



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

**SECURING THE NORTHERN MARITIME BORDER
THROUGH MARITIME DOMAIN AWARENESS**

by

Jeffrey C. Westling

September 2010

Thesis Advisor:

Robert Bach

Second Reader:

Stanley Supinski

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE September 2010	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Securing the Northern Maritime Border Through Maritime Domain Awareness		5. FUNDING NUMBERS	
6. AUTHOR(S)		8. PERFORMING ORGANIZATION REPORT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.	
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) <p>Since September 11, 2001, both the United States and the Canadian governments have established plans and initiatives to improve maritime domain awareness (MDA) in their nations' ports and maritime approaches. Agencies entrusted with maritime homeland security for the United States are challenged to push detection, identification, and surveillance of maritime threats away from the U.S. shoreline.</p> <p>In the Great Lakes region, the proximity of the U.S.–Canada border complicates these efforts. A system-wide approach to homeland security on the Great Lakes is needed. Creation of a formal U.S.–Canada joint organizational entity with full-time representation from each federal agency, state, and province adjoining the Great Lakes would establish a binational MDA common operating picture while facilitating a timely, effective flow of information, intelligence, and resources.</p> <p>This research project describes the unique maritime homeland security issues confronting the Great Lakes, discusses requirements to achieve complete MDA and establish a common operating picture (COP), and reviews several models currently utilized for binational and port-centric collaboration. Finally, it recommends combining the port-centric concept of interagency operations centers required by the SAFE Port Act of 2006 with binational collaboration into a system-wide approach for a Great Lakes Maritime Operations Center.</p>			
14. SUBJECT TERMS Border Security; Maritime Domain Awareness; MDA; Common Operating Picture; COP; Nationwide Automatic Identification System; NAIS; AIS; Interagency Operation Center; Great Lakes; Maritime Security; Collaboration; Information Sharing; Surveillance; United States; Canada			15. NUMBER OF PAGES 99
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**SECURING THE NORTHERN MARITIME BORDER THROUGH MARITIME
DOMAIN AWARENESS**

Jeffrey C. Westling, P.E.
Commander, United States Coast Guard
B.S., United States Coast Guard Academy, 1991
M.A., Regent University, 2000

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2010**

Author: Jeffrey C. Westling

Approved by: Robert Bach
Thesis Advisor

Stanley Supinski
Second Reader

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Since September 11, 2001, both the United States and the Canadian governments have established plans and initiatives to improve maritime domain awareness (MDA) in their nations' ports and maritime approaches. Agencies entrusted with maritime homeland security for the United States are challenged to push detection, identification, and surveillance of maritime threats away from the U.S. shoreline.

In the Great Lakes region, the proximity of the U.S.–Canada border complicates these efforts. A system-wide approach to homeland security on the Great Lakes is needed. Creation of a formal U.S.–Canada joint organizational entity with full-time representation from each federal agency, state, and province adjoining the Great Lakes would establish a binational MDA common operating picture while facilitating a timely, effective flow of information, intelligence, and resources.

This research project describes the unique maritime homeland security issues confronting the Great Lakes, discusses requirements to achieve complete MDA and establish a common operating picture (COP), and reviews several models currently utilized for binational and port-centric collaboration. Finally, it recommends combining the port-centric concept of interagency operations centers required by the SAFE Port Act of 2006 with binational collaboration into a system-wide approach for a Great Lakes Maritime Operations Center.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM STATEMENT	1
B.	ARGUMENT.....	3
C.	RESEARCH QUESTIONS.....	4
D.	SIGNIFICANCE OF RESEARCH	4
E.	METHODOLOGY	5
II.	UNITED STATES MDA POLICY AND GREAT LAKES VULNERABILITY.....	7
A.	MDA POLICY—HSPD-13	7
B.	GREAT LAKES VULNERABILITY	9
C.	GMCOI AND THE U.S. COAST GUARD	10
D.	SECURE BORDER INITIATIVE AND ILLEGAL IMMIGRATION...12	
E.	NATIONAL BORDER PATROL STRATEGY	13
III.	COLLABORATION BETWEEN THE UNITED STATES AND CANADA IN MARITIME DOMAIN AWARENESS ON THE GREAT LAKES.....	17
A.	HISTORY OF BORDER CONCERNS	18
B.	BORDER ISSUES SINCE SEPTEMBER 11, 2001.....	19
C.	INTEGRATED CROSS-BORDER MARITIME LAW ENFORCEMENT OPERATIONS.....	20
D.	CANADA’S NATIONAL SOVEREIGNTY, SECURITY POSTURE, AND MDA	21
E.	MULTIAGENCY AND BINATIONAL PARTNERSHIPS FOR MDA ON THE GREAT LAKES SYSTEM.....	23
F.	U.S. AND CANADIAN BORDER POLICIES AFFECTING MDA ON THE GREAT LAKES	24
IV.	DEFINING MDA AND COP REQUIREMENTS.....	27
A.	COMMON OPERATING PICTURE (COP).....	31
B.	COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (C4ISR)	33
C.	NATIONWIDE AUTOMATIC IDENTIFICATION SYSTEM (NAIS) ..	36
D.	INTERAGENCY OPERATIONS CENTERS	41
E.	INTEGRATING THE REQUIREMENTS	45
V.	MDA MODELS.....	47
A.	EXAMPLE 1—DEPARTMENT OF DEFENSE—THE GOLDWATER-NICHOLS ACT OF 1986.....	47
B.	EXAMPLE 2: PROJECT SEAHAWK—CHARLESTON HARBOR OPERATIONS CENTER	50
C.	EXAMPLE 3: MARINE SECURITY OPERATION CENTRE (MSOC).....	53

D.	EXAMPLE 4: NORTH AMERICAN AEROSPACE DEFENSE COMMAND (NORAD)—US NORTHERN COMMAND (USNORTHCOM)	56
E.	EXAMPLE 5 (TECHNICAL SOLUTIONS)	59
1.	Harbor and Coastal Surveillance (HCS)—Northrop Grumman Corporation	59
2.	Project Athena—Raytheon	61
F.	CONVERGENCE OF MODELS	63
VI.	CONCLUSION AND RECOMMENDATIONS	65
A.	RECOMMENDATIONS	66
B.	GREAT LAKES MARITIME OPERATIONS CENTER ORGANIZATION	67
C.	GLMOC COMMON OPERATING PICTURE	70
D.	END REMARKS	73
	LIST OF REFERENCES	75
	INITIAL DISTRIBUTION LIST	81

LIST OF FIGURES

Figure 1.	Chart of Great Lakes Showing International Border between the United States and Canada (Source: NOAA nautical chart)	17
Figure 2.	Akwesasne Reservation on the St. Lawrence Seaway (Tribal lands are within the State of New York and the Canadian provinces of Ontario and Quebec) (Source: NOAA nautical chart)	19
Figure 3.	COP Geographic Layers for MDA (Source: USCG, 2004).....	28
Figure 4.	Nationwide Automatic Identification System (NAIS) Operational View (Source: NAIS Project Resident Office).....	41
Figure 5.	Interagency Operations Center Community Model (Source: USCG, 2010) ...	44
Figure 6.	HCS Web Client Home Page.....	61
Figure 7.	Project Athena (Source: USBP unclassified briefing slide)	62
Figure 8.	Great Lakes Maritime Operations Center Proposed Command Structure Including Primary Functional Areas Modeled after U.S. Department of Defense Unified Command or Joint Staff Structures	69

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Border Patrol Objectives (Source: National Border Patrol Strategy).....	14
Table 2.	National Border Patrol Strategy—Northern Border Strategic Focus (Source: National Border Patrol Strategy).....	15
Table 3.	Sample Sources of Information Collection to Support Maritime Domain Awareness (Source: USCG, 2004)	29
Table 4.	Nine Categories of Information Required for Maritime Domain Awareness (Source: USCG, 2004).....	32
Table 5.	Top-Level COP Requirements (Functional Areas) (Source: USCG, 2008a) ..	32
Table 6.	Nationwide Automatic Identification System (NAIS) High-Level Performance Specifications (Source: USCG, 2008b).....	39
Table 7.	Representative Port Partners by Category for IOC Membership (Source: USCG Commandant (CG-761))	43
Table 8.	Project SeaHawk Participating Agencies and Partners (Source: Beeson, 2007)	52
Table 9.	Canadian Strategic Security Activities (Source: Government of Canada, 2004)	54
Table 10.	Canadian Transport Security—Marine Security 6-Point Plan (Source: Government of Canada, 2004).....	55
Table 11.	MSOC Core Functions (Source: Government of Canada, 2005)	56
Table 12.	Interagency, Intergovernmental Organization and Nongovernmental Organization Coordination (Source: United States Joint Chiefs of Staff [USJCS], 2006.	58

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAR	After Action Reports
AIS	Automatic Identification System
AMSP	Area Maritime Security Plan
C4IT	Command, Control, Communications, Computers, Information Technology
CBP	U.S. Customs and Border Protection
CBSA	Canada Border Services Agency
CCG	Canadian Coast Guard
COP	Common Operating Picture
DHS	U.S. Department of Homeland Security
DOD	Department of Defense
FMSC	Federal Maritime Security Coordinators
GCCS	Global Command and Control Systems
GLMOC	Great Lakes Maritime Operations Center
GMCOI	Global Maritime Community of Interest
HCS	Harbor and Coastal Surveillance
IBET	International Border Enforcement Teams
ICS	Incident Command System
IGO	Intergovernmental Organization
IOC	Interagency Operations Center
MARSEC	Maritime Security
MDA	Maritime Domain Awareness
MOSIC	Maritime Operational Surveillance Information Centre
MSOC	Marine Security Operation Centre
NGO	Nongovernmental Organization
NIMS	National Incident Management System
NOAA	National Oceanic and Atmospheric Administration
NORAD	North American Aerospace Defense Command

NRP	National Response Plan
RCMP	Royal Canadian Mounted Police
SeaHawk	Charleston Harbor Operations Center
SAR	Search and Rescue
SBI	Secure Border Initiative
SBI _{net}	Secure Border Initiative Network
USBP	U.S. Border Patrol
USCG	United States Coast Guard
USG	United States Government
USN	United States Navy
USNORTHCOM	U.S. Northern Command
VTS	Vessel Traffic System
WBIED	Waterborne Improvised Explosive Device
WMD	Weapons of Mass Destruction

ACKNOWLEDGMENTS

First I owe great thanks and appreciation to my wife, Patricia, and children, Grace, Christopher, and Cassandra, for their loving support, patience, and understanding as I toiled over the completion of this thesis while simultaneously attending to competing work requirements and professional certification priorities. I would also like to thank my parents, Robert and Sandra Westling, and in-laws, Dr. James Robb and Barbara Jean Grover, for their support and encouragement in all my academic and professional-licensing endeavors.

I also wish to thank the faculty and staff of the Naval Postgraduate School's Center for Homeland Defense and Security for their dedication to and support of the students. In combination with the exceptional members of my cohort, this academic experience has been extremely memorable, highly challenging, and most enjoyable. Without question, I couldn't have completed this thesis without the steadfast assistance and guidance of Dr. Robert Bach. I am also grateful to Dr. Stan Supinski, who willingly accepted the challenge to serve as my second reader at the conclusion of my thesis preparation efforts.

Lastly, I want to thank the staff of the U.S. Coast Guard's Operations Capabilities Directorate, the Coast Guard's Acquisitions Directorate, and the staff at Northrop Grumman for providing access to various documents and discussions necessary for my analysis. This thesis is dedicated to all the Guardians of the Great Lakes and to the memory of my father.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

The United States' northern border with Canada poses several unique vulnerabilities in the maritime domain that are not experienced at the majority of U.S. ports on the east and west coasts. The minimal distances and open border between the United States and Canada provide significant opportunities for vessel-borne and other maritime threats to enter both nations. The close proximity between the two nations, including the sovereign Indian nations, along the Great Lakes and the St. Lawrence River provide opportunities and infinite access points for cross-border smuggling activity (including weapons, illegal immigrants, drugs, and money). Terrorist cells have been disrupted in Canadian and U.S. cities along the Great Lakes shoreline. The lack of adequate monitoring capability throughout the region extends to commercial and recreational vessels on the Great Lakes and rivers, resulting in a lack of maritime domain awareness (MDA) on the Great Lakes system. Limitations on the ability of armed U.S. and Canadian law enforcement agencies to pursue suspects across the international border reduce the chance that they will be caught.

The minimal distances between the United States and Canada throughout most of the Great Lakes system pose unique MDA challenges. Depending on the size, draft, and maximum speed of vessels transiting the Great Lakes and the St. Lawrence Seaway, much of the Great Lakes can be crossed in four hours or less at speeds of 30 knots. Some of the most heavily transited passages are only several hundred yards wide between United States and Canadian shorelines. Small vessels can illegally transport people, drugs, weapons, and money (including counterfeit) south into the United States or north into Canada. Given the current resources and technologies operating on the Great Lakes, it is impossible to observe or track these vessels in order to target them on a recurring basis for intercept. Partnerships among United States Department of Homeland Security (DHS) agencies, local law enforcement, and the Royal Canadian Mounted Police

(RCMP) have provided opportunities for cross-jurisdiction cooperation and sharing of resources, but the capacity for joint operations depends on the resources and mission of each agency.

Currently, DHS federal agencies are developing their agencies' common operating picture (COP) in order to improve the effectiveness of each agency's mission execution. Canada has established Marine Security Operations Centers (MSOCs) to collect, fuse, analyze, and disseminate intelligence and mission-critical information among Canadian agencies and the Integrated Border Enforcement Teams (IBET). The U.S. Homeland Security Presidential Directive 13, Maritime Security Policy (HSPD-13) directs a coordinated and collaborative intelligence effort among the departments of Homeland Security, Defense, Justice, and the Director of Central Intelligence that uses existing capabilities to integrate all available intelligence to identify and prevent maritime threats (White House, 2004). The Security and Accountability For Every Port Act (SAFE Port Act) of 2006 requires the Secretary of Homeland Security to "establish interaction operational centers for port security at all high-priority ports not later than 3 years after the date of enactment of the SAFE Port Act" (SAFE Port Act of 2006). While port-centric intelligence fusion centers and interagency operations centers meet agency specific requirements of HSPD-13 and the SAFE Port Act of 2006, the proximity of the United States and Canada, coupled with the historic peace between those nations, requires a system-wide operational view of the entire Great Lakes system. A high degree of interconnectivity between port-centric interagency operations centers is required to have a fully coordinated and collaborative planning, intelligence sharing and homeland security posture for all communities along the Great Lakes, interconnecting rivers, and the St. Lawrence Seaway.

With regard to the challenges that prevent complete maritime domain awareness (MDA) on the northern maritime border between the United States and Canada, research is very limited. The available literature can be classified as academic research, legislation, intelligence, policies or official guidelines, and government documents. The bulk of the academic literature regarding MDA consists of reports of Department of Defense educational institutions such as the U.S. Naval Postgraduate School and the U.S.

Naval War College, government documents produced by United States and Canadian agencies, and reports and papers produced in Canada. Most of this literature addresses the concepts of MDA that push United States borders as far offshore as possible while addressing how to maintain MDA in major east and west coast ports and approaches. Literature addressing MDA specific to the Great Lakes and the St. Lawrence Seaway is sparse.

Commander Robert Watts, USCG, states that “while there are many potential systems that could provide a high degree of surveillance and tracking, the actual *fusion* of this data remains problematic” (Watts, 2006). He claims that, to be effective, MDA must operate on the strategic, operational, and tactical levels of the organization while ensuring that these three levels remain linked to each other in order to maintain a common operating picture (COP) (Watts, 2006). To provide detailed and consistent MDA, the entire span of the lakes from Duluth, Minnesota, on Lake Superior to Massena, New York, on the St. Lawrence River must be viewed as a single maritime system.

Strategically, MDA must collectively address the security and protection of the six states, two Canadian provinces, and multiple Indian reservations that form the Great Lakes system shoreline. Operationally, a COP must be shared among partner agencies to allow each to exercise full jurisdictional authority while maximizing opportunities to develop effective partnerships, share limited resources, and clearly identify threats and targets of interest. Tactically, each jurisdiction must be able to operate its resources with full knowledge of potential threats and risks posed in the operating environment, to share real-time vessel threat and target information, and to coordinate among partner federal, state, local, and international homeland security and law enforcement agencies to thwart threats to the ports, waterway, and shores of both the United States and Canada.

B. ARGUMENT

Achieving full maritime domain awareness (MDA) on the United States–Canada maritime border requires an integrated multiagency, multistate, binational COP to mitigate, thwart, or neutralize terrorist and criminal threats throughout the Great Lakes system. DHS agencies need to establish a joint system that tracks and monitors all vessels

operating throughout the Great Lakes. Development of an integrated COP that presents full MDA will provide more opportunities for DHS agencies tasked with border responsibilities to share information and resources and to improve overall response to border-related threats against the United States. Interoperability between the Great Lakes Maritime Operation Center and each DHS agency major command office would allow for the sharing of the COP relative to the assigned area of responsibility. Data sharing between the United States and Canadian partners responsible for homeland security and MDA would be enhanced by interconnecting the United States Great Lake's COP and Canada's existing Maritime Security Operation Centres (MSOCs).

C. RESEARCH QUESTIONS

What elements of a COP are critical for the United States to improve MDA for the Great Lakes and the St. Lawrence Seaway? How can a COP be established to maximize the effectiveness of interagency partnerships to increase homeland security along the northern maritime border?

D. SIGNIFICANCE OF RESEARCH

Research regarding MDA on the Great Lakes expands on the existing concept of MDA and places it in the context of international borders that do not have the luxury of "pushing the border" and keeping the detection and deterrence of threats offshore. Such research will contribute to the existing body of data and analysis regarding the Great Lakes maritime domain.

This thesis will set the foundation for discussions regarding the need to develop integrated surveillance, detection, intelligence fusion, and operations capabilities on the Great Lakes that blend the operational and homeland security functions and information requirements of all United States agencies with their counterparts in Canada. The intent is to identify the MDA requirements for the Great Lakes and recommend how to integrate the key requirements and elements of existing operational pictures into a single COP that will increase the collaboration, cooperation, and effectiveness of these primary agencies tasked with securing the international border in this maritime domain.

