John Manley signed the Smart Border Declaration. The goal: to enhance the security of our shared border while facilitating the legitimate flow of people and commerce. Enhancing communication and coordination between the two nations and expanding integrated border enforcement teams were key commitments in the declaration.

Attorney General John Ashcroft, one of the first to publicly recognize the importance of the new relationship, remarked, "When we strengthen our northern border, we effectively deter those who may try and es-

cape detection, arrest, or prosecution. These integrated border enforcement teams not only enhance our border integrity, but also demonstrate the success of our joint cooperation on cross-border law enforcement."¹

IBET partnerships have become an effective multi-agency international task force. The goal is to align multinational, tiered resources in targeted areas presenting the greatest threat and to interdict criminal activity at border choke points. The construct employs a risk management approach designed to assess vulnerabilities and engage in proactive planning. IBETs focus on identifying, investigating, and interdicting persons and organizations that pose a threat to national security or are

engaged in other organized criminal activity.

Operation Shiprider

The Coast Guard has engaged the Royal Canadian Mounted Police (RCMP) in several joint initiatives along the U.S. and Canadian maritime border. Beginning in 2005, the Coast Guard and the RCMP participated in "Shiprider," several integrated maritime security pilot projects designed to test the concept of joint law enforcement operations in the maritime arena.

Shiprider was specifically designed as a tool to support integrated border enforcement team operations. To facilitate, each government cross-designated its counterpart law enforcement officers. For example, U.S. Immigration and Customs Enforcement cross-designated RCMP officers as customs officers. The RCMP cross-designated Coast Guard officers as "special supernumerary constables." Prior to participation in joint operations, Coast Guard and RCMP officers received law enforcement training on the duties and responsibilities involved with their cross designation at the Coast Guard's Maritime Law Enforcement Academy in Charleston, S.C.

This system allowed armed agents of both countries to conduct joint law enforcement

IBET Partners

Although the concept of the integrated border enforcement team was first implemented in Canada, the program has matured to a multifaceted law enforcement initiative comprised of Canadian and American law enforcement partners. The five core IBET partners are:

- the Royal Canadian Mounted Police,
- U.S. Customs and Border Protection,
- Canada Border Services Agency,
- U.S. Immigration and Customs Enforcement,
- the U.S. Coast Guard.

While these five agencies are core partners, regional, federal, state, local, provincial, and tribal law enforcement personnel are critical to effectively combating cross-border crime.

designed as a tool to support integrated border enforcement team operations. To facilitate, each govern-

CBP vessel on patrol. Photo courtesy of U.S. Customs and Border Protection.



operations in both nations' waters. The RCMP officer would have the primary lead in Canadian waters, with a Coast Guard officer supporting as directed. The converse would be true while in U.S. waters. The operation intended to remove the maritime border as an impediment to cross-border law enforcement, increasing operational effectiveness.



Shiprider participants from left: Petty Officer Craig Campbell, USCG; Constable Andrew Smith, RCMP; Petty Officer Kenneth Freeman, USCG; Constable Wally Silver, RCMP; Constable Robert Trepanier, RCMP; Petty Officer Robert Foucha, USCG. District 9 photo.

In January of 2007, the United States and Canada began the process to permanently establish Shiprider. The envisioned framework will be designed to enhance the level of cooperation in the maritime arena and will take an integrated operational approach to maritime law enforcement. The bi-national agreement will also address the complex legal issues and sensitive privacy concerns involved with law enforcement information sharing.

Solidifying Operations

As with any new international initiative, there are areas that will require development, continued bi-national support, mid-course monitoring, and improvements. Issues such as dedication of personnel and afloat/ashore assets, cross-border law enforcement training, communication interoperability, and information sharing will all need to be addressed. A year-long pilot project is planned to beta-test a new radio system that will address common frequency bands and the barriers in telecommunications laws.

enforcement team program. This program is a model for international cross-border law enforcement between two countries that have common national security interests ... The recent 2007 Operation Shiprider successfully

demonstrated bi-national cooperation during its two-month period of focused information sharing and integrated maritime operations. The IBET program's efforts to date are just the beginning of a long and fruitful relationship for all five core partners and other law enforcement agencies."

Shiprider Pilot Program

The most recent Shiprider pilot was a two-month project completed on September 30, 2007. Operations were conducted in Massena, N.Y., and in Blaine, Wash. Forty USCG and RCMP shipriders conducted more than 1,200 integrated patrols and performed 187 vessel boardings that resulted in 12 arrests and seizure of six vessels, 214 pounds of marijuana, over 1 million contraband cigarettes, and \$38,000 in illicit cash.

Shipriders also conducted several search and rescue missions and collected intelligence for shore-based investigators on both sides of the border. It was noted that Shiprider operations resulted in marked increase in land seizures of contraband (including tobacco, currency, drugs, and weapons) in the Massena area, demonstrating the potential for deterrent effect and displacement of cross-border criminal activity.

In assessing the value added by the operation, Ninth District IBET liaison officer LCDR Marc Burd stated, "A Shiprider crew allows the usual impediment of the international border, used by smugglers and organized crime as a shield to hide behind, to be torn away and replaced with a multi-jurisdictional officer's badge, assisting our law enforcement partners on both sides of the border."

About the author:

CDR Tyler is the border security program development officer at the Office of Law Enforcement at Coast Guard headquarters. She is responsible for the development and oversight of maritime law enforcement border policies and procedures. She has been with the Coast Guard since 1991 and has served in various capacities, such as legal counsel for the fisheries and alien migrant interdiction programs; JAG officer at the First Coast Guard District; criminal justice instructor at the Coast Guard Academy; and base legal officer, Kodiak, Alaska. She holds a B.A. in mathematics from Boston College and a J.D. from Suffolk Law School.