The primary consumer of this report is intended to be the Department of Homeland Security with the specific goal of substantiating the need and justifying the investment in a solution to provide an integrated COP for the Great Lakes' DHS community. This thesis will bolster the case for increased acquisitions and operations funding to design, develop, integrate, and test the information technology backbone for a multisensor COP that provides complete MDA on the Great Lakes.

E. METHODOLOGY

The horrific events of September 11, 2001, forever changed the way the United States examines, prepares, and addresses threats to its homeland security. While the attacks utilized aircraft, significant consideration has been given to protecting U.S. citizens, ports, and infrastructure from attack within the maritime domain. The primary goal of this thesis is to increase the collective understanding of the unique challenges to homeland security along the Great Lakes maritime border between the U.S. and Canada and to propose a binational, interagency maritime operation center that focuses on the Great Lakes as a single system, rather than a series of individual ports.

Chapter II highlights key elements of U.S. maritime security policy and its application to the Great Lakes. Chapter III presents a historical perspective of Great Lakes border concerns and the need for change, since 9/11 and details some of the current collaborative initiatives occurring on the border. In Chapter IV, the specific requirements to achieve port-centric MDA and establish a regional COP are synthesized from various mission needs assessments, operational requirements documents, and DHS acquisition strategies. Chapter V assesses several individual models for interagency collaboration with the intent to apply them to the unique security challenges that exist in the Great Lakes system. Finally, this thesis will propose an alternative to address the need for binational, interagency coordination and collaboration between the United States and Canada, across state and provincial jurisdictions and among hundreds of federal, state, provincial, and local agencies responsible for elements of homeland security along the maritime international border.

THIS PAGE INTENTIONALLY LEFT BLANK

II. UNITED STATES MDA POLICY AND GREAT LAKES VULNERABILITY

“While commercial aviation remains a possible target, terrorists may turn their attention to other modes. Opportunities to do harm are as great or greater, in maritime ... transportation” (9/11 Commission, 2003). When the 9/11 Commission report was released to the public on July 22, 2004, it was evident that the members of the 9/11 Commission clearly understood the risks and vulnerabilities to our nation’s ports and waterways in the post-9/11 world.

The proximity of major United States and Canadian ports of entry throughout the Great Lakes system provides a unique opportunity for terrorists to exploit international multimodal infrastructure and transportation nodes that intersect along the rivers interconnecting the Great Lakes. Railroad, vehicle, and pedestrian bridges between the United States and Canada cross the St. Lawrence River, the Niagara River, the Detroit River, and St. Mary’s River. Many of these bridges form the primary thoroughfares for citizens and commerce of both countries to transit from the midwestern states to the New England states across Canada’s Ontario province to shorten distances of travel. The vulnerabilities of these international crossings, the internationally shared navigational channels in the rivers underneath the bridges, and the adjacent roads and railroad tracks all provide an intertwined transportation system where a failure in any single system due to terrorist events or natural disasters has the distinct reality of rendering another mode temporarily useless. Additionally, travel across open water on Lake Superior, Lake Michigan, Lake Huron, Lake St. Clair, Lake Erie, and Lake Ontario provide uncontrolled access for more than a thousand miles of international border with opportunities to access even greater distances of shoreline.

A. MDA POLICY—HSPD-13

Homeland Security Presidential Directive 13, Maritime Security Policy (HSPD-13), states that “the United States, in cooperation with our allies and friends around the world and our State, local and private sector partners, will work to ensure that lawful

private and public activities in the Maritime Domain are protected against attack and criminal and otherwise unlawful or hostile exploitation. These efforts are critical to global economic stability and growth and are vital to the interests of the United States” (White House, 2004, p. 2). HSPD-13 directs a coordinated and collaborative intelligence effort among the departments of Homeland Security, Defense, Justice, and the Director of Central Intelligence that uses existing capabilities to integrate all available intelligence to identify and prevent maritime threats (White House, 2004, p.).

The Department of Homeland Security framed MDA as consisting of accurate information, intelligence, surveillance, and reconnaissance of all vessels, cargo, and people extending well beyond our traditional maritime boundaries (United States Department of Homeland Security [USDHS], 2005, p. ii). The greatest challenge in securing the maritime domain is the vastness of expanse, the medium by which threats can move, and the “broad array of potential targets that fit the terrorists’ operational objectives of achieving mass casualties and inflicting catastrophic economic harm” (USDHS, 2005). Three overarching principles guide the maritime strategy: 1) preserve the freedom of the seas, 2) facilitate and defend commerce, and (3) facilitate the movement of desirable goods and people across our borders while screening out dangerous people and material (USDHS, 2005). To further define this strategy, the “National Plan to Achieve Maritime Domain Awareness” states that MDA consists of:

- 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, and vessels or other conveyances, and
- The effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States. (USDHS, 2005)

To eliminate any confusion among federal agencies and homeland security partners, the strategy also defines four critical objectives to guide maritime security activities:

- Prevent terrorist attacks and criminal or hostile acts;

- Protect maritime-related population centers and critical infrastructure;
- Minimize damage and expedite recovery;
- Safeguard the ocean and its resources. (USDHS, 2005)

B. GREAT LAKES VULNERABILITY

While the Great Lakes are not, by definition, oceans, they are a single freshwater lake system that shares an international border of more than 1,000 nautical miles and connects oceangoing intercontinental commerce with interstate and international commerce at many large inland ports in Canada and the United States. For this reason, the same strategies that exist for oceangoing commerce and coastal ports should apply to vessels operating on and at ports located within the Great Lakes system. The same maritime threats to the maritime domain identified by the strategy are also present throughout the Great Lakes system. For example, non-state (terrorist) threats tied to the al-Qaeda network have been arrested in Lackawanna, New York, Detroit, Michigan, and Toronto, Ontario. Transnational criminal threats involved in movement of humans, weapons, money, and drugs have been caught through joint law enforcement actions at land-based ports of entry and on the waters of the Great Lakes system by federal, state, local, and Canadian law enforcement personnel. Additionally, the Great Lakes system directly provides for the recreation and livelihood of millions of people throughout the United States and Canada.

Given the vital interests located on the Great Lakes, any terrorist or natural or man-made environmental catastrophe anywhere in the Great Lakes system has the potential to cripple commerce, or to render drinking/industrial water supplies and recreational avenues useless, even if only temporarily. Additionally, due to the close proximity of the border to both the United States and Canada—in some cases less than 100 yards—illegal immigrants can access miles of relatively unpopulated area where they can quickly cross the border between countries, unnoticed by homeland security and law enforcement personnel. The importance of the Great Lakes system and the myriad opportunities for exploitation of homeland security vulnerabilities only increase the need

for interstate and international cooperation and coordination among all states, levels of government, and with Canada to protect the people, the commerce, and the environment that depend on this precious international resource.

C. GMCOI AND THE U.S. COAST GUARD

To achieve awareness across such expansive and diverse areas, a fully cooperative and collaborative Global Maritime Community of Interest (GMCOI) is essential to meeting the strategic goals and objectives of HSPD-13. The GMCOI includes “the federal, state and local departments and agencies with responsibilities in the maritime domain” (USDHS, 2005, p. ii). Due to shared and common maritime interests and risks, GMCOI also includes public, private, and commercial stakeholders, as well as foreign governments and international stakeholders (USDHS, 2005).

The National Plan to Achieve Maritime Domain Awareness clearly identifies the objectives that constitute the MDA essential task list guiding capabilities that the United States will pursue in conjunction with the GMCOI:

- 1) Persistently monitor in the global maritime domain:
 - a. Vessels and craft;
 - b. Cargo;
 - c. Vessel crews and passengers;
 - d. All identified areas of interest.
- 2) Access and maintain data on vessels, facilities, and infrastructure.
- 3) Collect, fuse, analyze, and disseminate information to decision makers to facilitate effective understanding.
- 4) Access, develop, and maintain data on MDA-related mission performance.
(USDHS, 2005)

The strategy described in the “Maritime Sentinel: Coast Guard Strategic Plan for Combating Maritime Terrorism” leverages the Coast Guard’s military, maritime, and multimission heritage to embrace and develop a threat-based, risk-managed approach to combating terrorism in our nation’s ports and waterways (USCG, 2006b). To meet the requirements of the various strategic documents and directives regarding maritime

security, the Coast Guard is actively developing common operating pictures (COP) for all major ports. The purpose of the COPs is to provide real-time information on blue, red, and white forces (friendly, enemy, and neutral vessel/target tracklines) operating in the maritime domain.

Existing data sharing opportunities and sources that currently support the formation of the COP include classified DoD feeds, USCG Cutter and COP-capable aircraft track reports, and Vessel Traffic Service (VTS). According to Coast Guard operational requirements documents, a future data feed currently in design is the Automatic Identification System (AIS). Also, a well-developed nationwide network of surface radars, radio communications towers (high and low level HF sites), Coast Guard, Navy, and National Oceanic and Atmospheric Administration (NOAA) vessels and buoys form the basis of the vessel tracking within many of the nation's major ports and waterways, including their seaward approaches (open ocean).

The challenge for the maritime community of interest along the Great Lakes is to overcome the realities of only partial geographical coverage and vessel tracking. Currently, for instance, vessel tracking is handled through 1) aircraft overflights (Coast Guard and Coast Guard Auxiliary aircraft, U.S. Air Force, Customs and Border Patrol, Canadian Coast Guard, Royal Canadian Mounted Police, and state and local law enforcement aircraft), 2) government agency vessels (federal, state, local, and Canadian government), 3) radio direction finding (DF) capabilities resulting from mariner transmissions from marine-band radios, 4) tracking devices installed on target vessels under court or local law enforcement orders, and 5) reliance on existing Canadian shore-based radar systems that are available to the Coast Guard Search and Rescue (SAR) Missions coordinator for SAR purposes. A Coast Guard VTS operating in St. Mary's River monitors and guides ships through the congested confluence of Lakes Huron, Michigan, and Superior and the interconnecting St. Mary's River. Additionally, a VTS-like system of radars exists in the St. Lawrence Seaway but is operated under the

jurisdiction of the St. Lawrence Seaway Development Corporation, the private entity that holds many of the Captain of the Port authorities as transferred by the United States government prior to September 11, 2001.

D. SECURE BORDER INITIATIVE AND ILLEGAL IMMIGRATION

Maritime monitoring along the Great Lakes is also limited in terms of enforcement against illegal immigration. Since 9/11, attention to border enforcement has increased on both the southern and northern borders, but along the maritime routes of the north, surveillance, sensors, and increased U.S. Border Patrol presence remain inadequate. The Secure Border Initiative (SBI) is designed to improve coordination of DHS agency assets and resources; increase sharing of intelligence and tactical information; improve detection, identification, and surveillance capability; and integrate technology with resource allocation to target potential shifts of illegal activity as they become maritime threats and thus a significant concern in the nation's ability to maintain complete maritime domain awareness throughout the Great Lakes system.

DHS announced the SBI on November 6, 2006. The intent of the multiyear plan was to coordinate all DHS efforts to secure the nation's borders and facilitate the legal entry and exit of people and the flow of legitimate commerce across all U.S. borders and through all authorized ports of entry. SBI calls for the integration of technology, DHS personnel, improved infrastructure and cooperation with state, local, and international partners (USDHS, 2006). While a significant focus of SBI has been on the United States–Mexico border, U.S. Customs and Border Protection (CBP) has made a concerted effort to triple the number of U.S. Border Patrol (USBP) agents assigned to the United States–Canada border and has doubled the number of CBP inspectors at the northern border ports of entry (USDHS, 2006). Several new USBP stations, some with marine facilities, have been constructed since 2005, including locations on the St. Lawrence River and the Niagara River that have significantly improved DHS interagency coordination and tactical operations while facilitating opportunities for improving cross-border partnerships and joint operations with International Border Enforcement Team (IBET) agencies.

To increase the opportunity for threat identification, classification, and interception, CPB launched the SBInet project to provide the USBP with the technology and infrastructure necessary to achieve border control that is functionally tailored to the specific terrains and challenges posed by each USBP sector (United States Customs and Border Patrol [USCBP], n.d.). SBInet is required to provide a solution that senses a cross-border entry into the United States, identifies the entry as legal or unlawful, classifies the threat with the number of people and armament, provides a means to respond to the entry, and dispatches the appropriate law enforcement solution (USCBP, n.d.). The ultimate goal of SBInet is to provide the common operating picture for CBP and its USBP agents to facilitate the interception and arrest of targets of interest. The challenge noted by available documentation is that, as the land borders and designated ports of entry are fortified through this integration of technology, infrastructure, and personnel, it is anticipated that threats will shift illegal entry of personnel and contraband to the ports. Given the minimal distances between the United States and Canada over much of the Great Lakes system, increased vigilance, improvements in monitoring and targeting capabilities, shared operational information, and coordination of homeland security assets and resources are necessary.

E. NATIONAL BORDER PATROL STRATEGY

The National Border Patrol Strategy highlights the need for improved coordination among agencies, consistent and trustworthy detection, identification and classification of entries, and a shared common operating picture. This strategy directly supports CBP's strategic goals of: 1) preventing terrorism through detection and prevention measures, 2) strengthening the control of U.S. borders at and between designated ports of entry, and 3) protecting America and its citizens by prohibiting the introduction of illicit contraband and illegal immigrants (USCBP, n.d.). Table 1 summarizes the Border Patrol's five main objectives to meet CBP's goals.

Table 1. Border Patrol Objectives (Source: National Border Patrol Strategy)

National Border Patrol Strategy—Five Main Objectives
1. Establish substantial probability of apprehending terrorists and their weapons as they attempt to enter illegally between the ports of entry.
2. Deter illegal entries through improved enforcement.
3. Detect, apprehend, and deter smugglers of humans, drugs, and other contraband.
4. Leverage “Smart Border” technology to multiply the effect of enforcement personnel.
5. Reduce crime in border communities and consequently improve quality of life and economic vitality of targeted areas.

The northern border requires international partnerships with Canadian law enforcement and intelligence agencies in addition to coordination with other federal, state, local, and tribal organizations. Evidence of increased partnerships includes the increased joint presence of IBET agencies, joint staffing of the CBP fusion center on Grand Island, New York, the collocation of Coast Guard personnel and vessels at the Massena, New York, USBP station, and adjacent command locations of Coast Guard and USBP stations in the Thousand Islands region of the St. Lawrence River. These partnership and resource coordination initiatives are in full alignment with the northern border strategic focus of the National Border Patrol Strategy.

Table 2. National Border Patrol Strategy—Northern Border Strategic Focus
(Source: National Border Patrol Strategy)

National Border Patrol – Strategic Focus Elements
<ul style="list-style-type: none"> • Balance intelligence use, other agency liaison efforts, technology, and equipment use, and personnel.
<ul style="list-style-type: none"> • Identify threat areas and resource requirements to mitigate and defeat threats.
<ul style="list-style-type: none"> • Acquire communications and data infrastructure to support detection and response.
<ul style="list-style-type: none"> • Expand detection technologies and sensing platforms.
<ul style="list-style-type: none"> • Improve mobility and rapid response capability.

As described in this chapter, the United States has already established basic policies and guidance related to MDA improvements through its Maritime Security Policy (HSPD-13), the Coast Guard’s Maritime Sentinel Strategic Plan, Customs and Border Protection’s Secure Border Initiative, and the National Border Patrol Strategy. These policies and strategies provide a foundation for expansion of MDA concepts that require continued refinement where detection, identification, and potential interception of threats cannot occur dozens of miles offshore. A critical element to successfully address MDA concerns on the Great Lakes is the need for binational collaboration and coordination between the United States and Canada due to the proximity of the shared border to each nation’s shore. Given the mutual use and risk of the Great Lakes, the protection of the maritime domain cannot be unilateral.

THIS PAGE INTENTIONALLY LEFT BLANK

III. COLLABORATION BETWEEN THE UNITED STATES AND CANADA IN MARITIME DOMAIN AWARENESS ON THE GREAT LAKES

“The almost 4,000-mile-long border between the United States and Canada is the longest undefended border in the world. But this boundary line has been changing—from one that is open and safe to one that requires increased security and policing, especially in light of last year’s terrorist attacks and the 1999 arrest of an Algerian national in possession of high explosives” (McAleavey, 2002, p. 1). This chapter will briefly describe the history of the undefended border, border-related security issues affecting both nations, and several positive steps taken to mitigate risks and improve the security posture of the Great Lakes system.

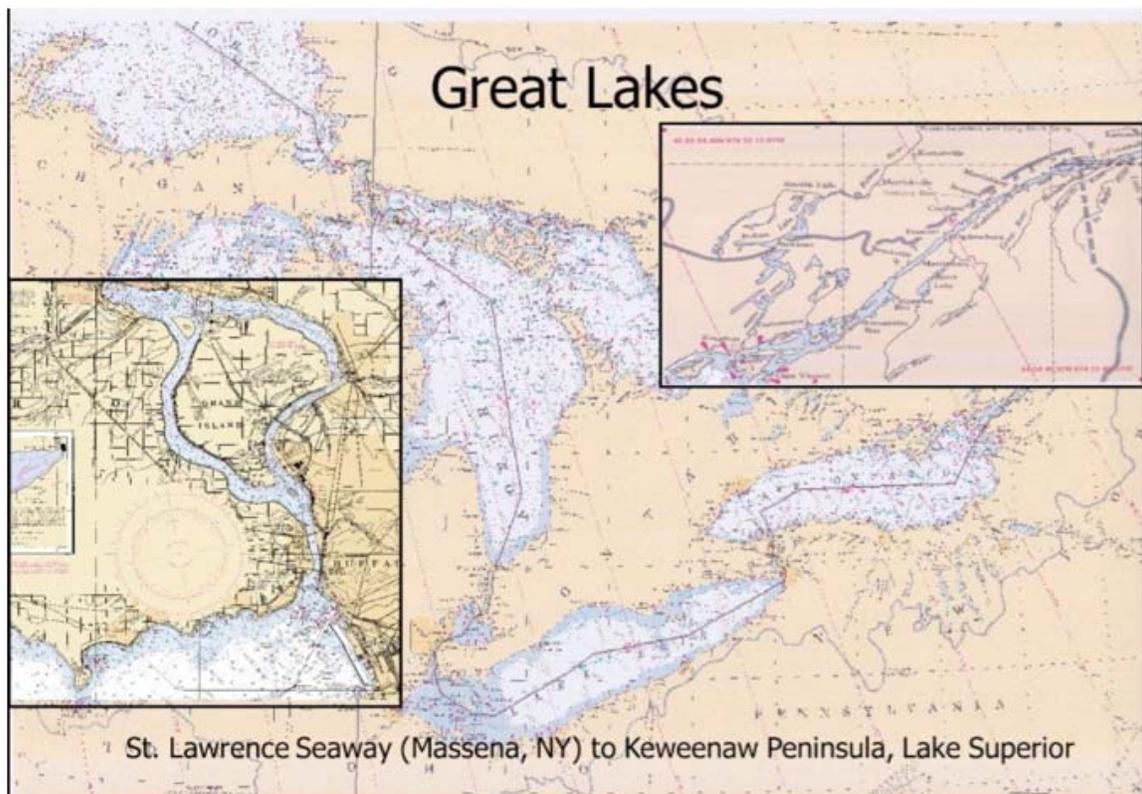


Figure 1. Chart of Great Lakes Showing International Border between the United States and Canada (Source: NOAA nautical chart)

A. HISTORY OF BORDER CONCERNS

A host of research, data, briefings, and discussions from United States and Canadian sources highlight security issues and concerns resulting from a porous United States–Canada border. While detailed data and reports exist in classified documents, the generalized challenges that exist are also summarized sufficiently in unclassified documents and research. Challenges peculiar to the Great Lakes and the St. Lawrence Seaway affect the ability to obtain complete MDA, including the close proximity of the shorelines between the United States and Canada, the sovereignty of Indian reservations, and the complications of the Rush-Bagot Agreement of 1817.

The Rush-Bagot Agreement allows only one vessel on Lake Ontario “not exceeding one hundred tons burthen and armed with one eighteen pound cannon” (Rush-Bagot Agreement of 1817). Additionally, it allows two similar vessels and armament on the upper lakes and one on Lake Champlain. This nearly two-hundred-year-old treaty requires that all other armed vessels on the Great Lakes be dismantled and that no other vessels of war be built or armed on the Great Lakes (Rush-Bagot Agreement of 1817).

Consultations between the United States and Canadian governments in March 2003 concluded that “the Coast Guard vessels to be armed are law enforcement vessels operating domestically under the Department of Homeland Security, and are not naval forces under the Department of Defense. Both governments are of the view that the Rush-Bagot Agreement was not intended to cover law enforcement vessels with the light armaments herein described, nor are their actions described herein contrary to the object and purpose of the agreement” (United States Department of State [USDOS], 2003). According to this pro memoria document, armament consists of M-60, .50 caliber machine gun, or like automatic weapons. Bruce Levy, Director, U.S. Transboundary Division conveyed to Nancy Mason, Director, Office of Canadian Affairs at the U.S. Department of State, that “although not formally falling under Rush-Bagot, we share your view that our discussions were consistent with the spirit and intent of the Agreement and, therefore, in the interests of our respective Governments” (Levy, 2003).

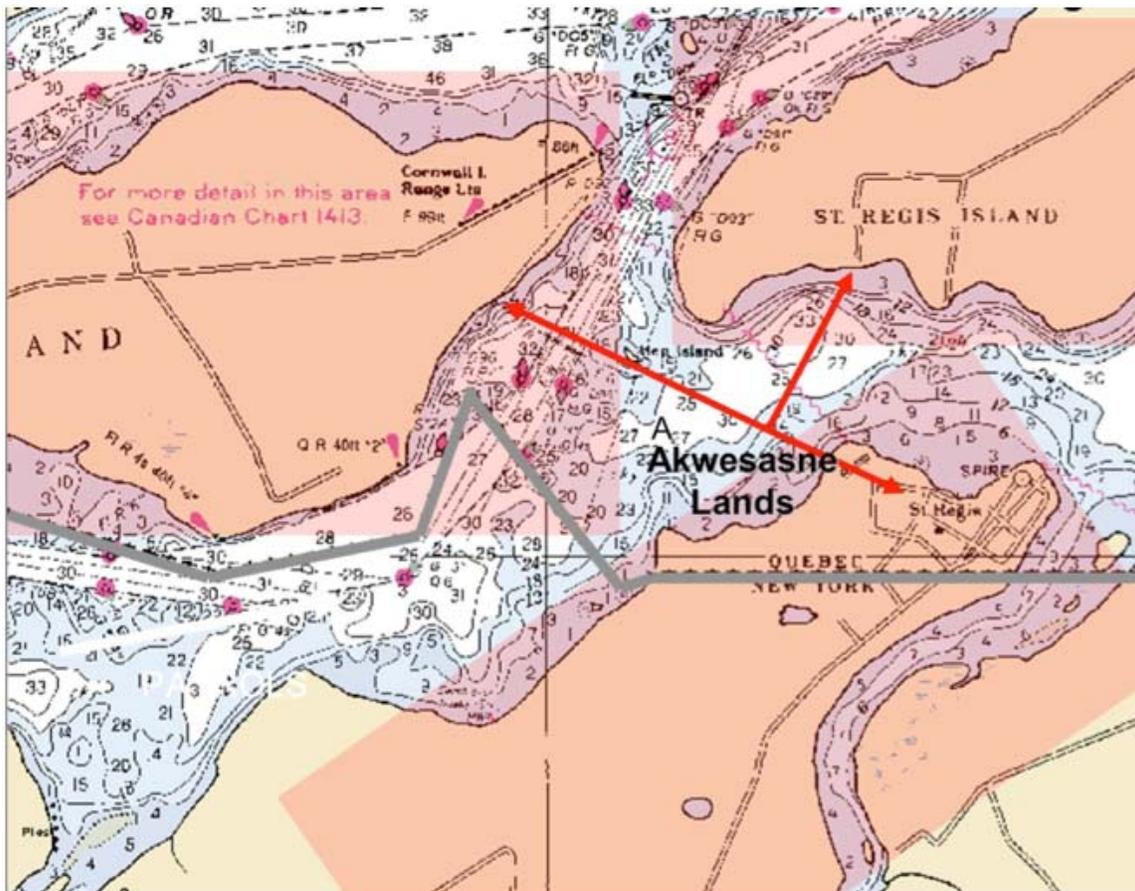


Figure 2. Akwesasne Reservation on the St. Lawrence Seaway (Tribal lands are within the State of New York and the Canadian provinces of Ontario and Quebec)
(Source: NOAA nautical chart)

B. BORDER ISSUES SINCE SEPTEMBER 11, 2001

Peter Andreas noted that “the immediate U.S. response to the terrorist attacks included a dramatic tightening of border inspections and a toughening of the policy discourse about borders and cross-border flows” (Andreas, 2003, p. 1). He correctly claims that “while there has been considerable clandestine cross-border activity along the northern U.S. border, this has largely remained under the political radar screen as American border anxieties have been directed southward.... The openness of the border, labeled ‘the world’s longest undefended border,’ has traditionally been a source of

mutual pride, but is now perceived as a source of vulnerability by the United States” (Andreas, 2003). However, Andreas’s assertion that “the Coast Guard now stops *all* boats crossing the Great Lakes and escorts gas and oil tankers” (Andreas, 2003) is not true.

In 2000, the U.S. Border Patrol was unable to accurately assess the level of illegal activity along the northern border, due in part to shortcomings in the commonly used data. The 2000 assessment concluded that the border patrol was “unable to adequately respond to illegal activity” due to the presence of only 324 border patrol agents assigned to a 4,000-mile segment of the northern border. The report also found that the “northern border sectors lacked sufficient essential equipment, or ‘force multipliers,’ such as radios, cameras, sensors, and boats that could improve enforcement capabilities” (United States Department of Justice [USDOJ], 2002, p. 2). While “the chief patrol agents unanimously agreed that border control and security had become their number one priority since September 11, 2001,” staffing, equipment needs, and intelligence capability to support enforcement operations has not yet been met and is limited at best (USDOJ, 2002).

In testimony before the U.S. House of Representatives Armed Services Committee on August 1, 2006, Captain Patrick Brennan, USCG, briefed the key issues and challenges regarding northern maritime border security. Captain Brennan, the commander of USCG Sector Detroit, claimed that the shared border with Canada poses both physical and jurisdictional challenges. He stated, “Unlike search and rescue operations during which the border is transparent, law enforcement operations involve a ‘solid’ border which we cannot ordinarily cross between ports.... This means that on a frequent basis pursuit of suspect vessels must stop at the border” (Brennan, 2006).

C. INTEGRATED CROSS-BORDER MARITIME LAW ENFORCEMENT OPERATIONS

Adequate border security requires cooperation between U.S. and Canadian agencies. One successful approach to overcoming the jurisdictional barriers is the Integrated Maritime Security Operation (IMSO), or “Shiprider,” that provides both the U.S. Coast Guard and the Royal Canadian Mounted Police (RCMP) opportunities for joint-manning of each other’s vessels for enforcement and security operations.

One cannot gain an understanding of Coast Guard operations along the northern border without considering the fact that nearly every Coast Guard mission, if it is to be executed efficiently and effectively, requires some form of cooperation with a sister Canadian agency with similar mission.... Interagency cooperation for border security involves close cooperation between all DHS components, the FBI, State, and county resources through several avenues.... Another effective avenue of cooperation occurs through the Area Maritime Security Committees. These committees, and their executive bodies, provide the Federal Maritime Security Coordinators (FMSC) with advice on identification and mitigation of threats, serve as a link between law enforcement agencies and ship and marine terminal operators to communicate threat information and change Maritime Security levels (MARSEC) to respond to threats, and assist the FMSC with maintenance of the Area Maritime Security Plan (AMSP). (Brennan, 2006)

Captain Brennan also notes that Coast Guard personnel now staff the Great Lakes–St. Lawrence Seaway Marine Security Operations Center, an interdepartmental Canadian effort designed to detect and deter threats on the maritime border (Brennan, 2006).

D. CANADA’S NATIONAL SOVEREIGNTY, SECURITY POSTURE, AND MDA

Since September 11, 2001, the effort of the United States to increase its security posture has been matched by comparable discussions and changes in Canadian homeland security policies, initiatives, and enforcement. Significant volumes of reports, research, and public discussion are available in official Canadian government documents, academic institutions, homeland security forums, the Canadian media, and citizen organization documents.

The United States and Canada have a long history of cooperation that smoothes the path in these efforts. Lieutenant Commander Bruce Grissom, U.S. Navy, notes that “one struggle that is being faced by U.S. policy-makers is how to establish partnerships with our hemispheric neighbors that increase homeland security while maintaining borders that enhance free flow of goods and services in an ever increasing global economy” (Grissom, 2004, p. 1). He highlights the defensive pact established prior to World War II between the United States and Canada, where President Roosevelt

“proclaimed that the United States would not stand idly by if Canadian soil was threatened” (Grissom, 2004). Similarly, Canada’s Prime Minister acknowledged that country’s obligations to provide support should the United States be attacked. Grissom claims that “the NORAD agreement between the United States and Canada was driven by America’s desire for security in an increasingly unsure world,” referring to the creation of the joint US/Canadian military command in 1958 to protect both nations from Soviet threats (Grissom, 2004).¹

The NORAD agreement between the United States and Canada has set a foundation for future direct military partnerships. Technologically, Canada is able to procure systems that would be interoperable with U.S. capabilities. The only hindrance to future partnerships might be the will of Canadian policy-makers to partner with the United States in an area such as missile defense. (Grissom, 2004)

Grissom then goes on to highlight Canada’s \$29 billion reduction in defense spending and a 50% cut in troops over the past decade.

Lieutenant-Commander Kearney and Lieutenant-Commander Millar, Canadian Naval Forces, claim that two major security concerns that affect Canadians are: 1) potential terrorist threats, and 2) United States unilateral action if Canadians are not observed to be doing “enough” to deny terrorists entry to Canada (Kearney & Millar, 2004, p. 63). They claim that

to meet the concerns of Canadian maritime security, and to ensure our ongoing cooperation with the US, Canada must be capable of effectively monitoring and controlling activity within our territory and the areas of the ocean over which we claim authority. This requires an ability to provide indications and warning functions, to monitor, track and analyze events occurring on, under, and over Canada’s three dimensional maritime approaches, and to share this maritime picture with the appropriate agencies of the government responsible for enforcing Canadian law. (Kearney & Millar, 2004)

¹ NORAD, the North American Aerospace Defense Command, is a binational military command focused on the air defense of North America and located in Colorado Springs, Colorado.

Most importantly, they state, “the existing coastal Naval Operations Centres will need to be expanded into Maritime Fusion Centres, and an additional facility will need to be established for the Great Lakes and St. Lawrence Seaway. These centres should be staffed utilizing a Joint Combined Interagency Approach to increase interagency cooperation and coordination” (Kearney & Millar, 2004).

E. MULTIAGENCY AND BINATIONAL PARTNERSHIPS FOR MDA ON THE GREAT LAKES SYSTEM

Official government documents produced by both United States and Canadian federal agencies highlight the successes and challenges of interagency, multiagency, and binational partnerships. A number of approaches, including the International Border Enforcement Teams (IBET), Integrated Cross-Border Maritime Law Enforcement Operations, and Marine Security Operation Centers (MSOC) are currently functioning on the Great Lakes.

IBETs are a multiagency, binational alliance among United States, Canadian, and tribal law enforcement agencies who share the mission of protecting the shared border. “Since September 11, IBETs have acquired sensor systems, night-vision devices, computers, global positioning systems, and automatic personnel and vehicle locators. But integrating advanced technology into IBET tactical operations is proving to be a challenge” (Kearney & Millar, 2004). Communications interoperability and surveillance continue to be issues requiring resolution.

In a June 2002 speech, Dr. LeBeuf of the Royal Canadian Mounted Police (RCMP) highlighted that “partnerships between Canada and the U.S. are nothing new. The two countries have long been seen as partners, creating, by force of circumstances, a stable, natural bond for a very long time” (LeBeuf, 2002, p. 2). Quoting Archer Stephens (1991), he stated that “the border has not traditionally been the source of any concerns with respect to mutual security,” noting that “criminal justice has been a domestic issue because the two countries’ legal cultures varied in their respective approaches and philosophies” (LeBeuf, 2002). Dr. LeBeuf acknowledges that “it is conceivable to say the border is permeable leaving citizens on either side vulnerable not only to disease, such as

smallpox, but also to bioterrorism and criminality” (LeBeuf, 2002). “The security of Canada and the US are inextricably linked and intervulnerable” (LeBeuf, 2001, p. 3). He also claims the border performs revenue, regulatory, and immigration functions. Supporting binational partnership between Canada and the United States, he discusses the importance of collaborative partnerships as preferable to cooperative partnerships. Clarifying his concept of collaborative partnerships, he highlights the IBETs, intelligence sharing, and joint enforcement operations, further detailing the anticipated impacts of partnerships and unanticipated outcomes.

F. U.S. AND CANADIAN BORDER POLICIES AFFECTING MDA ON THE GREAT LAKES

Limited academic research exists regarding reviews and evaluations of current policies and practices for MDA on the Great Lakes. Even less literature was located that addressed the transfer of Captain of the Port authorities and MDA surveillance to the St. Lawrence Seaway Development Corporation (SLSDC), a U.S. entity, and the St. Lawrence Seaway Management Corporation (SLSMC), a Canadian entity. A definite void exists regarding how the transfers of these authorities prior to September 11, 2001—and the lack of changes since the attacks on United States soil—enhance or detract from homeland security and MDA for both nations.

Lisa Seghetti notes that both the United States and Canada are striving to balance border security with the facilitation of legitimate cross-border travel and commerce and with the protection of civil liberties.

Compared to its southern counterpart [with Mexico], the northern border historically has been understaffed and lacked the necessary infrastructure to adequately screen individuals seeking entry into the United States. Although the southern border has seen more illegal activities over the years, there has been growing concern over the insufficient number of personnel assigned to the northern border, the increasing amount of illegal activity that occurs at the northern border, and the potential for terrorists to sneak into the United States through the northern border.” (Seghetti, 2004, p. 2)

Seghetti briefly addresses the content and impacts of the Enhanced Border Security and Visa Entry Reform Act of 2002, the Intelligence Reform and Terrorism Prevention Act of 2004, and Section 110 of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA). Additionally, she highlights the joint measures taken by the United States and Canada from 1995 to present. Specifically, she identifies the 30-point plan referred to as the “Smart Border Accord,” the joint statement of cooperation on border security and migration of December 3, 2001, the Canada–U.S. Partnership Forum (CUSP), NEXUS, IBETs, shared facilities, preinspections, and North American perimeter security (Seghetti, 2004).

On September 9, 2002, President Bush and Canadian Prime Minister Chretien held a joint press conference where they announced the launching of FAST, or Free and Secure Trade and the SMART Border initiatives. The purpose of these agreements was to simplify travel for people who routinely cross the international border, while increasing overall security through the ports of entry (White House, 2002a). Elements of the Smart Border Action Plan that affect the maritime border include biometric identifiers, permanent resident cards, ferry terminals, compatible immigration databases, international cooperation, clearance away from the border, joint facilities, customs data, in-transit container targeting at seaports, IBETs, joint enforcement coordination, integrated intelligence, counter-terrorism legislation, and joint training and exercises (White House, 2002b).

Recently, some progress has been made regarding international cooperation for cross-border law enforcement operations between the United States government and the government of Canada. On May 26, 2009, an agreement was signed between the Secretary of the U.S. Department of Homeland Security and the Canadian Minister of Public Safety to permanently establish joint-nation cross-border law enforcement operations, which are commonly referred to as “Shiprider.” The agreement prescribes specific procedures, authorities, and limitations on DHS components and Canadian law enforcement officers regarding maritime operations in shared waterways along the United States–Canada border. The purpose “is to provide the Parties additional means in shared waterways to prevent, detect, suppress, investigate, and prosecute criminal offenses or

violations of law including, but not limited to, illicit drug trade, migrant smuggling, trafficking of firearms, the smuggling of counterfeit goods and money, and terrorism” (US–Canada Framework Agreement, 2009). While each nation retains complete authority within its own territory, the framework clearly defines the authorities, training, custody of persons, vessels or things detained or seized, accountability, use of force, information sharing, and cooperation in investigation and law enforcement/homeland security proceedings.