Acknowledgements:

LCDR Marc Burd, U.S. Coast Guard District Nine, and Mr. Ben Thomason, program analyst, USCG Atlantic Area.

Endnote:

¹ Dept. of Justice press release, November 19, 2003.





The International Trade Data System

The Coast Guard joins a global data-sharing initiative.

by LCDR MIKE DOLAN
Chief, Cargo Security Branch
U.S. Coast Guard Office of Port and Facility Activities

On January 24, 2008, RDML Brian Salerno, the U.S. Coast Guard Assistant Commandant for Marine Safety, Security and Stewardship, signed a letter of intent for the Coast Guard to become the 43rd participating government agency in the International Trade Data System. This decision opens the door for the Coast Guard to explore new ideas for using information to improve programs, harmonize processes with other agencies, and reduce regulatory burden on industry.

When announced at the February 2008 meeting of the Commercial Operators Advisory Committee, this decision generated applause and acclaim. The senior industry leaders who comprise the committee represent major companies that import the consumer goods our nation relies on. These leaders know that the global marketplace's future progress requires an emphasis on data and technology. As a heavily regulated community, they were happy to see the Coast Guard join a project intended to streamline the process of delivering required information to the government.

So What Is the International Trade Data System?

The International Trade Data System (ITDS) is an ongoing, long-term U.S. interagency community of interest. The Customs and Border Protection automated commercial environment (ACE) major acquisition project, which is creating and modernizing computer network interfaces with the international trade community, supports the ITDS community. The ITDS members' requirements will shape the spiral development of ACE capabilities. The objective is to provide a

single portal for commercial entities to submit all trade data and information required by the federal government. Once through the ACE portal, the data then goes into the ITDS community's repository.

The project intends to facilitate more streamlined operations in that commercial entities will submit information to the government only once, in paperless form. Currently, many different agencies require information from commercial entities, and companies must respond to each agency individually, often on paper. The ITDS-sponsored ACE project will greatly simplify and expedite interaction with the federal government. Just as importantly, regulatory agencies will benefit by having complete visibility of all trade data along with connection to all the other agencies' programs and activities.

Opportunities for interagency coordination and program improvement abound, and some agencies have already reaped benefits. For example, the Federal Safety Inspection Service achieved a 44-fold increase in the tonnage of ineligible product detected, detained, and removed from the food supply in one year using information obtained through an early version of the ACE portal.¹

Why Is This Important to the Coast Guard?

Like most high-level policy issues, the decision to participate in ITDS had both political and pragmatic drivers and implications. First, the politics. Signed into law in October 2006, the Security and Accountability for Every Port Act of 2006 states, "All federal agencies that

require documentation for clearing or licensing the importation and exportation of cargo shall participate in the ITDS.” The act also states, “It is the sense of Congress that agency participation in the ITDS is an important priority of the federal government ...”²

Originally it was assumed that the law did not require the Coast Guard to participate in the International Trade Data System because the agency does not conduct the activities listed for clearing cargo. However, the Coast Guard is a border security agency responsible for clearing the vessels that move the bulk of imported cargo. That’s where pragmatic considerations came into play: it was clear that, to maximize the system’s potential, Congress expected all federal agencies to support the ITDS project. If it declined to join, the Coast Guard risked alienating itself from Congress, dozens of other federal agencies, and the international trade system—not a good position to be in.

Additionally, Coast Guard leadership began to see potential value in the concept. Program managers started to recognize that participation in the International Trade Data System could give the Coast Guard not only access to information, but to other agencies’ processes and programs, as well. This access would have a cumulative value that exceeded any cost of participation.

Finally, because the ACE system and the ITDS agency network interfaces were already being built, the Coast Guard realized that the window of opportunity was limited. The longer the wait to join, the less influence it would have had on the design of the network interface. And so, with a leap of faith, the Coast Guard joined the International Trade Data System with some visionary ideas of what it might achieve.

Big Challenges

Now we come to the not-so-fun part of participation in ITDS and ACE—figuring out all the possible pitfalls and hurdles inherent in any new, complex information network. The technical hurdles are probably the easiest to spot, such as standard network interface issues consisting of varied connection and data security issues. The most problematic hurdle will be integrating existing Coast Guard systems with the International Trade Data System design and architecture, if necessary. This will depend entirely on which projects are pursued, because each project will be associated with its supporting systems. For example, the integration of the Coast Guard’s Marine Information for Safety and Law Enforcement (MISLE) system may depend upon the hazardous materials safety program.



Daily Coast Guard activities are becoming increasingly driven by information management and networking with other agencies. USCG photo by Mr. Telfair Brown.

To even begin to understand the technical challenges ahead, we have to recognize the scope of policy development that must take place. Participating government agency status requires its own set of obligations, such as developing a concept of operations and possibly even memorandums of understanding or memorandums of agreements. Once the interagency instruments are in place, the Coast Guard must then analyze the constraints of existing agency policy, both programmatic and technological. This may restrict the scope of proposed projects and applications. This work will also uncover gaps in policy that may need to be addressed.

Finally, we recognize that once ITDS is ready for use, personnel will need sufficient guidance and training to capitalize on the available information. Because the ACE portal is web-based, there won’t be new hardware requirements, but personnel will still need to know how to enter and navigate the interface to retrieve information.

As a large, complex organization, we are at the most exciting phase of this new initiative. We are envisioning all the wonderful things that we can achieve, and stand ready to deal with the challenges that lie ahead. Participation in the International Trade Data System gives us a powerful tool and a path forward to make sure that the Coast Guard stays current with technology and stays engaged with the regulated community.