This review of the history of both binational collaboration and current partnerships between the United States and Canada provides encouraging evidence that steps have already been taken in the right direction to address vulnerabilities in the Great Lakes region. The next step is to examine the technical requirements to achieve complete MDA and establish a COP.

IV. DEFINING MDA AND COP REQUIREMENTS

The purpose for the Coast Guard's MDA capability is to provide superior knowledge to secure the homeland and sustain effective maritime operations to federal, state and local agencies, public and private stakeholders, and foreign governments and international organizations that share common risks and interests. To date, there is no apparent action to define a single set of operational requirements for a national common operating picture that fully represents the needs of all DHS and DoD components within the maritime domain. However, the Coast Guard has assumed the lead for the development of various initiatives that will bolster the national common operating picture with a focus on allowing for the effective collection, analysis, and dissemination of key information and intelligence to regional command centers, partner agencies, and components sharing maritime domain awareness, homeland security, law enforcement, and national defense missions.

Properly established, MDA provides a series of geographic layers in which operations can be categorized and focused to increase the likelihood that threats and challenges will be detected and addressed before they become issues requiring casualty response (Figure 3). Differing levels of United States authority, capability, and activities are permitted within each layer. To be most effective, simultaneous activities must occur to collect, synthesize, analyze, and act on data and information from each geographic layer. Table 3 summarizes the geographic layers and a representative sample of the types of information, activities, or sensor data collected within each for incorporation into the COP.

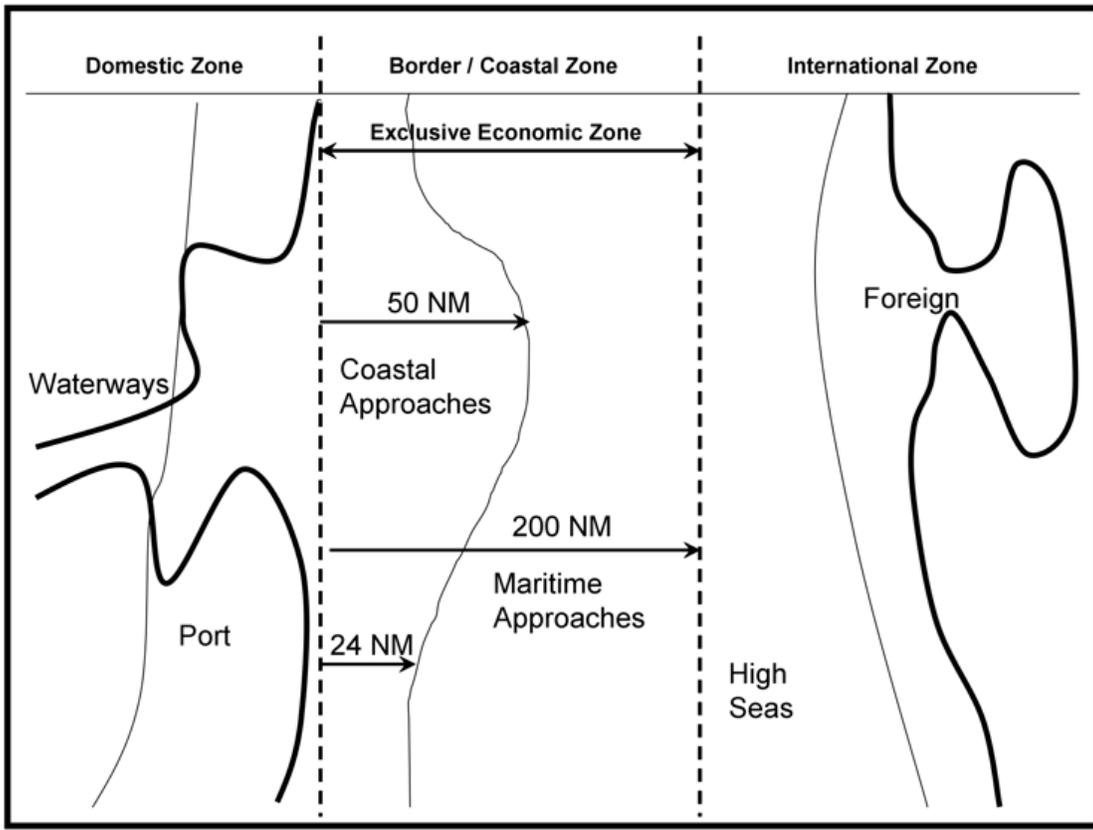


Figure 3. COP Geographic Layers for MDA (Source: USCG, 2004)

Table 3. Sample Sources of Information Collection to Support Maritime Domain Awareness (Source: USCG, 2004)

Foreign
<ul style="list-style-type: none"> • Safety of Life at Sea (SOLAS) vessels (periodic collection)
<ul style="list-style-type: none"> • AIS-equipped vessels in foreign ports (collaborative governments)
<ul style="list-style-type: none"> • Global Maritime Distress and Safety System
<ul style="list-style-type: none"> • Human Intelligence (HUMINT)
<ul style="list-style-type: none"> • Customs and Border Protection—pertinent cargo/people data
<ul style="list-style-type: none"> • Port security audits
High Seas
<ul style="list-style-type: none"> • National Vessel Movement Center—Notice of Arrival
<ul style="list-style-type: none"> • AIS: data collected from long range/over-the-horizon position reporting systems
<ul style="list-style-type: none"> • Surface and air patrols
<ul style="list-style-type: none"> • Environment / Infrastructure / Friendly Forces / Facilities: Collected from pertinent stakeholders
Maritime Approaches
<ul style="list-style-type: none"> • Wide-area surveillance in chokepoints and port approaches/high-density traffic areas (including radars and AIS)
Coastal Approaches
<ul style="list-style-type: none"> • Near real-time collection of all vessel categories near restricted channels and high-traffic areas; near shore commercial facilities; closed areas; periodic collection elsewhere
<ul style="list-style-type: none"> • Notice of Arrival information
<ul style="list-style-type: none"> • RESCUE 21—radio direction finding
<ul style="list-style-type: none"> • Coastal radar in chokepoints and port approaches
<ul style="list-style-type: none"> • Underwater detection
<ul style="list-style-type: none"> • NAIS—Blue Force Tracking and data from AIS-equipped vessels
<ul style="list-style-type: none"> • Port, facility, and vessel security plans and assessments

Ports
<ul style="list-style-type: none"> • Real-time collection of all vessel categories near critical infrastructure, restricted channels, closed areas (periodic collection elsewhere)
<ul style="list-style-type: none"> • HUMINT—collected from Port Partners (proposed Interagency Operations Center-represented agencies)
Waterways
<ul style="list-style-type: none"> • Data collected from National Marine Fisheries Service (NMFS)
<ul style="list-style-type: none"> • Existing vessel tracking systems (including Vessel Traffic Services, Inland Rivers Vessel Movement Center, St. Lawrence Seaway Management/Development Corporations)
<ul style="list-style-type: none"> • RADAR
<ul style="list-style-type: none"> • Electro-optical/Infrared sensors from private & public sources, including digital photos and video

The closer that vessels, maritime events, and activities are to the coast of the United States (see Table 3), the more definitive and comprehensive is the required information. The goal of MDA data and information collection is to detect vessels and understand their activities within 2,000 miles of the United States shoreline for the following reasons:

- Identify known and probable vessel, cargo, and people threats and challenges;
- Improve alignment of ship identification and transit information with existing 96-hour notice-of-arrival requirements;
- Provide the time necessary to analyze data and develop a response plan well in advance of vessel arrival near a United States port or shoreline;
- Capture data from vessels transiting near the United States even though they do not intend to enter a United States port. (USCG, 2004)

The balance of this chapter will summarize the critical requirements from several initiatives and concepts to improve maritime domain awareness, sharing of pertinent information, and establishment of Interagency Operations Centers. Specifically, the discussion will focus on defining the requirements for 1) a common operating picture, 2) the need for command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR), 3) the Nationwide Automatic Identification System (NAIS), and 4) Interagency Operations centers.

A. COMMON OPERATING PICTURE (COP)

In order to achieve complete MDA, all mission or functional areas of the components and agencies tasked with maritime homeland security functions must be incorporated into a common architecture that provides each with the ability to share near real-time information, synthesize inputs from multiple sources, and quickly analyze the data to effect improved decision making prior to losing the opportunity to investigate and act on threats identified. While there are many different formal definitions of a COP, the concept and intent are similar.

The COP is a display of relevant information shared by more than one command. The COP provides a shared display of friendly, enemy/suspect, and neutral tracks on a chart, with applicable geographically referenced overlays and data enhancements. The COP contains a decision-maker toolset fed by one or more distributed and exchanged track and object databases. Each user can filter and contribute to these databases according to area of responsibility and command role. The COP environment may include distributed data processing, data exchange, collaboration tools, and communications capabilities. The COP may include information relevant to the tactical and strategic levels of command. This includes, but is not limited to, geographic information systems data, assets, activities and elements, planning data, readiness data, intelligence, reconnaissance and surveillance data, imagery, and environmental data. The COP facilitates collaborative planning and assists all echelons in achieving situational awareness. (United States Coast Guard [USCG], 2004)

The COP must be all-inclusive of information and data feeds pertinent to the maritime domain. DHS and DoD shore, surface, and air assets, as well as assets of partner agencies at the state, local, and international levels of government, must be

represented in the COP to aid successful deployment of appropriate assets based on jurisdictional authorities to respond across the complete spectrum of mission sets represented in the maritime domain. It is critical that the COP accept information from a multitude of sensors and inputs owned or collected by a myriad of sources, especially those of government components or agencies with maritime responsibilities. Since the COP must serve multiple government organizations of varying authorities and responsibilities, the COP must provide all operational commanders with the information needed to make sound decisions (Table 4). Additionally, the COP must 1) inform operational commanders of strategic implications to mission success; 2) exchange strategic, operational, and tactical information with supporting interagency organizations; 3) effectively plan, execute, and evaluate multiple mission events; and 4) effectively interface with DHS, DoD, DOJ, state, local, and tribal partners to satisfy maritime homeland security, homeland defense, and law enforcement mission requirements (United States Coast Guard [USCG], 2004). To achieve these requirements, COP capabilities can be organized into nine top level functional requirements as summarized in Table 5.

Table 4. Nine Categories of Information Required for Maritime Domain Awareness (Source: USCG, 2004)

Information Categories for Maritime Domain Awareness	
Conveyances	Ships, aircraft, barges, ferries, boats
People	Crew, master, passengers, non-passengers, port workers
Facilities	Port terminals, piers, cranes, petrochemical facilities
Cargo	Containers, vehicles, bulk cargo, hazardous materials
Environment	Weather, currents, natural resources, rookeries, fish stocks
Infrastructure	Nuclear power and chemical plants, railheads, transportation nodes, bridges, locks and dams
Maritime Geospatial	Sea lanes, oceanic regions, coastal and navigable waterways
Threats/Challenges	Identified threats, illegal migration, offshore drilling
Friendly Forces	Military, federal, state, local, allied

Table 5. Top-Level COP Requirements (Functional Areas) (Source: USCG, 2008a)

Common Operating Picture Top Level Functional Requirements	
Maritime Domain Awareness	The COP provides situational awareness capability tailored to provide current and projected disposition of friendly, enemy/suspect, and neutral tracks (Blue / Red / White) and forces through near real time (NRT)/real time (RT) communications, reports, sensor data and/or other service or agency provided data sources. Enhancements to COP MDA data will be amplified with information from various databases and sources, including geospatially referenced (GIS) data.
COP Graphical User Interfaces (GUI) and Applications	COP graphical user interfaces and applications must be available to access, display and manipulate COP information.
Decision Support	The COP must contain a decision-maker toolset fed by one or more distributed and exchanged track and object databases.
Resource Management	The COP environment includes information on force readiness and status of component or agency resources.
Intelligence	The COP environment will receive finished and semi-processed intelligence information.
Force Protection (FP)	The COP environment is integrated with warning and planning tools required to minimize vulnerability of component and agency forces and the activities, organizations or infrastructure of concern to the components and partner agencies.
Information Availability, Assurance and System Administration	The host enterprise system and network shall meet and maintain minimum Information Assurance (IA) standards in accordance with established protocols that ensure information integrity and availability.
Interoperability Standards	All COP data that will be exchanged, or has the potential to be exchanged, shall be available in a format consistent with open systems architecture standards so COP data may be exchanged with mission partners within DoD, DHS, other government agencies or foreign governments.
Network Communications and Exchanges	The COP will operate in a network-centric environment that provides secure access to COP data sources and applications and supports information exchange across multiple security domains and networks.

B. COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (C4ISR)

C4ISR systems provide the foundation upon which an effective MDA COP must be built. These systems provide operators, analysts, and decision makers with essential situational awareness, data processing, and information exchange tools integral to mission performance. These systems are comprised of three components that form the

basis of the network backbone upon which the COP will operate. These components include:

- 1) *Command and Control (C2) systems*: Provide core decision-making tools to rapidly collect and process extraordinary amounts of uncorrelated data and information from multiple sources. Resulting data solutions and interconnected data networks facilitate the review and merger of disparate information to direct unified and often worldwide actions (USCG, 2009).
- 2) *Communications, Computers, and Information Technology (C4IT) elements*: Provide the network infrastructure, including the data storage, enterprise service bus, data processing, and information analysis tools, and hardware and software components, displays, and graphical user interfaces that allow personnel to input and manipulate data, collate and analyze information, and generate intelligence for strategic and tactical decision making.
- 3) *Surveillance and Reconnaissance*: Refers to data collection through the use of available sensors to locate, identify, and observe vessels, persons, and threats (USCG, 2009).

Each C4ISR element is essential to form a networked system that allows for the immediate conversion of relevant mission information into appropriate decisions and tactical mission activities. When advanced sensor data is fused with mission-planning information from multiple sources and various port partners, federal/state/local agencies, and foreign nations, then decision makers and joint stakeholders are better able to rapidly gather, analyze, and exchange secure and unambiguous information and intelligence.

The requirements for a functional C4ISR infrastructure include:

- Capability to provide operational commanders with sufficiently detailed information and intelligence to make sound and timely decisions;
- Ability to rapidly inform executive leadership of strategic implications to mission success;
- Ability to rapidly exchange strategic, operational, and tactical information and intelligence with supporting commands, components, and agencies;

- Ability to effectively plan, execute, and evaluate multiple mission events;
- Ability to effectively interface with DHS, DoD, state, local, and tribal partners to satisfy joint and individual mission requirements; and
- Ability to effectively incorporate intelligence community–derived data and analyses into C4ISR systems to support planning and operations at the component/agency level as well as joint activities. (USCG, 2009)

A critical aspect of C4ISR infrastructure is to create a system of sensors that allows for persistent surveillance:

Persistence means that when global, theater, or local reconnaissance finds something of intelligence or actionable interest, ISR systems, including processing and analytic systems, maintain constant, enduring contact with the contact. This increases the understanding about the target, which enables a faster decision cycle at all levels of command and supports the application of precision force to achieve desired effects. (Pendall, 2005, p. 41)

Persistent surveillance utilizes a variety of sensor technologies, whether manned, unmanned, remotely operated, fixed or radio frequency to integrate with a human interface that allows for the application of judgment and experience to enable decision making while mitigating risks. Continuous surveillance through a myriad of sensors within the ports and waterways, including long-range vessel tracking and identification systems such as the Nationwide Automatic Identification System, provides unprecedented opportunities to collect, collate, synthesize, and adjudicate information and intelligence in the maritime domain. To the maximum degree possible, automation of anomaly detection is critical in order to alert operation centers of potential threats or targets of interest requiring additional scrutiny.

While persistent vessel tracking capability currently exists in discrete areas where the Coast Guard maintains Vessel Tracking Services (VTS), the ability to track is primarily accomplished via radar and vessel radio reports, relying heavily on voice communications to associate vessel identity and radar images. Additional information on the vessel (e.g., cargo, course, and speed) is gathered by or verified by watchstanders where limited shore-based AIS coverage exists (USCG, 2005). In near-coastal areas,

Coast Guard and other agency or component vessels and aircraft patrols—and other means of collecting vessel location information, including self-reporting by ships—only provide “snapshot” surveillance. Continual vessel position and destination information, course and speed, vessel identification, and other information is critical to assessing potential threats posed by vessels and to protecting vessels while in transit. Vessel tracking information must be correlated with other sensors and databases to aid in anomaly detection, identify innocent vessels from targets of interest, and give decision makers accurate and timely information to allocated resources for increased surveillance and/or interception (USCG, 2005).

C. NATIONWIDE AUTOMATIC IDENTIFICATION SYSTEM (NAIS)

To gain a complete understanding of activities occurring in the maritime environment requires detailed real-time or near real-time information about vessels operating in the maritime domain, particularly vessel location and identity. The ability to detect, classify, identify, and track vessels is the foundation upon which other information can be added. By combining and correlating vessel information (e.g., activities, origins, itinerary) decision makers can assess the vessel’s intentions and activities in relation to its operating area and better determine what, if any, action should be taken (USCG, 2005).

The International Maritime Organization (IMO) established Automatic Identification System protocols for three reasons: 1) as a collision avoidance tool; 2) as a tool for vessel traffic services; and 3) as a means for coastal states to get information on vessels operating near their coasts (USCG, 2005). In 2000, the IMO “adopted a new requirement for all ships to carry an AIS transceiver capable of providing information about the ship to other ships and to coastal authorities automatically” (Watts, 2006). Effective no later than December 31, 2004, the IMO regulation “requires AIS to be fitted aboard all ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages, and all passenger ships irrespective of size.... Ships fitted with AIS shall maintain AIS in operation at all times except where international agreements, rules or standards provide

for the protection of navigational information” (Watts, 2006). This AIS standard and protocol was adopted by the Maritime Transportation Security Act (MTSA) of 2002 (46 U.S.C. 70114). NAIS will leverage the AIS technology and international communication standards as the basis for vessel tracking and the exchange of safety and security information with AIS-equipped vessels.

The international regulations require that AIS shall:

- Provide information—including the ship’s identity, type, position, course, speed, navigational status and other safety-related information—automatically to appropriately equipped shore stations, other ships and aircraft;
- Receive automatically such information from similarly fitted ships;
- Monitor and track ships; and,
- Exchange data with shore-based facilities. (Watts, 2006)

The international regulation, coupled with the AIS standard and protocol as addressed in MTSA 2002, provides the basis for the establishment of NAIS. Based on early surveys of representative users who would be directed to utilize the NAIS in their daily operations, the Coast Guard identified the following essential MDA tasks that could be partially or fully supported by NAIS:

- Monitor all vessels and other craft in the Marine Environment all the time;
- Monitor all cargo in the Marine Environment all the time;
- Monitor all identified areas of interest in the Marine Environment all the time;
- Access and maintain data on facilities and infrastructure in the Marine Environment;
- Collect, analyze, and disseminate information on the Marine Environment to decision makers to facilitate understanding. (Watts, 2006)
-

Additionally, NAIS capability will provide the following operational functions:

- Receipt and transmission of AIS information in order to detect, identify, monitor and track AIS-equipped vessels and to communicate data to and from shoreside and shipboard AIS equipment.
- Network services to enable conveyance of data between shoreside AIS equipment, processing equipment and command and control (C2) systems and interoperability with such systems.
- Data management capabilities, including data processing, recording, retrieval, warehousing and analysis.
- Interoperability and interface with a variety of C2 systems, including user interfaces for situation display, analysis and control of the system. (USCG, 2006)

Table 6. Nationwide Automatic Identification System (NAIS) High-Level Performance Specifications (Source: USCG, 2008b)

Nationwide Automatic Identification System (NAIS) Requirements
Maritime Safety
<i>Search and Rescue</i>
<ul style="list-style-type: none"> • Provide near-real-time locations for AIS-equipped vessels in distress • Provide locations of nearby AIS-equipped “Good Samaritans” capable of assisting in searching for and / or rescuing mariners in distress • Track progress of USCG and other assisting vessels, aircraft and resources actively conducting search patterns • Enable watchstanders to replay search vessel tracks to evaluate coverage efficiency and enable decision-makers to redirect assets as necessary
<i>Safety Broadcasts</i>
<ul style="list-style-type: none"> • Enable transmission of Marine Information Broadcasts (MIBs), weather and other safety-related broadcasts • Provide urgent navigation warnings, AtoN status, waterway closures, critical chart corrections and other pertinent navigation information • Allow automatic transmission of scheduled safety broadcasts to AIS-equipped vessels operating in defined geographic areas (custom or pre-defined areas)
<i>Aids to Navigation (AtoN)</i>
<ul style="list-style-type: none"> • Transmit AtoN status messages based on regional Captain of the Port discretion • Facilitate identification of hazards to navigation not marked by physical AtoN and transmit location and characteristics of those hazards to support the analysis of waterways and vessel movement • Facilitate collection of vessel voyage information to assist in traffic pattern analysis, waterways management, the placement of AtoN, and traffic separation schemes
<i>Safe Navigation</i>
<ul style="list-style-type: none"> • Extend the range of vessel-to-vessel AIS communications through use of repeater functions at AIS shore stations in areas of poor voice coverage and radar shadows
<i>AIS VHF Data Link (VDL) Management</i>
<ul style="list-style-type: none"> • Monitor and manage the VDL to ensure AIS viability during periods of high volume and / or radio interface • Shift AIS traffic to alternate frequencies in the event of emergency or natural disaster
Maritime Security
<i>Maritime Domain Awareness (MDA)</i>
<ul style="list-style-type: none"> • Provide near-real-time AIS vessel location information to unclassified and classified Command and Control (C2) and intelligence collection systems, specifically the Common Operating Picture (COP) • Provide real-time AIS data feeds to port partner components and agencies, including federal, state, and local government representatives of the Interagency Operations Centers (IOCs)
<i>Port Security</i>
<ul style="list-style-type: none"> • Provide Captains of the Port with means to notify vessels of changes to the Maritime Security Level and to monitor compliance with security zones • Enable operational commanders to identify, select and target vessels for law enforcement action, security screening inspections, boarding and other security measures • Provide near-real-time location of target vessels to effectively coordinate vessel interception and deploy boarding and inspection teams
Maritime Mobility
<i>Maritime Incident Investigation</i>
<ul style="list-style-type: none"> • Provide detailed record of a vessel’s movements and AIS message transmissions covering the time before, during and after the event • Provide detailed records of other vessels in the area that may have witnessed or contributed to incidents under investigation
<i>Navigation Mobility</i>
<ul style="list-style-type: none"> • Provide vessel tracking data to C2 and intelligence systems to monitor vessel activity • Provide additional means to exchange navigation data and other pertinent marine information

As currently designed, NAIS will provide the capability to receive vessel information from 50 nautical miles, transmit to a distance of 24 nautical miles from shore, and address the requirements contained in Table 6. This current planned capability increases the existing AIS coverage by more than 400% and fills the capabilities gap for transmit and blue-force tracking functionality. Future plans for NAIS include the extension of AIS receiver coverage to a distance of 2,000 nautical miles from the U.S. shore (see Figure 4). Technology feasibility studies are currently underway and include the use of satellite-based AIS coverage, offshore AIS relays, and commercial AIS subscriptions. However, the NAIS solution does not currently include plans to provide the necessary GUI for operators to fully utilize the functionality that is inherent in the system architecture currently under development. Providing the user access to functionality provided by NAIS, as well as other C2 systems, is the basis for creating Interagency Operations Centers.²

² Reference documents are personal inter-office communications of the NAIS Project Resident Office and Project Management Office.

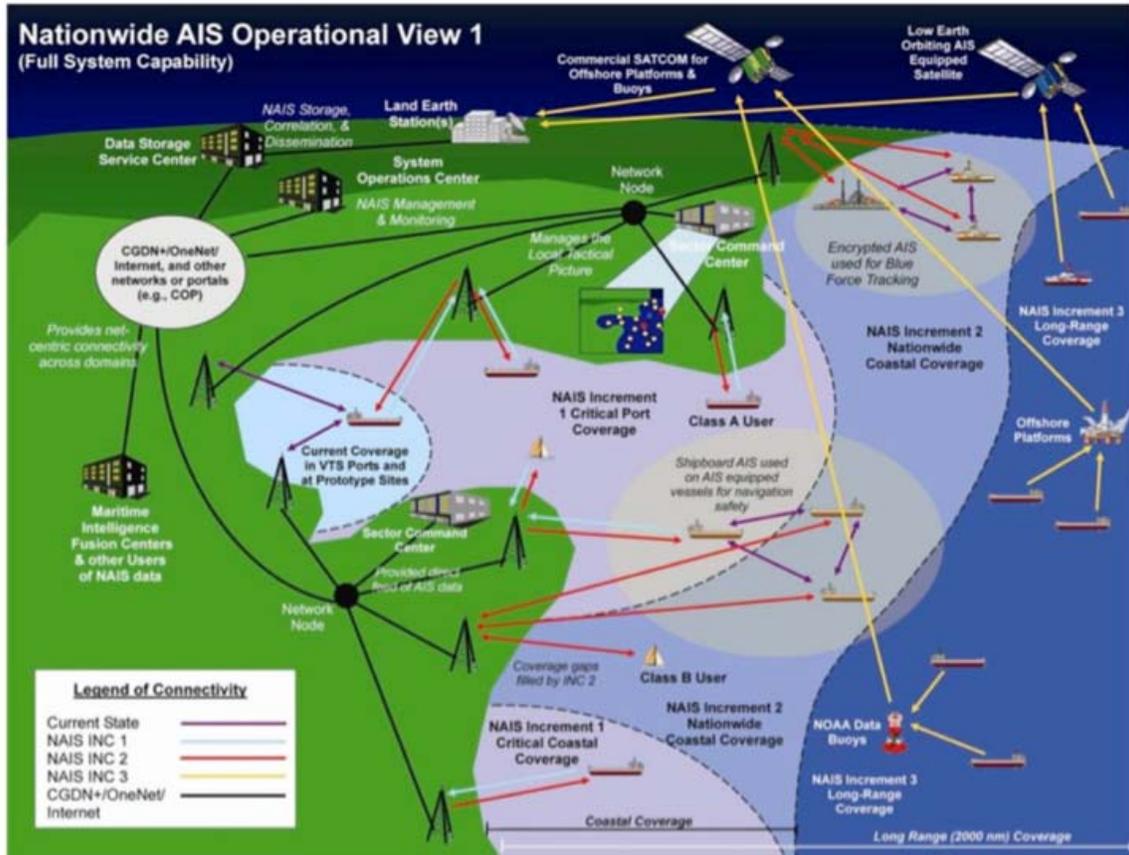


Figure 4. Nationwide Automatic Identification System (NAIS) Operational View (Source: NAIS Project Resident Office)

D. INTERAGENCY OPERATIONS CENTERS

Following the 9/11 attacks, major maritime safety and security gaps were identified by the U.S. Coast Guard, the Department of Homeland Security, and the United States Congress. The identified gaps highlighted a lack of: “(1) basic awareness of vessel activities near vulnerable port and coastal infrastructure; (2) systems linking the ever-increasing volume of vessel information in ways that help decision makers determine threat and develop the correct course of action; and (3) infrastructure for effective information sharing and joint operations with port partners” (USCG, 2010). To address these gaps, the Security and Accountability for Every Port (SAFE Port) Act of 2006 provided the following mandate:

The Secretary shall establish interagency operational centers for port security at high-priority ports not later than 3 years after the date of the enactment of the SAFE Port Act. (SAFE Port Act of 2006)

The U.S. Coast Guard assumed a key leadership role for the Department of Homeland Security and commenced the development of the Interagency Operations Centers Concept of Operations with a corresponding operational requirements document to start the major systems acquisition process.

While ongoing interagency coordination is conducted in U.S. ports, the process in most is conducted on an ad hoc basis. A field survey of Customs and Border Protection (CPB) and Coast Guard personnel conducted in 2007 by the Coast Guard's Research and Development Center identified significant obstacles to interagency coordination. Of particular note were 1) the distances between field offices, 2) poor collaboration tools, and 3) lack of collaboration procedures (USCG, 2010). Additionally, available gap analyses reiterate the need for AIS and shore-based sensors to enable persistent surveillance in the ports and approaches.

The creation of Interagency Operations Centers (IOCs) is intended to improve and facilitate the daily interaction, training, planning, exercise, and execution of maritime safety and security missions within the ports by centrally accommodating federal, state, local, private sector, and congressionally mandated committee representatives in a single operational center that is designed to enhance interagency collaboration (Table 7).

Table 7. Representative Port Partners by Category for IOC Membership (Source: USCG Commandant (CG-761))

Federal	State/Local	Private Sector
<ul style="list-style-type: none"> ▶ U.S. Coast Guard ▶ Customs and Border Protection ▶ Immigration and Customs Enforcement ▶ U.S. Navy ▶ Transportation Security Administration ▶ Federal Emergency Management Agency ▶ DHS—Other ▶ Department of Transportation ▶ Federal law enforcement ▶ Department of Justice—FBI ▶ National Oceanic and Atmospheric Administration 	<ul style="list-style-type: none"> ▶ Port Authority ▶ State law enforcement ▶ Emergency management ▶ Public health ▶ Pilots ▶ State first responders (non-LE) ▶ Local law enforcement ▶ Local first responders 	<ul style="list-style-type: none"> ▶ Private sector representatives ▶ Intermodal transportation representatives ▶ Associations that represent stakeholder groups
		Committees
		<ul style="list-style-type: none"> ▶ AMSC ▶ Area Committee ▶ Port Readiness Committee

The goal of the IOCs is to develop a proactive security posture that combines integrated vessel targeting, interagency operational planning, and operational monitoring capabilities. IOC membership efforts will be united with the following principles:

- Early identification and/or interdiction of maritime threats, violations of law and maritime transportation security incidents;
- Interagency assessment of risk regarding vessels, people or cargo moving through high-priority ports by the application and understanding of fused intelligence products, federal, state and local security concerns, and local crime trends;
- Improved awareness of maritime activity within high-priority ports or other vulnerable areas shared with all IOC members;
- Positive control of high-risk vessels, people or cargo; and
- Maximum operational transparency and coordination among IOC members. (USCG, 2010)

These principles can be achieved by integrating intelligence, jointly identifying and mitigating risks, and coordinating responses.

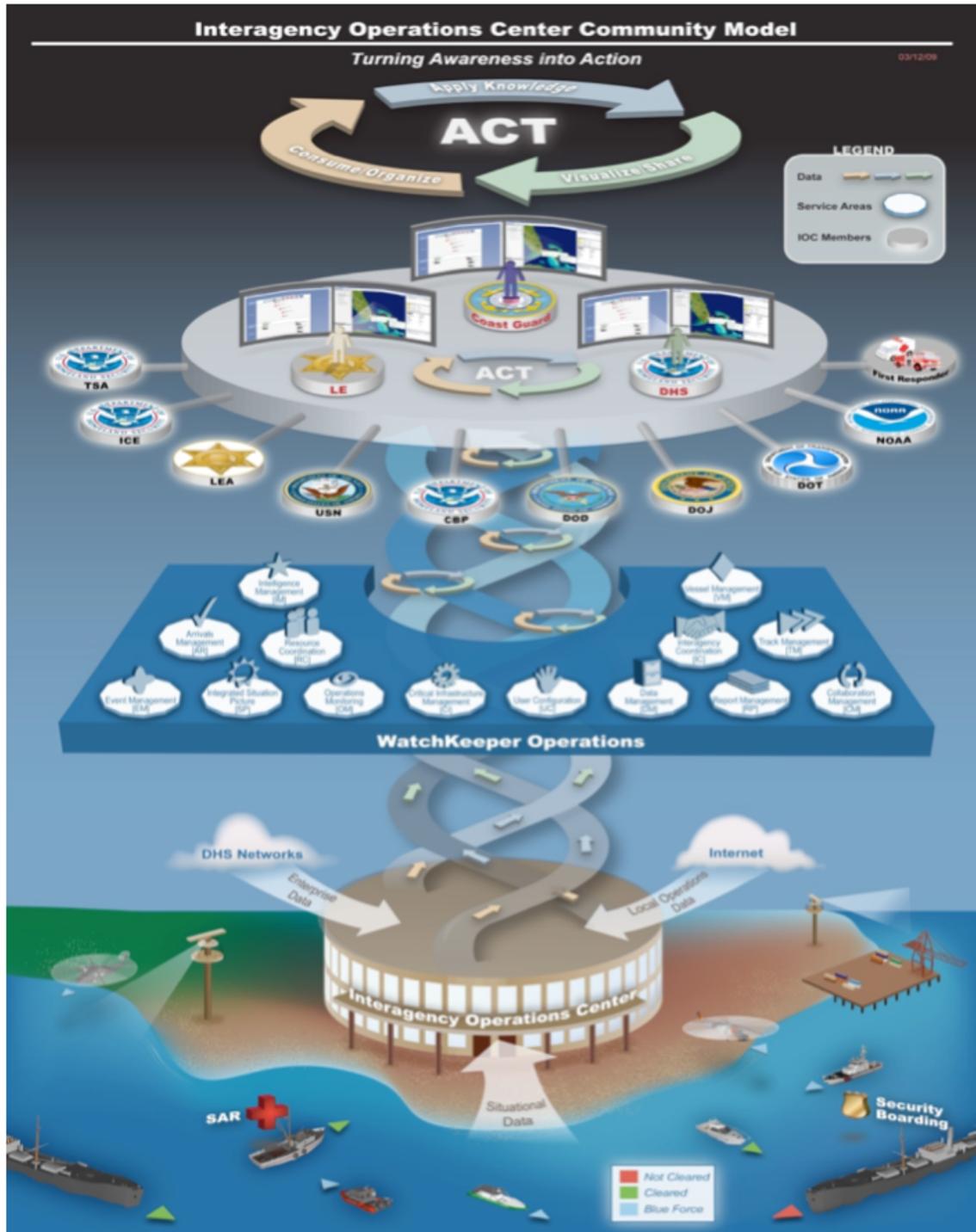


Figure 5. Interagency Operations Center Community Model (Source: USCG, 2010)

E. INTEGRATING THE REQUIREMENTS

As noted, MDA is a concept that requires a complete comprehension of all vessels, people, and cargo transiting in or near U.S. waters with the goal of understanding vessel activity to a distance of 2,000 nautical miles from the U.S. shore. To effectively accomplish MDA, a myriad of sensors must be leveraged to reach a state of persistent surveillance of all vessels, people, and cargo contained in the maritime environment. While various HF radio-based, visual, and electronic methods of surveillance and communication exist, fully instituting the internationally recognized AIS protocols and technologies through the Nationwide Automatic Identification System (NAIS) is critical to the long-range tracking of vessels and allowing for two-way ship-to-shore and vessel-to-vessel communications. Additionally, the encryption capabilities that will be inherent in the “blue force tracking” functions of NAIS will equip the port partner representatives of the Interagency Operations Centers to better coordinate intelligence collection, targeting, and response activities while minimizing premature announcement of interception plans to unsuspecting targets. The Congressional mandate to establish IOCs as directed in the SAFE Port Act of 2006 is critical to a successful acquisition strategy as detailed specifications and appropriation justification documents are prepared for future funding in the federal budget process. While port-specific operating procedures must be developed based on each port’s partner matrix, unique threats, asset and resources availability, and geography and climate considerations, the concept of establishing joint protocols, tools, and processes to maximize interagency collaboration with the private sector and congressionally mandated maritime/environmental committees is critical to long-term mission success.

Currently, separate and distinct planning and development efforts for the COP, C4ISR, NAIS, and IOCs are occurring independently and somewhat isolated from each other. While each initiative is a step in the right direction to meet the intent expressed in HSPD-13 and the SAFE Port Act of 2006, the greatest value to improving the homeland security posture across the Great Lakes northern border is to completely integrate these projects with others that may be under development by other DHS agencies or state or local governments and with the capabilities available from the Canadian government.

Technological solutions should have sufficient open architecture to allow for total integration of C4ISR and various sensor applications with NAIS and existing MDA databases that will maximize the decision-making and coordination activities at the interagency operations centers.