About the author:

In his current headquarters assignment, LCDR Mike Dolan works on international and domestic cargo security standards and strives to align cargo security policies between the Coast Guard and other DHS agencies. LCDR Dolan enlisted in the Coast Guard in 1991. He is a graduate of Embry Riddle Aeronautical University, Marine Corps Expeditionary Warfare School, and the Naval War College.

Endnotes:

- ¹ Report to Congress on the International Trade Data System, November 2007, page 12.
- ² Public Law 109-347, Section 405.



Managing the Risk

The National Small Vessel Security Summit.

by MR. DAVID M. VAN NEVEL
Maritime Program Specialist
U.S. Coast Guard Maritime Domain Awareness and Information Sharing

Since 9/11, much of the focus in maritime security has been on large commercial vessels. However, world events have led many security experts to become concerned that terrorists could exploit small vessels (those of less than 300 gross tons) to cause disruption and damage to our maritime transportation system. Small commercial vessels run the gamut from towing and fishing vessels to uninspected passenger vessels. Recreational small vessels could be anything from jet skis to yachts. There are approximately 13 million registered recreational vessels¹ as well as an estimated 4 million unregistered recreational boats in the United States.²

Additionally, large numbers of small vessels operate within close proximity to critical infrastructure.³ One limited study of select ports around the U.S. showed that many small vessels were likely to operate within close proximity to important infrastructure. For nine ports examined, there were approximately 3,000 small commercial vessels, 3,000 fishing vessels, and 400,000 recreational vessels that were likely to operate near important maritime infrastructure.⁴

The National Small Vessel Security Summit

With such large numbers of small vessels operating within the vicinity of critical infrastructure, complete elimination of risk would be impossible without sacrificing fundamental freedoms and individual liberty. The goal, therefore, is to manage this risk based on the expected consequences, resulting in acceptable levels of security.

The Department of Homeland Security (DHS) recognized that the agency should address small vessel risks

INFORMATION



Admiral Thad Allen, Commandant, USCG, responds to a participant question. USCG photos by Mr. Telfair H. Brown.

in close consultation with small vessel stakeholders. Therefore, DHS invited more than 400 participants with a range of interests in small vessels to the National Small Vessel Security Summit. Presenters included the honorable Michael Chertoff, Secretary, U.S. Department of Homeland Security; ADM Thad Allen, Commandant, U.S. Coast Guard; Mr. W. Ralph Basham, Commissioner, U.S. Customs and Border Protection; and Mr. Vayl Oxford, Director, Domestic Nuclear Detection Office.

Over the course of two days in June 2007, DHS personnel and other officials engaged small vessel stakeholders in discussions on a range of issues regarding security risks relevant to small vessel operations in the





DHS Secretary Michael Chertoff delivers the keynote address, underscoring the importance the agency places on small vessel security.

U.S. maritime domain. Objectives for the National Small Vessel Security Summit included:

- Educate small vessel stakeholders on security risks in the U.S. maritime domain.
- Provide a national forum for small vessel stakeholders to present and discuss their ideas on developing security measures to mitigate gaps in small vessel management and control in the maritime domain.
- Provide a national forum for state and local government officials, as well as private members of the small vessel population, to discuss transportation concerns regarding security threats and present their ideas for addressing those threats.
- Record all issues and concerns from the small vessel stakeholders and complete an after-action report for the public, industry, and government to support conclusions for national-level decisions involving the development of small vessel security measures to detect, deter, interdict, and defeat terrorist use of small vessels in the U.S. maritime domain.⁵

The Department of Homeland Security recognized that not everyone interested in small vessel security could make the trip to the Washington, D.C., area. Furthermore, issues vary significantly among regions, so a number of regional summits are planned as well. Interested parties can check for further information on the regional summits at www.dhs.gov.

DHS Response

Although the dialogue with the small vessel community is still ongoing, DHS has already started to take action on summit findings. For example, the agency organized a small vessel security workgroup to draft a DHS small vessel security strategy.

Since the summit, the Coast Guard has launched the vessel identification system (VIS). VIS data consists of registration and ownership data from participating VIS states and the USCG National Vessel Documentation Center. VIS data will only be accessible to registration and law enforcement personnel. States that participate in the VIS will have access to boat registration and ownership data from other states and USCG-documented vessels in a single database.

The Coast Guard is also working diligently to improve America's Waterway Watch (AWW), which seeks to leverage those who live and work in and around our nation's waterways as an additional set of eyes and ears.⁶ In addition to increasing public awareness of the AWW program, the Coast Guard is also in the process of developing and expanding an effort modeled after the 13th District's Citizen's Action Network.⁷ It is currently working to expand the Citizen's Action Network program nationally, recruiting volunteer citizens to act as a force multiplier for the Coast Guard and training them to be agents of maritime domain awareness.

The U.S. Department of Homeland Security's Domestic Nuclear Detection Office announced a pilot program that will provide maritime radiation detection capabilities for state and local authorities in Washington's Puget Sound and California's San Diego areas. The program involves development of a radiation detection architecture that will reduce the risk of radiological and nuclear threats that could be illegally transported on recreational or small commercial vessels.

The national summit is but the first step in a series of efforts to build a culture of partnership between the government and the small vessel community. Much work remains to be done, but with the publication of the DHS small vessel security strategy, the private sector and federal, state, and local governments will have a common framework as we work together to reduce small vessel-related risks.