V. MDA MODELS

Several multi-dimensional operational models have been developed that allow for collaborative command functions across multiple agencies and permit the integration of multiple sensors into a command and control suite, thereby facilitating fusion of data and information to improve intelligence collection and decision making. While much of the available material is proprietary, sensitive, or classified, the following discussion outlines the key characteristics of several models for multiagency maritime security and safety operations suites that could be applied to meet the requirements discussed in Chapter IV.

A. **EXAMPLE 1—DEPARTMENT OF DEFENSE—THE GOLDWATER-NICHOLS ACT OF 1986**

For most of the history of the United States, the armed forces were unique and autonomous as they trained, prepared for, and carried out the president's direction for national security and defense. Each branch of the armed services set its own policy, established operational plans, and acquired war-fighting capabilities and equipment based on the needs and mission roles ascribed to its branch of service. James Locher III noted that "the Army and Navy were not able to solve their differences during World War II. Afterward, Congress settled the dispute in terms broadly favorable to the Navy's concepts—ones that preserved Navy and Marine Corps independence more than they met the requirements of modern warfare. Despite reported operational setbacks over the next forty years, subsequent reorganization efforts offered only slight improvements" (Locher, 2001). As addressed by Arizona Senator Goldwater and Alabama Representative Nichols, the Goldwater-Nichols Act of 1986 set the stage for significant changes to the defense command and control structure to improve collaboration among the services. The legislation specifically addressed multiple issues, but it achieved four primary results: it 1) improved military advice to the president, National Security Council, and Secretary of Defense through the Joint Chiefs of Staff; 2) assigned clear responsibilities for unified and mission-specific combatant commands; 3) increased attention on force-wide, inter-

service strategic and contingency planning to ensure more efficient use of defense resources; and 4) established a firm expectation for joint operations and interoperability among the service components (Goldwater-Nichols Act of 1986).

A key element of command and control was resolved by Goldwater-Nichols through the creation of an unquestionable line of authority and the formation of a governing body that consisted of the key stakeholders for national defense. The legislation bestowed clear and distinct authorities on the chairman of the Joint Chiefs of Staff, elevating this position to serve as the key advisor to the president on all military issues, concerns, and strategic recommendations. Each Department of Defense service was assigned a peer role in the Joint Chiefs of Staff. As originally required by the National Security Act of 1947, the Goldwater-Nichols Act reiterated the function of the Joint Chiefs of Staff to provide 1) unified strategic direction to combatant forces, 2) operation under unified command, and 3) integration into an efficient team of land, naval, and air forces (Goldwater-Nichols Act of 1986). Collectively, the Joint Chiefs of Staff, with advice from the commandant of the Coast Guard when appropriate, provide a force-wide perspective to the defense and security of United States interests, addressing all domains of concern (maritime, land, air, space, and cyberspace).

Acting on the advice of the Joint Chiefs of Staff, the president creates combatant commands responsible to conduct military missions in the assigned theater of operations. Unified combatant commands are composed of forces from two or more military services; they have most recently been thoroughly exercised through Northern Command, Central Command, Southern Command, European Command, and African Command. The establishment of unified commands recognizes the distinct capabilities, expertise, and training offered by each service component, and it serves to build a joint operational force that synergizes the capabilities across all domains to neutralize or dominate all threats. The significance of the unified combatant commands is that all authority across all force components is placed in one individual with a staff made up of all services to advise, plan, and execute assigned missions.

A major focus of the Joint Chiefs of Staff and unified combatant commands is joint strategic and contingency planning. The integrated use of capabilities, personnel, and resources is stressed to capitalize on the skills, expertise, and equipment that each service maintains in its inventory. Leveraging the strengths of each component increases the probability of mission success while strengthening the collaboration and trust among those charged with mission execution. Additionally, joint planning establishes a framework for the assignment of each service's assets to contingency plans that facilitate joint-service training exercises, improving confidence and cooperation prior to operational deployment.

The common theme throughout the Goldwater-Nichols Act is mutuality and interoperability among the armed forces. To achieve the fullness of this mandate, the Department of Defense established consistent acquisitions policies and procedures across the department, rather than leaving defense systems acquisitions solely at the discretion of the service chief. Current DOD policy requires that "capability needs and acquisition management systems shall use Joint Concepts, integrated architectures, and an analysis of doctrine, organization, training, material, leadership and education, personnel and facilities in an integrated, collaborative process to define needed capabilities to guide the development of affordable systems" (United States Department of Defense [USDOD], 2008). The Joint Requirements Oversight Council (JROC) oversees this guidance by ensuring that all components' requirements are fully defined and integrated to ensure a complete, interoperable defense system. Additionally, section 1251 of the National Defense Authorization Act of 2008 amended Title 10 U.S.C. § 2350a(e) to require an analysis of potential opportunities for international cooperation for all Acquisition Category I programs before the first milestone decision point.³

³ Acquisition Category I (ACAT I / ID) programs are Major Defense Acquisition Programs (MDAPs) estimated by the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) to require eventual expenditure for research, development, test, and evaluation of more than \$365 million (Fiscal Year 2000 constant dollars) or procurement of more than \$2.19 billion (Fiscal Year 2000 constant dollars). Defense Acquisition University Glossary, 13th ed., November 2009.

In summary, the Goldwater-Nichols Act of 1986 established very clear responsibilities and authorities of the chairman of the Joint Chiefs of Staff to ensure that a joint recommendation is provided to the president or delegated defense decision maker. Each chief of staff is directly responsible to ensure that the functional needs, capabilities, and resource requirements of all services are represented to ensure mutuality and interoperability in all operational domains. To properly prepare and equip the military forces, unified commands support the Joint Chiefs of Staff by ensuring that all strategic and contingency plans address the full spectrum of requirements for military operations with the collective assets and resources available to confront any threat or execute any mission. These joint plans form the basis for developing joint requirements for military acquisitions that focus on capabilities to meet all operational needs with complete interoperability between all armed forces across all domains.

B. EXAMPLE 2: PROJECT SEAHAWK—CHARLESTON HARBOR OPERATIONS CENTER

Since its inception in 2003, Project SeaHawk has served as a model of multijurisdictional interagency collaboration between federal, state, and local port partners; it was cited as an example of the IOC directive mandated in the SAFE Port Act of 2006 (SAFE Port Act of 2006). Located in Charleston, South Carolina, the Charleston Harbor Operations Center—or SeaHawk—provides a comprehensive port security solution that leverages the unique resources and information of all participating agencies into a single unified command structure to provide a holistic view of the port of Charleston.

When Congress authorized the establishment of the SeaHawk task force in the Fiscal Year 2003 Omnibus Appropriations Bill, it reiterated previous expectations for a fundamental mutuality and interoperability among operational forces to enable the flow of information and intelligence, promote interagency cooperation, and facilitate a systems approach to acquiring security and defense capabilities and to preparing operational doctrine (Beeson, 2007). As noted by the Project Seahawk task force, these expectations (of unity of effort among federal, state, and local agencies charged with various security

mandates in a single port) aligned with the previous expectations of unity of command, mutuality, and interoperability established for the Department of Defense components under the Goldwater-Nichols Act of 1986 (USDOJ, n.d.). Thus, a unified command structure, interoperability among assets and equipment, interagency collaboration, shared utilization of limited resources, and compilation of information into corroborated intelligence were foundational in the SeaHawk construct.

Project SeaHawk fully integrates the staff, financial resources, and assets into a consolidated, collaborative, unified command structure that provides round-the-clock safety and security to the port of Charleston. More than 40 distinct entities form the unified command, each bringing unique expertise, equipment, information, and intelligence to bear (Table 8). The task force director is assigned by the U.S. Department of Justice, which established a unified command structure utilizing the principles and guidance of the universally recognized Incident Command System (ICS). Each functional area is staffed by representatives of the member agencies to ensure consistency in plans, exercises, emergency response, and law enforcement activities throughout the port. The cross-pollination of the various federal, state, and local agencies has closed significant jurisdictional gaps by providing a full-spectrum situational-awareness approach that facilitates joint operations and coordination of resources to address prevention and response mission activities. The collaborative environment of the unified command structure increased efficiencies in the fusion of information to form actionable intelligence, resulting in key decision makers from the responsible agencies being able to target and mitigate risks, or to intercept and disrupt threats throughout the port.

Table 8. Project SeaHawk Participating Agencies and Partners (Source: Beeson, 2007)

Project SeaHawk Participating Agencies and Partners		
Department of Justice	State of South Carolina	Local
US Attorney's Office	SC State Law Enforcement Division	Charleston Sheriff's Office
FBI Joint Terrorism Task Force	State Fusion Center	Charleston Area Marine Law Enforcement Unit
	SC State Ports Authority Police Dept	City of North Charleston Police Dept
Department of Homeland Security	SC Dept of Health and Environmental control	City of Charleston Police Dept
Customs and Border Protection		Town of Mt Pleasant Police Dept
US Coast Guard		Charleston County Emergency Preparedness
Immigration and Customs Enforcement		
Department of Defense		
Defense Criminal Investigative Service		
US Navy		
US Air Force		
Federal Assisting Agencies	State Assisting Agencies	Local Assisting Agencies
Office of Naval Intelligence	South Carolina Air National Guard	Beaufort County Sheriff's Department
Office of Special Investigations	South Carolina State Transport Police	Port Royal Police Department
US Secret Service		Georgetown County Sheriff's Office
Internal Revenue Service		City of Georgetown Police Department
Department of State		
Diplomatic Security Service		
Transportation Security Agency		Civilian / Private Participants
Rail and Cargo Security		Lloyd's of London (LMIU)
Technology Assessment and Integration		SCRA
Office of National Risk Assessment		Various Defense Contractors
DHS Domestic Nuclear Detection Office		Charleston Branch Pilots Association
DHS Homeland Security Advance Research Projects		Maritime Association for the Port of Charleston
Office of Domestic Preparedness		
Oak Ridge National Laboratory		
Federal Law Enforcement Training Center		

Utilizing various command, control, communications, computers, and information technology (C4IT) applications, the participating agencies are able to combine various data streams into a single port-centric common operating picture providing complete situational awareness across jurisdictional boundaries. Data and information from various sources combine to form a joint information portal containing law enforcement, intelligence, and proprietary information to increase the visibility of potential threats or targets requiring further screening, investigation, and possibly interrogation. Integrated with Northrop Grumman's Hawkeye sensor array, all available data is combined in a manner that allows watchstanders to conduct surveillance activities through a multitude of sensors, including radar, video, infrared, and AIS.⁴ SeaHawk's culture, C4IT systems,

⁴ Interview of April 15, 2010, with Mr. Tom Fagre, Northrop Grumman Corporation, lead system engineer for the Hawkeye system.

and unified command structure equip decision makers to efficiently and promptly assign resources that meet the requirements of any threat, concern, mission, or exercise that might occur in the port of Charleston.

C. EXAMPLE 3: MARINE SECURITY OPERATION CENTRE (MSOC)

In June 2002, the Canadian Department of Defence initiated the Maritime Operational Surveillance Information Centres (MOSIC) project to expand the capabilities and functions of existing Canadian Navy facilities to improve the navy's intelligence collection, management, and dissemination abilities. The project focused on developing an integrated information system that would transform the navy's approach to "collecting, managing, storing, displaying and sharing maritime intelligence surveillance and reconnaissance information and data" (Government of Canada, 2005).

Building on the MOSIC concept, an MSOC project scope statement noted that the "Government of Canada's inter-agency and interdepartmental marine intelligence, surveillance and reconnaissance capability is based on business processes, information technology infrastructure and personnel resources developed to meet specific individual agency or departmental mandates. International and domestic events have highlighted the need for more inter-agency and interdepartmental collaboration and interoperability and thus are directing changes to the way we develop marine situational awareness in general; and to the way we plan and carry out responsibilities to marine security threats in particular" (Government of Canada, 2005). To address this area of concern, the Canadian government established Marine Security Operation Centres (MSOCs) to "enable agencies and departments to work collaboratively to prepare and distribute consistent, timely and trustworthy inter-agency and interdepartmental marine intelligence, information and data to national, provincial, local and international agencies. These agencies will integrate the marine intelligence, information and data into the total situational awareness picture that will be used by decision-makers to resolve marine security threats" (Government of Canada, 2005). As recently as 2005, official Canadian project documentation highlighted that "the process of integrating or fusing intelligence, surveillance and reconnaissance information, data and products to generate situational awareness in the maritime realm in

near real time is non-existent to a large extent due to technical and/or format incompatibility, personnel and procedural impediments, policy constraints and lack of fusion tools” (Government of Canada, 2005). Expanding on the two existing Department of National Defence Maritime Intelligence and Data Fusion Centres located in Halifax, Nova Scotia, and Esquimalt, British Columbia, the Canadian government recognized the importance of establishing a coherent, cohesive, and robust maritime security posture that extended beyond its military forces.

To meet the mandate of Canada’s national security policy in April 2004 (Government of Canada, 2004), various agencies of the government, including the Department of National Defence, had to reevaluate their existing intelligence collection, surveillance, integration, and dissemination policies. Addressing several key strategic areas (Table 9), a six-point plan called for improving transportation security, specifically marine security (Table 10). Significantly, national security policy specifically stated that staffing of each Marine Security Operation Centre (MSOC), would include personnel from Canada Border Services Agency (CBSA), Canadian Coast Guard (CCG), Department of National Defence, Royal Canadian Mounted Police (RCMP), and Transport Canada (Government of Canada, 2004).

Table 9. Canadian Strategic Security Activities (Source: Government of Canada, 2004)

Canadian Strategic Security Needs
Intelligence
Emergency Planning and Management
Public Health Emergencies
Transportation Security
Border Security
International Security

Table 10. Canadian Transport Security—Marine Security 6-Point Plan (Source: Government of Canada, 2004)

Transport Security: Marine Security 6-Point Plan
1. Clarify responsibilities and strengthen co-ordination of marine security efforts
2. Establish networked marine security operations centres
3. Increase the Canadian Forces, RCMP, and Canadian Coast Guard on-water presence and Department of Fisheries and Oceans aerial surveillance
4. Enhance secure fleet communications
5. Pursue greater marine security co-operation with the United States
6. Strengthen the security of marine facilities

Each MSOC is to provide maritime situational awareness along Canada’s coasts and detect, assess, and respond to marine security threats that could adversely impact Canada’s safety, security, environment, or economy (Table 11). Threats include emerging terrorist activity, over-fishing, pollution, and foreign transnational organized crime (e.g., drug trafficking, piracy, human smuggling). The goal is to provide a physical and organizational structure that facilitates marine situational awareness by transforming and fusing marine intelligence and operations information and data collected by partner agencies and departments into a common operational picture or single source of complete situational awareness.

Headed by Canadian Forces Maritime Command, the centres will include staff from CBSA, Transport Canada, the RCMP, and the Canadian Coast Guard. Reflecting the approach the Canadian Forces and Canadian Coast Guard take to carry out search and rescue operations, these Marine Security Operations Centres will have the authority and capacity, through interagency staffing, to bring to bear all civilian and military resources necessary to detect, assess, and respond to a marine security threat. Marine Security Operations Centres will be networked with the Coast Guard’s vessel traffic and communications systems, and with the new Government Operations Centre in Ottawa. (Government of Canada, 2004)

As the MSOCs develop, “inputs into the centres would include everything from surveillance assets (aircraft, ships, terrestrial radar and space-based systems) to electronic vessel locator feeds, at sea weather reports and internet provided marine vessel information services” (Government of Canada, 2005).

Table 11. MSOC Core Functions (Source: Government of Canada, 2005)

Marine Security Operation Centre Core Functions
1. Manage collection of all marine information and intelligence, surveillance, and reconnaissance data
2. Analyze marine information and intelligence, surveillance, and reconnaissance data
3. Archive marine information and intelligence, surveillance, and reconnaissance data
4. Generate marine information and intelligence, surveillance, and reconnaissance products including the recognized marine picture
5. Exchange marine intelligence, information, and data with appropriate agencies and senior decision makers
6. Provide marine intelligence, information, and data inputs to the Government of Canada Agency and Departmental Command Structures
7. Bring to bear all civilian and military resources necessary to respond to a marine security threat within the framework of the national emergency response structure

D. EXAMPLE 4: NORTH AMERICAN AEROSPACE DEFENSE COMMAND (NORAD)—US NORTHERN COMMAND (USNORTHCOM)

Established by formal agreement between Canada and the United States in 1958, NORAD is a binational command that centralizes operational control of air defense for the North American continent. The 1996 agreement renewal redefined NORAD’s missions to include aerospace warning and control for North America with a mechanism for aerospace defense cooperation and provisions for binational management of operations and decision-making. Aerospace warning includes monitoring man-made objects in space and the detection, validation, and warning of attack against North America by aircraft, missiles, or space vehicles. Additionally, NORAD was given

direction to assist civil authorities of both nations to detect and monitor aircraft suspected

of illegal drug trafficking (North American Aerospace Defense Command [NORAD], n.d.).

In April 2006, the agreement was further amended to address monitoring and response to threats from “non-state actors or terrorist groups that might choose to challenge North American security, the symmetry and asymmetry of the weapons and methods they could employ, and the transnational grid and global nature of these threats” (Agreement between the Government of the United States of America and the Government of Canada [NORAD agreement], 2006). The missions of NORAD were updated to provide 1) aerospace warning, 2) aerospace control, and 3) maritime warning for North America. Aerospace warning was updated to reflect the needs for processing, assessing, and disseminating intelligence and information for threats in the aerospace domain. Aerospace control provides binational authority to provide surveillance and positive operational control of U.S. and Canadian air space when the need arises. Lastly, the recent addition of maritime warning directs NORAD to process, assess, and disseminate intelligence and information for maritime areas and internal waterways, including maritime approaches, of the United States and Canada. Utilizing mutual support agreements with other commands and agencies, NORAD will warn responsible agencies of maritime threats or attacks enabling the identification, validation, and response by national commands and agencies responsible for maritime defense and security (NORAD agreement, 2006). NORAD’s Vision 2020 acknowledges this mandate by establishing the goal to “provide timely, accurate maritime warning of threats to, and attacks against North America” with the intent to establish and nurture effective partnerships with appropriate organizations and agencies to help “ensure the necessary awareness of the maritime domain” (NORAD agreement, 2006).

NORAD and USNORTHCOM utilize the model of mutuality and unity of command framed by the Goldwater-Nichols Act of 1986. The unified command structure staffs each directorate with members of all five U.S. armed services in addition to Canadian military personnel as appropriate. Joint Publication 3-08 sets a doctrinal basis for interagency coordination, intergovernmental organization and multinational operations (Table 12). Effective interagency, intergovernmental organization (IGO), and

nongovernmental organization (NGO) coordination cannot rely on the traditional command and control philosophy utilized for military operations. Conflicting goals, authorities, policies, procedures, and decision-making techniques may challenge collaborative efforts. Decision-making and planning processes for non-DOD agencies, IGOs, and NGOs are not always as detailed or rigid as those inherent in military organizations. To achieve a unity of effort, it is critical that strategic goals are clearly stated with detailed specific objectives and mutually accepted roles and rules for interaction to establish trust and understanding among agencies and organizations.

Table 12. Interagency, Intergovernmental Organization and Nongovernmental Organization Coordination (Source: United States Joint Chiefs of Staff [USJCS], 2006.

Systematic Approach to Building and Maintaining Interagency, Intergovernmental and Nongovernmental Organization Coordination
1) Forge a collective definition of the problem in clear and unambiguous terms
2) Understand the overall US Government (USG) strategic goal in addition to the objectives, end state, and transition criteria for each involved organization or agency.
3) Understand the differences between US national objectives, end state and transition criteria and those of intergovernmental organizations (IGO) and nongovernmental organizations (NGO).
4) Establish a common frame of reference.
5) Capitalize on experience.
6) Establish courses of action or options.
7) Establish responsibility.
8) Plan for the transition of key responsibilities, capabilities and functions.
9) Direct all means toward unity of effort.

To facilitate coordination among agencies, IGOs, NGOs, and the private sector, NORAD-USNORTHCOM established a Directorate of Interagency Coordination. This directorate provides interagency context to decision-making processes, anticipates requests for assistance through the National Response Plan (NRP) framework, and provides interagency situational awareness, assessments, and synthesis of interagency information to the NORAD-USNORTHCOM commander and agency representatives. In practice, this directorate attempts to anticipate gaps and seams between DOD and represented agencies to maximize collaboration and cooperation across the spectrum of

agencies, IGOs, and NGOs before mobilizing for actual response operations (Nightingale, 2006).

E. EXAMPLE 5 (TECHNICAL SOLUTIONS)

1. Harbor and Coastal Surveillance (HCS)—Northrop Grumman Corporation

Harbor Coastal Surveillance (HCS) is a Northrop Grumman sensor integration suite that

Integrates off-the-shelf computers, communications, and sensors with sensor processing and MDA databases to form a flexible, standard based, service oriented architecture that supports the automated collection, analysis, and dissemination of essential information for: (1) coastal surveillance and security; (2) port and harbor security; (3) vessel traffic management; (4) critical infrastructure protection; (5) anti-terrorist force protection; and (6) interdiction and response. (Northrop Grumman, n.d.)

Built on a commercial variant of the Global Command and Control Systems (GCCS) architecture, HCS provided extensive sensor-based persistent surveillance capabilities by integrating vessel Automatic Identification System (AIS) communications data, radar surveillance, and video and infrared feeds into a single command and control system with a common graphical interface and display.

Active sources of information from multiple sensors and data streams are correlated and cross-referenced against substantial vessel databases that include vessel characteristics, ownership, owner, cargo, and voyage information. Multisource correlation aids decision makers in identifying targets of interest for further research, investigation, and possible interdiction. Vessel data, including real-time position, course, and speed, along with the data from the various correlated databases, is depicted on a chart-based interactive display, thereby providing interagency watchstanders with full and complete situational awareness of the port or maritime domain. The COP provided by HCS tethers vessel tracks to a set of MDA data, thereby identifying vessels, their intended movement, associated owners and crew, and cargo. Target-of-interest and anomaly-detection rules can be created to evaluate vessel tracks against geographic

regions, security or safety zones, outputs from data queries, and vessel and transit profiles contained within the associated databases and shared agency information sources. HCS can be adapted through tailoring of hardware, sensor, and software configurations to meet desired functionality and is completely scalable to allow for stand-alone systems or full utilization as a multi-layered (local port—regional fusion center—national COP), multimission support system, including full use of encrypted AIS (EAIS) or blue-force tracking. HCS was designed using open-systems architecture to allow for complete interoperability and integration with DOD, USCG, and Interoperable C4I Services software products used by coalition partners. Additionally, HCS is customizable and supports TCP/IP and web service interfaces to provide interoperability with military and non-military applications requiring data exchange (Northrop Grumman, n.d.).

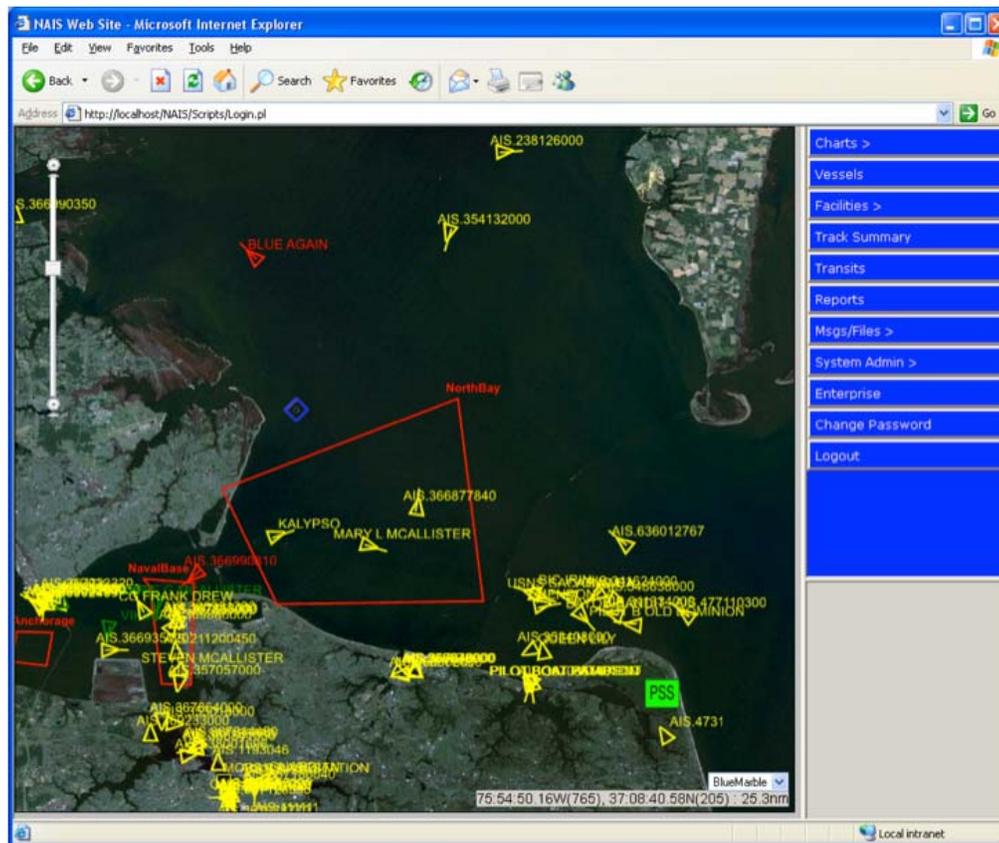


Figure 6. HCS Web Client Home Page5

2. Project Athena—Raytheon

In 2005, USNORTHCOM, USBP, and Raytheon tested Raytheon’s Project Athena multisensor system in an interagency, binational environment along Lake Ontario. The objectives were to “(1) provide information and intelligence on the void of knowledge regarding illicit narcotics trafficking, (2) detection and disruption of terrorist attacks against U.S. interests, and (3) detection and apprehension of U.S. immigration law violators” (USDOD, 2005). The operational concept placed two sensor packages

⁵ Yellow indicates vessels transmitting current AIS data but the vessel track has not yet been identified. Vessels with names have been identified from the database but track information is not contained within the MDA database. Yellow vessels with numbers have yet to be identified. Blue indicates “blue-force” vessel. Red vessels indicate potential targets of interest due to anomaly in transit and/or database information. Green vessels mean the vessel’s AIS data matched all information contained in the vessel databases.

consisting of radars and optical and infrared cameras on the Lake Ontario shore. Athena integrated these sensors with tracking beacons, AIS, and weather data feeds into the COP. Athena fused the data and vessel information to track more than 300 targets simultaneously. Timely tactical decisions were made by the multiagency task force representing federal, state, local, and Canadian homeland security and law enforcement. Targeting of anomalies provided interdiction opportunities for law enforcement units (Figure 7).

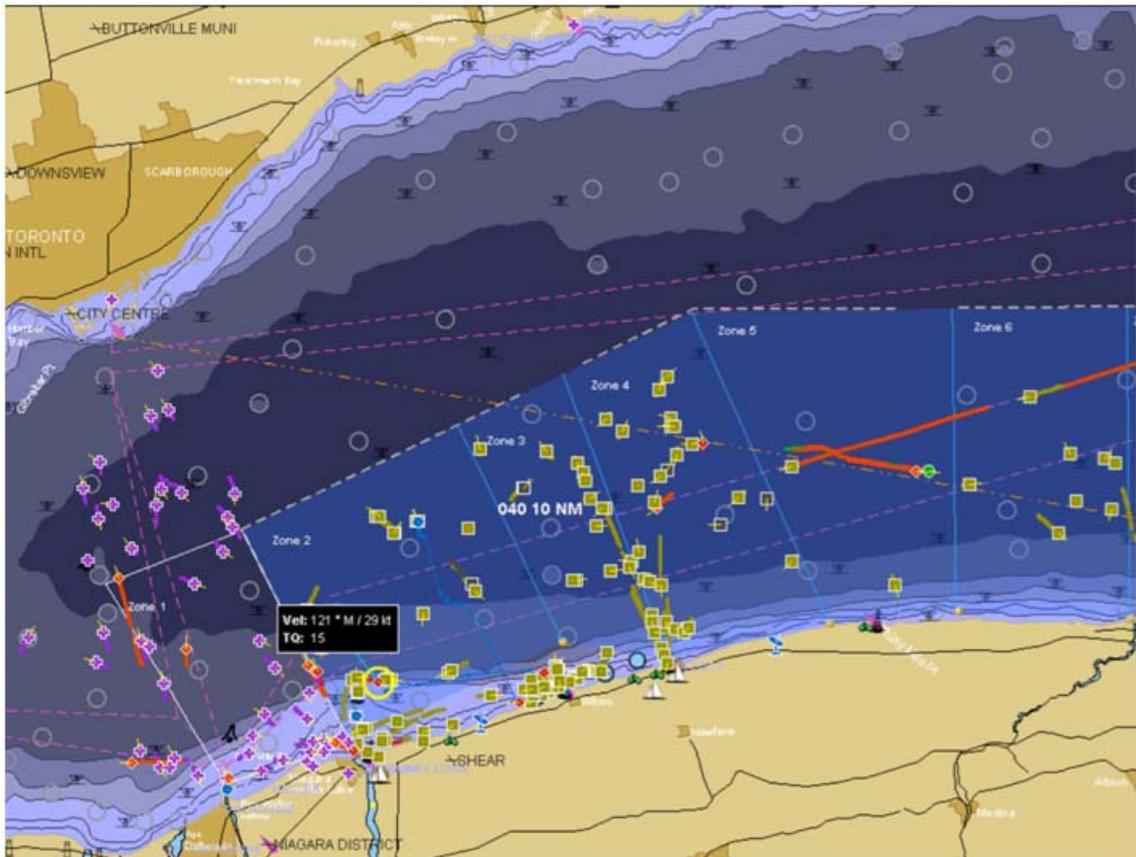


Figure 7. Project Athena (Source: USBP unclassified briefing slide)⁶

⁶ Green squares represent vessels whose voyage started and ended in the U.S. Purple “plus signs” are vessels that started and ended in Canada. Red diamonds are potential targets of interest that crossed the international border.

F. CONVERGENCE OF MODELS

These six models share common threads of interoperability, mutuality of mission planning, exercise and execution, and the sharing of data and information to allow for fusion into strategic and tactical intelligence useable either independently by the responsible jurisdiction or in coordinated efforts. Specifically, the Goldwater-Nichols Act establishes a framework for U.S. federal agency interoperability and joint mission focus. Project SeaHawk demonstrates a port-centric collaborative partnership among federal, state, and local agencies and jurisdictions. The MSOC provides a similar collaborative entity among Canadian federal, provincial, and local agencies with the addition of several U.S. federal law enforcement agencies that are members of the IBET. NORAD's operational control of air defenses for the entire North American continent sets an example for a similar partnership in the maritime domain. A critical component to the success of all these existing models is the utilization of technology to facilitate persistent surveillance, data collection, information analysis, intelligence fusion, visual COP displays, and shared decision-making tools. Application of these elements simultaneously into an interoperational collaborative environment with clear lines of authority and responsibility provides a blueprint for a binational, interstate, interprovincial, and interagency solution to achieve MDA.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION AND RECOMMENDATIONS

The National Plan to Achieve Maritime Domain Awareness (USDHS, 2005) clearly outlines the need and intent for those entrusted with maritime security and safety to fully comprehend all threats in the maritime domain. The establishment of plans and processes, the acquisition and deployment of resources and assets to prevent threats from entering our ports or from engaging in illicit activities, along with the legal ability to respond, are critical and necessary steps. While the intent of MDA is to detect, identify, track, and deter the threat as far from the United States border or territorial waters as possible, the Great Lakes poses a unique challenge in that significant United States ports are contained within a closed maritime system bounded by the United States and Canada, with minimal distances between the two nations. The goals outlined in the various MDA guidelines published by the Department of Homeland Security, U.S. Coast Guard, and Department of Defense apply fully to the Great Lakes environment, but elements of the strategy that push the threat detection and response miles offshore are unrealistic, given the close proximity of the border to the U.S. and Canadian shoreline.

There is no single solution to all the security challenges that must be addressed to obtain complete MDA. Local infrastructure, especially critical infrastructure requiring elevated monitoring, patrols, prevention, and response capabilities, dictates variances in resource and asset requirements. Uniqueness of local geography and geology affect 1) the regional or local requirements and capabilities of vessel types and placement required to cover the navigable area, 2) the type, quantity, and location of sensors used to detect, identify, and monitor vessels, maritime activities, and potential threats, and 3) the types of agreements and jurisdictional authorities that must be in place and practiced prior to a security breach or major homeland security event.

Because vessels traversing the Great Lakes pass through waters adjoining multiple states and provinces within miles (and often yards) of shore, traveling from port to port while crossing in and out of various jurisdictions, the Great Lakes must be viewed as a single system for homeland security, rather than as a series of specific ports, as

outlined in the Port Safety Act of 2006. The proximity of the border—with the distance between the shores of the United States and Canada being, in some cases, less than one mile—requires binational participation and cooperation to ensure that the integrity of the Great Lakes system remains unchallenged.

A. RECOMMENDATIONS

The following recommendations draw from the models and requirements previously discussed in Chapters IV and V and apply them to the unique environment of the Great Lakes. These recommendations expand on the concepts and actions already taken along the northern maritime border to consolidate the system-wide view in a Great Lakes MDA COP. The intent is to enhance the ability of those entrusted with security on the Great Lakes system, as well as those in local ports and jurisdictions, to recognize and understand the threats at all levels requiring coordination and response.

The vast area and number of jurisdictions located along the shores of the Great Lakes indicate a significant need to follow the SAFE Port Act requirements of establishing port-centric or Captain of the Port–centric Interagency Operations Centers (IOCs). These should be located at the major ports, collocated with or in close proximity to Coast Guard or Customs and Border Protection sector command centers. As demonstrated in the model provided by the Charleston Harbor Operations Center (SeaHawk), these IOCs ought to include representation of all federal, state, and local agencies entrusted with homeland security and defense missions, utilizing a National Incident Management System (NIMS) unified command structure outlined in the National Response Framework. The nature of the Great Lakes environment requires an interconnection among all IOCs on the lakes. This necessity is illustrated by oceangoing vessels bound for Lake Superior that must first pass through at least two Captain of the Port zones prior to arriving in port. Similarly, there are no routes possible for vessels heading to places like Duluth, Minnesota, or Chicago, Illinois, that don't transit through adjacent Captain of the Port zones and between the Great Lakes utilizing the river

borders. Further, the constant travel of the commercial carriers, or “lakers,” between the Great Lakes ports does not lend itself to the same arrival notification process used by oceangoing vessels operating in the coastal ports under various nations’ flags.

Utilizing a blended concept adapted from NORAD and SeaHawk, an overarching Great Lakes Maritime Operations Center (GLMOC) should be established to provide complete MDA oversight, collaboration, fusion of information and intelligence, and coordination across the Great Lakes border region. This operations center would maintain the full picture of maritime activity from the western end of Lake Superior in Duluth, Minnesota, to a point east of Quebec City, Quebec, where the St. Lawrence River enters the Gulf of St. Lawrence. The GLMOC should be a binational, interagency, multistate and multiprovince entity that provides a system-wide approach to maintaining an MDA COP, with a primary focus on facilitating unified prevention and response activities for threats inherent in the Great Lakes system.

B. GREAT LAKES MARITIME OPERATIONS CENTER ORGANIZATION

To operate effectively as a permanently established operations center, the GLMOC should blend the military structure for a unified command with that of the National Incident Management System (NIMS). To clarify and distinguish between the unified command structures, the military construct of unity of command “runs from the President to the Secretary of Defense to the Commander of the combatant command to the DOD on-scene commander” (USDHS, 2008a). In contrast, all jurisdictions represented in a NIMS-based unified command “jointly provide management direction to an incident through a common set of incident objectives and strategies and a single Incident Action Plan” where “each agency maintains its authority, responsibility and accountability” (USDHS, 2008a, p. 48). While a primary function of the GLMOC is to provide intelligence and coordination of resources and assets or to facilitate assistance to the local NIMS incident commander, unified command, or IOC, the purpose of the GLMOC is to maintain a Great Lakes system-wide perspective on a not-to-interfere basis with local command and jurisdictional control of mission execution or response activities. For the United States, the GLMOC commander reports to the secretary of the Department

of Homeland Security, rather than a single DHS component or agency. For Canada, the GLMOC commander reports to the Canadian Minister of Public Safety or the appointed delegate.