About the author:

Mr. Van Nevel is a graduate of the U.S. Coast Guard Academy and Georgetown University Law Center. He served on active duty and in the U.S. Coast Guard Reserve. Mr. Van Nevel is a maritime program specialist on the USCG headquarters Maritime Domain Awareness and Information Sharing staff.

Endnotes:

- ¹ "2006 Boating Statistics," COMDTPUB 16754.20, U.S. Coast Guard, p. 18.
- ² "United States Coast Guard Navigation Safety Information Prototype User Needs and Wants Study/Business Case," U.S. Coast Guard Research and Development Center, March 10, 2003, Table 5: NSI User Group Characteristics.
- ³ The USA Patriot Act of 2001, 42 U.S.C. § 519 c(e), defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and as-

- sets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."
- ⁴ "An Assessment of Small Vessel Populations in U.S. Waters," U.S. Coast Guard Research and Development Center, June 2007, p. 31.
 - ⁵ "Report of the DHS National Small Vessel Security Summit," Homeland Security Institute, October 19, 2007. This report is available at www.dhs.gov.
 - ⁶ For more information on AWW, visit www.americaswaterwaywatch.org.
 - ⁷ For more information on the program, see www.uscg.mil/d13/can/.

PARTICIPANT FINDINGS

Discussions at the summit were wide-ranging and covered many aspects of maritime governance.

Highlights included:

Need for a national strategy

This strategy should address international cooperation to identify threats as far from our shores as possible. It needs to be flexible to allow for local conditions and should not advocate procedures that are unduly burdensome or overly restrictive.

Stakeholder view of the small vessel threat

Participants generally viewed recreational vessels as a larger threat than commercial small vessels. Small commercial operators tend to be involved in smaller, closer-knit maritime communities and are on the water every day, making it more likely that these operators would notice if something was amiss.

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

Participants felt that overly restrictive and burdensome regulations do little to increase security, and will alienate the small vessel community.

Improve intelligence, analysis, and dissemination

Summit stakeholders generally agreed that there needs to be improved intelligence and the ability to act upon it.

Expand education and outreach to citizen stakeholders

America's Waterway Watch was discussed extensively, and summit participants expressed a very strong consensus that it needs to be expanded and re-energized.

Operator and vessel identification

Opposition to a "federal" recreational boating license was universal. There was some acceptance of boating licenses that would incorporate already existing identifications, such as a "boating" endorsement on a state motor vehicle operator's license.

Employ technologies to detect radiological and nuclear threats

There was widespread support for use of radiation detectors, despite some concern over operational effectiveness and the ability to use them far enough away from the port to allow for adequate response.

Reassess security zones

Security zones were the subject of much discussion at the summit. There was not, however, a consensus on whether they should be more clearly marked and publicized. Some felt that this might make it easier to identify possible targets of attack. There was agreement, however, on the need to educate the boating public on safety and security zones.

Endnote:

Adapted from the "Report of the DHS National Small Vessel Security Summit," Homeland Security Institute, October 19, 2007. This report is available at www.dhs.gov.



INFORMATION



The Hawaii Superferry

Information sharing leads to operational success.

by CAPT VINCE ATKINS
former Commander, U.S. Coast Guard Sector Honolulu

ENS MEGHAN HOUGH
U.S. Coast Guard Sector Honolulu

The complexities of maritime operations are often compounded by factors such as the variability of the sea itself, differing and sometimes overlapping legal authorities, and the presence of a wide range of concerned agencies with varying competencies and capabilities. Information sharing reduces operational complexity and sets the stage for success. A recent operation in Hawaii underscores how information sharing, taken in the broadest sense, can increase interagency effectiveness and public understanding.

Hawaii Superferry (HSF) came to Hawaii to start a high-speed ferry service between the Hawaiian islands of Oahu, Maui, and Kauai. The Superferry vessel, the *Alakai*, is a 350-foot high-speed catamaran designed to carry 866 passengers and 282 vehicles.

Unfortunately, strong opposition from segments of the local population shadowed the start of *Alakai's* service. Citizens and environmental groups opposed to this new service voiced several concerns, citing *Alakai's* lack of an environmental impact study, the possibility of increased traffic congestion, and the potential for introducing invasive species and harming marine life. Legal challenges were initially successful in Maui, but did not preclude HSF operations into Kauai.



An *Alakai* protester in Nawiliwili Harbor, Kauai, demonstrates directly in front of the *Alakai*. Honolulu Star-Bulletin photograph by Mr. Tom Finnegan.

A Hostile Operating Environment

Alakai's initial operations were greeted by an estimated 300 protestors in Kauai. People gathered outside the ferry's shoreside facility, taunted would-be passengers, blocked vehicles, and, in some instances, caused minor property damage. Protesters on shore threw coconuts and other debris at Coast Guard responders and several scuffled with the Kauai Police. The crowd forced the HSF facility to close its gates due to security concerns.

While hundreds of protesters demonstrated on shore, some protesters entered the water and blocked the harbor with surfboards and kayaks, making it unsafe for the ferry to transit into the port. HSF decided to cancel its second Kauai port call, and, due to continuing public unrest, decided to temporarily halt its Kauai operations altogether.

Localized protests grew into a larger referendum on the pace of change in the Hawaiian Islands and dominated local headlines. Several court cases were initiated and court injunctions temporarily kept the *Alakai* from sailing. As the courts wrestled with the legalities of the situation, law enforcement agencies had to prepare for the ferry's possible return to full service and the subsequent widespread civil disturbances it could cause ashore and in the harbors.

Federal, state, and local authorities faced the challenge of balancing a number of seemingly contradictory objectives: upholding the law, ensuring public safety, ensuring the safe arrival and departure of the ferry in multiple ports and jurisdictions, and protecting and promoting constitutional freedoms. Information sharing was critical for successful operations. Further, information sharing needed to be viewed with the broadest scope—not just as an exchange among government agencies, but with the public at large.

Unique Challenges

Multiple agencies had to consider the possibility of same-day operations on two different islands, Maui and Kauai. Island differences such as port geography, community reactions, and local forces were critical planning considerations. As it turned out, HSF decided to continue to defer operations in Kauai due to simmering public sentiments, so actual operations only occurred in Maui. Kauai had still not started operations as of this issue's publication.

Early protests in Kauai were relatively small, but endangered public safety at sea and ashore. By blocking *Alakai's* transit into the harbor, protesters violated well-established security zone regulations designed to protect large-capacity passenger vessels. Likewise, since many of the protesters were either swimming, on surfboards, or in kayaks, agencies were concerned they could not move out of the *Alakai's* way fast enough, endangering themselves and/or the ferry. Further, the pro-



USCG Station Kauai's small boat is shown removing protesters on surfboards from the path of the *Alakai* into Nawiliwili Harbor, Kauai. Protesters were removed for their own safety and for the safety of the ferry and its passengers. USCG photo by Petty Officer 3rd Class Michael De Nyse.

testers could have been injured by the propeller-driven boats working to enforce the security zone.

The geographical consideration that both Maui's and Kauai's ports were small and did not leave much room for maneuvering or navigational error compounded both security and safety concerns. Hawaii's Department of Transportation was also concerned that other harbor traffic would be greatly impacted. In an island state (with only one port each to service Kauai and Maui), free-flowing maritime commerce is not just a business concern, but is central to the state government's ability to take care of its citizens. Almost all food, fuel, and consumer products has to arrive through the ports. The state could not risk the ferry blocking a channel if she were to go aground while avoiding protestors. It also wanted to avoid sending a signal that corporate citizens did not enjoy equal protection under the law.

Operational planning and execution posed other complications, as they would involve different county authorities for the two ports as well as different policing capabilities. It was unclear what reception the ferry might receive when operations resumed. The press, in "man on the street" interviews, led officials to conclude that demonstrations would be larger. As the situation developed, constitutional issues of freedom of speech and assembly arose. Also, local and cultural expecta-



tions of unfettered access to the sea became operational planning factors.

Not all public expectations were aligned with the protestors, however. Some citizens and industry groups were, ironically, concerned by Coast Guard and state and local law enforcement restraint in this matter. Some characterized this restraint as an inability or unwillingness to enforce the law and safeguard commerce. Some incorrectly extrapolated the seeming inability to control protestors as an inability to safeguard against potential terrorists. They reasoned that, if law enforcement couldn't handle civilians on surfboards, how could it withstand a determined terrorist attack within our ports? Public confidence was at stake.

Achieving Interagency Alignment

This unique situation of protesters operating both on land and in the water made it imperative for local, state, and federal agencies to work together in order to understand and align the various legal authorities and jurisdictional concerns. Pre-established, close interagency working relationships were essential to effective planning and mission execution. The Coast Guard; its port partners; and various county, state, and federal government officials routinely worked together on a number of committees, at exercises, and during other operational incidents. These mature relationships eased communications, created interagency trust, and en-

abled agreement on priorities and objectives, greatly increasing operational efficiency.

One local information sharing initiative paid huge dividends during this operation. The Hawaii State Law Enforcement Coalition (SLEC) is a multi-agency coalition of Hawaiian law enforcement agencies including the Coast Guard and the Hawaiian Departments of the Attorney General, Public Safety, Land and Natural Resources, and Transportation. The pre-established partnerships created by SLEC facilitated planning and logistics for this complex operation.

Another critical factor was the Coast Guard's excellent working relationship with the state of Hawaii. Direct communications between the district commander and the Hawaiian governor were frequent; discussions about operational courses of action and potential outcomes were frank; and decisions reflected the careful, necessary balance among public safety, maritime commerce, and the citizenry's right to lawful assembly and speech.

The mechanism that provided for information sharing and interagency alignment was a unified command structure consistent with the National Incident Management System. The Incident Command System (ICS) provides an organizational structure and process wherein agencies with differing authorities, competencies, and equities may come together to work toward a common goal. ICS provides a venue and process for information



An *Alakai* protester in Nawiliwili Harbor, Kauai, demonstrating in front of the ferry, creating serious safety and port security concerns. USCG photo by Petty Officer 3rd Class Michael De Nyse.

sharing, which can be especially helpful when there are complex issues to resolve.¹

Not all involved agencies were ICS-conversant at the beginning of the operation, but this did not prove to be a problem, as ICS processes are easily explained and understood.

The operational challenges, varying agency concerns, and differing agency capabilities were laid bare and discussed thoroughly during the frequent meetings of the unified command. Alignment, cooperation, and compromise were essential in driving toward an operational plan that met the seemingly incongruent objectives.

Execution of the Operation

The unified command worked together to develop a plan that recognized differing authorities and competencies. Operations were divided into two components: onshore and waterborne security operations. The local police department was in charge of onshore operations, while the Coast Guard took the lead in waterborne operations. The two groups collaborated and created an overall plan designed to reduce the number of on-water protesters, provided a pre-designated protest zone, and developed coordinated methods to deal with illegal and unsafe protests.

The relationship with the Maui County prosecutors and the Maui Police Department (MPD) was particularly important. Close coordination between federal and local prosecutors provided a plan that offered short-term support in processing illegal protesters and a long-term deterrent strategy to eventually reduce the numbers of protesters. MPD also worked extensively with the Coast Guard to ensure seamless jurisdiction from the shoreline into the water. The state Department of Land and Natural Resources (DLNR) provided jet skis to patrol the security zone boundaries. The state Department of Transportation provided logistics support essential to mission execution.

The coordinated plan required a temporary fixed security zone to ensure the safety of the vessel and its passengers. The Coast Guard issued an emergency regulation that permitted it to control harbor waters one hour prior to the ferry's arrival, during the time it was in port, and until 10 minutes after the ferry's departure. Concurrently, the fixed security zone provided for an area where protesters could legally assemble.

Operational Success

The implementation of the new security zone required extensive public affairs efforts to ensure the affected maritime stakeholders and ocean recreation community understood the scope of the security regulations. DLNR and county mayoral offices helped the outreach effort by connecting the unified command with protest groups and canoe and surfer clubs.

To allay concerns regarding access by other users not interested in protesting the ferry, the Coast Guard granted access on a vessel-by-vessel basis while the security zone was in effect. To increase compliance, the unified command formed a joint public information staff to meet with the public on several occasions to outline security zone boundaries and explain the legal consequences of violating the zone.

Public outreach proved successful in deterring a large number of protesters from illegally entering the on-water security zone. Information sharing helped inform the general public of the unified command's objectives. Certainly, a number of citizens disagreed with the operation, but others grew to understand and support the unified command's objectives.

It's important to note that the intended result of this information sharing process and interagency collaboration was not to change the protesters' opinions regarding the ferry operation. In this instance, information sharing achieved its intended goals: allowing the *Alakai* to transit in and out of Maui without incident, allowing protesters to voice their dissent, and helping agencies to make the best use of unique authorities and competencies.

About the authors:

CAPT Vince Atkins graduated from the Coast Guard Academy in 1982 and has served in commands ashore and afloat. At the time of the Alakai incident, CAPT Atkins served as commander of Sector Honolulu.

ENS Meghan Hough graduated from the Coast Guard Academy in 2007 and is stationed in the enforcement division at Sector Honolulu.

Acknowledgements:

The authors gratefully acknowledge the support of CDR Kathy Moore, CDR Todd Wiemers, and LT Darwin Jensen while developing this article, but more importantly, for their distinguished and professional conduct during the operation itself.

Endnote:

¹ For more information about the National Incident Management System and Incident Command System, see the Winter 2006-2007 edition of *Proceedings*.



INFORMATION



This Ain't Your Daddy's Coast Guard

A blueprint for change.

by MR. BEN THOMASON
Program Analyst, CACI Corporation

For those of us who have been around the Coast Guard for awhile, the past few years may well be remembered as the most dynamic in its history. The move to the Department of Homeland Security; the highly publicized Katrina rescues; deployable specialized forces; and the arrival of new cutters, boats, and aircraft have been the harbingers of a more significant transformation. In his state of the Coast Guard address, Coast Guard Commandant ADM Thad Allen outlined a synergistic strategy in pursuing the challenges of the 21st century:

"Achieving awareness in the maritime domain, including intelligence and information sharing at all levels of government, is a key to our maritime security. Better awareness of what is out there leads to better

unity of effort in maritime planning and operations. We need to have a common operating picture. We also need to integrate our operational capabilities and efforts with our private sector partners to better prepare for, respond to, and recover from incidents."¹

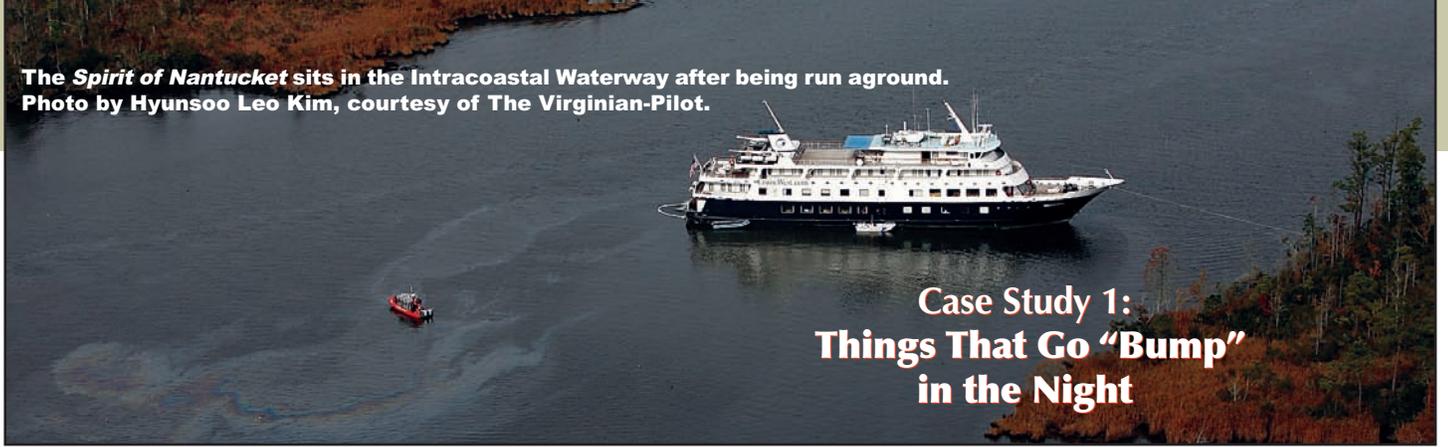
The Coast Guard has a strong leadership role in maritime security as articulated in the National Strategy for Maritime Security; the Coast Guard Strategy for Maritime Safety, Security and Stewardship; and the Safe Port Act of 2006. The questions at hand are "How well is the doctrine and policy implemented? How well does it actually work? What information sharing tactics, techniques, and procedures are in place?"

continued on page 22

Army Command Sgt. Maj. William J. Gainey, foreground, senior enlisted aide to the chairman of the Joint Chiefs of Staff, pilots a Coast Guard utility boat in the Chesapeake Bay with USCG Senior Chief Petty Officer Daniel B. Kilbourne. Sgt. Maj. Gainey recently toured Coast Guard Sector Hampton Roads units to meet Coast Guard personnel and to gain a better understanding of Coast Guard roles and missions. U.S. Coast Guard photo by Petty Officer 3rd Class Kip Wadlow.



The *Spirit of Nantucket* sits in the Intracoastal Waterway after being run aground. Photo by Hyunsoo Leo Kim, courtesy of The Virginian-Pilot.



Case Study 1: Things That Go “Bump” in the Night

At 5:30 a.m. on Nov. 8, 2007, the *Spirit of Nantucket* struck a submerged object while cruising from Alexandria, Va., to Charleston, S.C., and began taking on water in the Intracoastal Waterway near Pungo, Va. To stabilize the situation, the captain elected to ground the vessel. Sector Hampton Roads dispatched an HH-60J from Elizabeth City that lowered a rescue swimmer and dewatering pumps to the vessel. To facilitate information sharing, the command:

- initiated a command center critical incident communication to simultaneously brief the Fifth District, Atlantic Area, and Coast Guard headquarters within minutes of notification;
- alerted the maritime incident response team, which dispatched local municipal maritime first responders to the scene;
- briefed members of the Virginia Maritime Association and Virginia Port Authority of potential maritime transportation system issues.

The Two-Minute Drill

0610 - Incident reported to Coast Guard

0700 - Air Station Elizabeth City and Stations Portsmouth and Elizabeth City responders on scene; commenced dewatering and boom deployment

0740 - MIRT responded: EMS, police, fire

0745 - Incident command post established

1030 - Disembarked passengers via Coast Guard utility boat

1200 - Interagency planning initiated to stabilize vessel, mitigate pollution, draft salvage plan, secure waterway, and implement safety zone: issued urgent marine information bulletin and press release

1330 - Commenced dive/salvage operations

1700 - U.S. Army Corps of Engineers (USACE) surveyed area, found navigational hazard (NAVHAZ), marked channel

Friday 09 NOV 07

1300 - Salvage plan approved

1700 - USACE awarded commercial contract for NAVHAZ removal

1800 - Alternate channel marked for shallow-draft vessels

1830 - Sector conducted interagency operations brief

Saturday 10 NOV 2007

1200 - Vessel salvage operations completed

2000 - NAVHAZ removed

2200 - Waterway reopened, mission complete

During the post-incident hotwash, several interagency players commented that the operation almost seemed scripted, reminiscent of previous exercises. The sector's relationship building within the maritime community had promoted a cooperative spirit and a level of trust that fast-tracked vessel recovery and NAVHAZ removal.

CAPT Patrick Trapp of Sector Hampton Roads remarked, "I can't say enough about the immediate support the sector received from the maritime incident response team, Virginia maritime community, and, most particularly, the Corps of Engineers. Within hours of the grounding, the corps' side scan sonar located the hazard and contracted its removal. We moved quickly to close the waterway, and more importantly, to reopen it as soon as it was safe for commerce."



A Coast Guard crew from Station Portsmouth unloads passengers from the *Spirit of Nantucket* after it ran aground. USCG photo by Petty Officer 2nd Class Kip Wadlow.

The Birth of Sectors, or “Physician, Heal Thyself”

Prior to reaching out to port partners, the Coast Guard needed to get its own house in order by addressing information sharing issues within its legacy groups and marine safety offices. Despite being siblings, a number of port-level commands treated their counterparts as distant cousins. The events of September 11, 2001, served to accelerate the process of restructuring our shore-based forces into multimission sector commands.

ADM James Loy, who served as USCG Commandant until 2002, coined the watchwords “preparation equals performance.” In legacy USCG groups, this meant highly trained boat crews and aviators were poised to respond. In the marine safety offices, this translated to contingency planning, exercises, and Incident Command System oil spill response. The merger to sectors provided a crosswalk of these competencies.

Externally, the sector structure reduced the size of our customers’ Rolodexes by providing what VADM James Hull described as a single “belly-button to push” for assistance. Internally, the sector organization simplified resource allocation and risk-based decision making to lessen exposure and mitigate threats. More importantly, the USCG sector became a conduit to implement a “deck plate” level of information sharing essential to Coast Guard mission execution.

Sector Hampton Roads:

Gatekeeper of the Chesapeake Bay

There are now 35 USCG sectors that serve the maritime industry and boating public. These commands are examples of a “bottom-up” focus on information sharing. Sector Hampton Roads, like so many of its counterparts, weathered years of sheet rock dust and portable office space that characterized the transition to the sector structure. This process morphed the resources of two groups and a marine safety office that served the Chesapeake Bay, served the ports of Hampton Roads and Richmond, and maintained an extensive presence in the mid-Atlantic region.

Even as the sector stood up, leadership recognized the necessity to effectively manage change. Leadership theorists have described this as “storming and forming,”² where much of an upstart’s energy is sapped meeting a mission, leaving less that can be devoted to process improvement. It is analogous to trying to change a flat tire while moving down the interstate. Search and rescue, port security, and hazardous chemical responses allow zero tolerance for failure. The sectors and their

command centers operate in a highly dynamic environment offering few opportunities for “do-overs.”

CAPT Patrick Trapp wasn’t a plank owner but assumed command as Sector Hampton Roads was still acquiring its sea legs. Fortunately his predecessor, CAPT Robert O’Brien, left a full sea bag. CAPT Trapp remarked, “A lot of good work was underway, but there was an ever-present temptation for fighting local brushfires, and being consumed in the ‘now.’ Getting in the fray may give you a sense of accomplishment, but it’s simply not a strategic approach. ADM Allen refers to this as the ‘tyranny of the present.’ Early on, the mission remained paramount, but whenever there was a respite, we shifted forces in an effort to build essential elements of planning, exercises, and networking interagency relationships.”

Experience Is Something You Gain Right After You Needed it the Most

Initially CAPT Trapp moved to ensure that the sector had sufficient resources devoted to long-term planning. He took a two-fold approach, first allocating energetic department heads and staff to the command center, response, prevention, and planning. He also used his position as captain of the port, chairman of the area maritime security committee, and his involvement with the Virginia Maritime Association to personally work the interagency issues.

He then turned the focus on the operational impact of interagency cooperation and information sharing. The efforts have already reaped benefits (see sidebars). According to CAPT Trapp, “I attribute the rapid recovery from the grounding of the *Spirit of Nantucket* and the success of Jamestown 2007 to our front-loaded approach in sharing information and stressing interpersonal relationships—putting faces with names, long before you need to call on them. Both responses were significant contrasts in execution, but the information flow and teamwork maximized safety, and minimized the disruption to the maritime public.”

About the author:

Mr. Ben Thomason is a program analyst, maritime domain awareness and information sharing, USCG Atlantic Area. Past assignments include chief of staff/chief of operations, Fifth Coast Guard District; operations officer, Air Station Houston; executive officer, Air Station Houston Borinquen, P.R.; and commanding officer, Air Station Clearwater. He has also served on the board of directors of the Maison Fortune Orphanage, Hinche, Haiti.

Endnotes:

1. “New Threats, New Challenges, New Strategy,” state of the Coast Guard address, Washington, D.C., February 13, 2007.
2. “Leading the Team Organization: How to Create an Enduring Competitive Advantage,” Dean Tjosvold and Mary M. Tjosvold, 1991.



Case Study 2: America's Anniversary Weekend



A Coast Guard maritime safety and security team provides security for the ships *Susan Constant*, *Godspeed*, and *Discovery*, replicas of the original ships that brought the first English colonists to Virginia in 1607. U.S. Coast Guard photo by Petty Officer Christopher Evanson.

Jamestown 2007 commemorated the 400th anniversary of the first permanent English settlement in North America. The president of the United States and the Queen of England were among the 63,000 visitors during the three-day celebration. James City County was responsible for public safety and for ensuring security for the president and royal family—a huge undertaking. What the municipal government needed most was a planning process and an operational structure.

Fortunately DHS mandated the use of the Incident Command System (ICS). Although ICS was developed to respond to incidents, it is now the preferred system to provide the unity of command for non-emergency management settings.

The Official Language

Because of its reputation for ICS “literacy,” Sector Hampton Roads was designated as the senior federal official and assigned key roles in all sections of the unified command. In choosing which provisions might best suit its needs, sector planning staff used the exercise format to effectively prepare and respond during Jamestown 400.

The plans incorporated provisions for awareness, prevention, preparedness, response, and recovery. The staff also arranged for members of the Training Center Yorktown Contingency Planning School and subject matter experts from previous national events to conduct onsite assessments and critiques during the three-day weekend.

During the event, the majority of the Coast Guard’s resource hours were dedicated to the maritime operations branch, which focused on the James River. The mission was to prevent and deter waterborne terrorist attacks, mitigate their effects on the public, minimize impact on maritime commerce, and establish maritime emergency response plans in event of actual attack.

One of the primary ways to the event grounds was via the Jamestown-Scotland ferry, which transported over 6,000 vehicles across the James River during the event. Performing vehicle security inspections, coordinating the historic vessel movements, and patrolling the fireworks area presented a significant resource drain to the USCG operations section, maritime operations branch, and on-the-water patrol commander.

Working Together Equals Success

More than 40 federal and commonwealth agencies and local participants comprised the unified command, including:

- Transportation Safety Administration: DHS-designated federal coordinating officer;
- Federal Bureau of Investigation: shared law enforcement databases;
- Virginia Army National Guard: weapons of mass destruction technical expertise;
- Virginia Dept. of Environmental Management: hazmat response;
- James City County: provided county employees for the unified command, preplanning activities, fire, police, pre-event planning;
- Coast Guard: senior federal official.

Additionally, when the USCG command discovered a shortfall of experienced and knowledgeable ICS staff for key positions, Coast Guard members became the “pinch hitters and relief pitchers” due to their knowledge, training, and experiences.

Jeanne Zeidler, executive director of Jamestown 2007, said, “Anniversary weekend truly exceeded our expectations. The enthusiasm and excitement of visitors was tangible. With the help of the dedicated staff, volunteers, and organizations who came together to produce this wonderful event, it was truly the once-in-a-lifetime experience we always thought it would be.”¹

Endnote:

¹ www.jamestown2007.org.



**U.S. Department
of Homeland Security**

**United States
Coast Guard**



A Coast Guard 33-foot fast response boat crew escorts the USS *Monterey*, a Navy cruiser based in Norfolk, Va., during the 2008 Parade of Ships in New York Harbor. The Coast Guard traditionally provides security to incoming vessels each year during this celebration. U.S. Coast Guard photo by PA3 Annie R. Berlin.