The resident staff of the GLMOC, while permanently or administratively assigned and owned by the responsible agency or governing jurisdiction, would be operationally controlled or responsible to the GLMOC command structure. This ensures that the system-wide monitoring and processing of Great Lakes maritime information is viewed on a systems level rather than exclusively at the represented agency or jurisdiction port-centric view. In this regard, the construct for daily operations more closely mirrors a military unified command structure similar to NORAD, modified for an interagency, multistate, binational unified command structure (see Figure 8). Each major federal (U.S. or Canadian) agency and each state or province should provide adequate staffing to represent its respective jurisdiction in each of the eight unified command functional staffs.

The unified commander and deputy commander could be alternated between a senior appointee from the U.S. Department of Homeland Security and Public Safety Canada, but both positions cannot simultaneously be from the same nation. The U.S. DHS representative may be appointed from the department or any of its subordinate agencies but should be at the flag officer or senior executive service level with full department-wide authority delegated directly from the DHS secretary.

Agency and state or provincial representatives in each functional area serve as peers under a facilitator to ensure work efforts are coordinated without a rank or hierarchy placed on any individual representative's or jurisdiction's requirements over another.

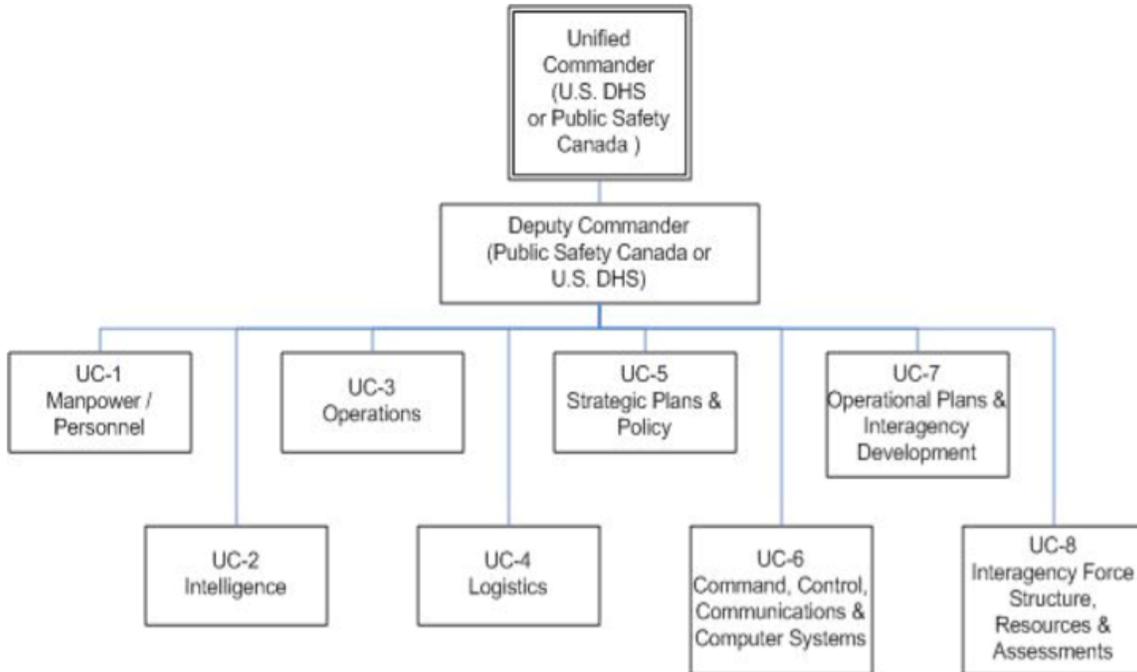


Figure 8. Great Lakes Maritime Operations Center Proposed Command Structure Including Primary Functional Areas Modeled after U.S. Department of Defense Unified Command or Joint Staff Structures

Maintaining the system-wide perspective, the functional areas collect data, fuse information and analyze intelligence, and promptly disseminate operational and tactical intelligence to the responsible jurisdiction or incident command post to take appropriate action. Additionally, the functional areas develop system-wide plans and agreements for ratification and approval by the federal agencies, state or provincial governors, with appropriate consideration for local government adoption as determined by the responsible governor. Since each federal agency, state, and province will have various members assigned full time to the GLMOC, each jurisdiction must identify one member of its contingent as the lead. The designated lead will serve as the jurisdiction’s voice to the GLMOC senior management team to ensure that unity of effort throughout the GLMOC is achieved. Jurisdictional representatives will fulfill their functional area responsibilities under the unified staff element, but will be administratively responsible to their jurisdiction’s designated lead.

The top level of the unified command should be made up of a single agency representative with full reach-back authority from each federal agency with mission execution and jurisdictional authority along the Great Lakes, including all border-related mission sets. As peers within the top level of the unified command, each border state or province maintaining a significant Great Lakes port would have a single primary representative who is appointed to speak with the state's collective authority for their state's governor or homeland security director in their assigned functional area. Canadian agency and provincial representatives in peer roles to the United States federal agencies and state governors would have an equal voice in the GLMOC unified command. In this regard, the collaborative command environment should model the binational structure of the existing NORAD construct used to maintain positive control over the North American air space. Specifically, the structure should have multijurisdictional collaborative command elements that facilitate analysis, mission planning, and execution by addressing 1) manpower and personnel, 2) intelligence, 3) operations, 4) logistics, 5) strategic plans and policy, 6) command, control, communications, and computer systems, 7) operational plans and interagency development, and 8) interagency force structure, resources, and assessments. Additionally, authority to initiate integrated cross-border maritime law enforcement operations as authorized by the U.S. and Canadian governments (US–Canada Framework Agreement, 2009) should be used to its fullest extent on a Great Lakes system-wide basis in addition to a function of port-centric IOC mission coordination and execution.

C. GLMOC COMMON OPERATING PICTURE

To have a fully functional COP, GLMOC will have to leverage all available sources of information from across Great Lakes federal, state, and local jurisdictions and fuse the information into intelligence that is disseminated to agencies, states, or local organizations with the requisite jurisdictional authority to address the threat or issue. Regardless of the C4IT decision-making tool chosen as the COP software platform, the critical first step is to establish an integrated network of sensors to allow for persistent surveillance of the entire Great Lakes system by the GLMOC staff. The sensor network

must include AIS transmit-and-receive capabilities and encrypted AIS for blue-force tracking of all vessel classes meeting the international and United States AIS carriage requirements. Integration of the AIS tracking information coupled with the MDA databases will provide extensive visibility and real-time tracking of vessels required to carry AIS.

Of great concern is the risk posed by small vessels, including privately owned recreational vessels, operating on the Great Lakes. As noted in the DHS Small Vessel Security Strategy, “small vessels 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” (USDHS, 2008b, p. iv). To address these concerns and the lack of enough homeland security and law enforcement patrol personnel to effectively cover the entire expanse of U.S. and Canadian shoreline with round-the-clock patrols, technology must be leveraged to its fullest extent in order to conduct persistent surveillance of the small vessels operating throughout the Great Lakes system.

A radar surveillance system, similar to those used by the U.S. Coast Guard in its Vessel Traffic Services, should be installed that provides full coverage of the Great Lakes system. The radar system should fully integrate with the AIS feeds to correlate the actual locations of vessels with the data emitted from the AIS units located on the Class A and Class B vessels.⁷ Radar feeds should also be tied to a set of rules that highlight vessels,

⁷ Class A AIS carriage is mandated by the International Maritime Organization (IMO) for vessels 300 gross tons and greater engaged on international voyages, cargo ships 500 gross tons or more not engaged on international voyages, and all passenger ships carrying more than 12 passengers regardless of size. Class B AIS is not mandated by the IMO and has been developed for non-SOLAS (Safety of Life at Sea) commercial and recreational vessels. IMO International Convention for Safety of Life at Sea, Chapter V, 1974, December 2002 amendments, adopted 13 December 2002 and entered into force July 1, 2004 (<http://www.imo.org/>).

including the small vessels addressed above, that are in violation of border crossing regulations, security zone management, or where IOC or GLMOC watchstanders paint a target on a vessel of interest.

Wherever critical infrastructure, maritime activity (commercial or recreational), and geologically conducive shore features exist for illegal activity, video and infrared cameras should be installed. Additionally, all areas that have minimal distances between the United States and Canada need to maintain full visual surveillance. These areas include the St. Lawrence River, the Niagara River, the St. Clair River, and St. Mary's River. The sensor data should be received locally with video data sources controlled and operated by the local jurisdictions.

The Great Lakes system-wide COP should be built with initial focus on creating the network for persistent surveillance throughout the local ports, Captains of the Port, DHS command centers, and Canadian MSOC. The data sources should be integrated locally, and then connected to an enterprise architecture that is accessible to the GLMOC COP and other local port command centers as necessary. Acknowledging that not all local and state first responders have access to federal classified information, information sources should be distributed, to the degree possible, at the lowest acceptable security classification on a need-to-share basis for tactical action in the local ports. On a strategic and operational planning level, information obtained from the network of sensors should be pulled into the classified system for planning and detailed information, to be synthesized and shared with proper authorities in the federal, state, and provincial levels of government.

The overarching technical strategy should define and utilize a service-oriented enterprise architecture that allows for complete integration of sensor technologies into a single COP using non-proprietary or open architecture standards and protocols. This will facilitate the merging of existing databases and information technology infrastructure into a common enterprise solution that enhances the manipulation, analysis, display, and decision-making tools available. Additionally the use of open architecture will promote interoperability between agency-specific information technology systems, while providing greater flexibility for future modifications as operational requirements evolve.

While the IOCs maintain their focus on port-centric threats, activities, and concerns, the GLMOC would fuse the information obtained from each of the IOCs and Canada's MSOC. The GLMOC staff needs to assemble and analyze the various pieces of information with the data feeds populating the COP to detect and identify system-wide threats to better understand and mitigate risks throughout the Great Lakes system. As intelligence is formed, it must be quickly disseminated back to the IOCs or MSOC for the appropriate federal, state, or local jurisdictions to assign the appropriate resources and assets to deter, thwart, apprehend, or neutralize the threat.

D. END REMARKS

Current maritime homeland security strategies and doctrine attempt to ascertain and intercept threats well offshore or prior to entering domestic waters. However, they do not adequately address the close proximity between the United States and Canada along the Great Lakes and interconnecting rivers. The contiguity of the border prevents either nation from unilaterally exercising its maritime sovereignty to detect, identify, intercept, thwart, or otherwise neutralize homeland security threats prior to impacting its nation's ports or maritime domain.

The piecemeal nature of port-centric efforts of disparate pieces of information as currently managed prevents a system-wide approach and permits a variety of threats (small vessels, weapons, human trafficking, illegal drugs, counterfeit money, etc.) to enter unnoticed. A system-wide approach with the input and cooperation of all parties could begin to close the gap. As the two nations continue to work together to meet the threats, their cooperation on maritime domain awareness may well lay the foundation for the overall effort.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- 9/11 Commission. (2003). *The 9/11 Commission report: Final report of the National Commission on Terrorist Attacks upon the United States*. New York: W.W. Norton.
- Andreas, Peter. (2003). A tale of two borders: the U.S.-Mexico and U.S.-Canada lines After 9-11. Working Paper 77. Providence, RI: Brown University Press.
- Beeson, Scott. (2007). Project "SeaHawk" briefing by Capt. Scott Beeson to National Defense Industrial Association (NDIA). Retrieved September 4, 2010, from www.ndia.org/Resources/OnlineProceedings/Pages/7490_HomelandSecuritySymposium.aspx
- Brennan, Patrick W. (2006). National security implications of border security along the northern border; statement before the Armed Services Committee, U.S. House of Representatives, Congress #109, Session #02, 1 August 2006. Retrieved May 16, 2007, from <https://www.hsdl.org/?view&doc=66688&coll=limited>
- Goldwater-Nichols Act of 1986, Public Law 99-433, 99th Congress.
- Government of Canada. (n.d.). Marine Security Operations Centres. Retrieved August 29, 2010, from www.msoc-cosm.gc.ca/comms/faq/index_e.asp
- Government of Canada. (2004). Securing an open society: Canada's national security policy. Retrieved June 15, 2007, from <http://www.pco-bcp.gc.ca/docs/information/publications/natsec-secnat/natsec-secnat-eng.pdf>
- Government of Canada. (2005). Marine Security Operations Centres (MSOC) project scope statement amendment #1, Project No. 00000806, 22 Jun 2005, File No. 300000806-326, AL NO. 1, Government of Canada. Retrieved July 18, 2010, from <http://www.msoc-cosm.gc.ca/doc/pd-da/index-eng.asp>
- Grissom, Bruce. (2004). NORTHCOM revisited: Tri-national prospects for continental security. Newport, RI: Naval War College. Retrieved May 18, 2010, from <https://www.hsdl.org/?view&doc=29926&coll=limited>
- Kearney, George, & Millar, John. (2004). Canadian security and defence: The maritime dimension. *Canadian Military Journal* 5(3).
- LeBeuf, Marcel-Eugene. (2001). Quoting C. Sands: What are the policy options? Canada's policy choices. Managing our border with the United States. Toronto: Public Policy Forum.

- LeBeuf, Marcel-Eugene. (2002). Canada-US law enforcement border partnership—An evolving situation. Speech delivered at the Sixth Biennial Conference: International Perspectives on Crime, Justice and Public Order, London, UK, June 16–20, 2002.
- Levy, Bruce. (2003). Letter from Director Bruce Levy, U.S. Transboundary Division, Department of Foreign Affairs and International Trade, Canada, to Director Nancy Mason, Office of Canadian Affairs, United States Department of State.
- Locher, James R., III. (2001). Has it worked?—The Goldwater-Nichols Reorganization Act. *Naval War College Review* 54(4).
- McAleavey, Chris. (2002). “IBETing on a secure border.” *TECHbeat* Fall 2002.
- Nightingale, Barry. (2006). Directorate of Interagency Coordination Briefing, Fall 2006 Symposium: Introduction to NORAD and USNORTHCOM, and energy security. Colorado Springs, CO. October 4–6, 2006.
- North American Aerospace Defense Command (NORAD). Web site. Retrieved September 3, 2010, from www.norad.mil/about/agreement.html
- Northrop Grumman. (n.d.). Harbor and coastal surveillance HCS 1.3.X product specification. Proprietary document.
- Northrop Grumman. (2005). Hawkeye: Port and coastal surveillance system overview: PowerPoint presentation by Tom Fagre, Northrop Grumman
- Pendall, David W. (2005). Persistent surveillance and its implications for the common operating picture.” *Military Review*, November-December 2005.
- SAFE Port Act of 2006. Public Law 109-347-Oct.13, 2006, “Security and Accountability for Every Port Act of 2006,” Section 108.
- Seghetti, Lisa M. (2004). Border security: U.S.–Canada immigration border issues. Washington, D.C.: Congressional Research Service.
- United States Coast Guard. (2004). Common operational picture concept of operations (COP CONOPS), Version 1.1. FOUO.
- United States Coast Guard. (2005). NAIS mission needs statement, final version 9.4.2.
- United States Coast Guard. (2006a). USCG operational requirements document (ORD) for the Nationwide Automatic Identification System (Nationwide AIS) project. FOUO.

United States Coast Guard. (2006b). Maritime Sentinel: Coast Guard strategic plan for combating maritime terrorism.

United States Coast Guard. (2008a). Common operational picture operational requirements document (COP ORD). Version 1.0, May 13, 2008. FOUO.

United States Coast Guard. (2008b). Nationwide automatic identification system contract section J-2 performance specification, vol. 2, July 15, 2008.

United States Coast Guard. (2009). Command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) mission need statement, Version 1.1, draft 05. FOUO.

United States Coast Guard. (2010). Interagency operations centers concept of operations, version 1.0 (draft). FOUO.

United States Customs and Border Patrol. (n.d.). Web site. Retrieved August 26, 2007, from www.cbp.gov

United States Department of Defense. (2005). Operation after action report (GR 3544-05). Department of Defense Joint Task Force North. October 31, 2005. FOUO.

United States Department of Defense. (2008). Instruction 5000.02: Operation of the Defense Acquisition System. Retrieved June 15, 2010, from <http://www.dtic.mil/whs/directives/corres/ins1.html>

United States Department of Homeland Security. (2005). National plan to achieve maritime domain awareness for the national strategy for maritime security. Washington, D.C.: DHS.

United States Department of Homeland Security. (2006). Fact sheet: Nationwide plan review. Retrieved August 26, 2007, from www.dhs.gov/xnews/releases/press_release_0928.shtm

United States Department of Homeland Security. (2008a). National response framework. Washington, D.C.: DHS.

United States Department of Homeland Security. (2008b). Small vessel security strategy. Washington, D.C.: DHS.

United States Department of Justice. (n.d.). SEAHAWK: A model for port security, Project SeaHawk Task Force.

- United States Department of Justice. (2002). Follow-up report on border patrol's efforts to improve northern border security. Report No. I-2002-004 (redacted version). Washington, D.C.: Department of Justice.
- United States Department of State. (2003). Pro Memoria of the United States Department of State. Washington, DC. Retrieved August 16, 2010, from <http://www.state.gov/s/1/2003/44389.htm>
- United States Joint Chiefs of Staff. (2006). Joint Publication 3-08: Interagency, intergovernmental organization, and nongovernmental organization coordination during joint operations, Vol. 1, March 17, 2006.
- United States Northern Command. (2007). North American Aerospace Defense Command and United States Northern Command Vision 2020. Retrieved August 18, 2010, from <https://www.hsdl.org/?view&doc=87343&coll=limited>
- Watts, Robert. (2006). Implementing Maritime Domain Awareness. Master's thesis, Naval Postgraduate School. Retrieved July 11, 2010, from http://www.imo.org/safety/mainframe.asp?topic_id=754#regulations
- The White House. (2002a). Remarks by President Bush and Prime Minister Chretien on U.S.–Canada smart borders. Washington, D.C.: The White House, 2002. Retrieved January 25, 2007, from www.whitehouse.gov
- The White House. (2002b). Specifics of secure and smart border action plan. Washington, D.C.: The White House. Retrieved January 25, 2007, from www.whitehouse.gov
- The White House. (2004). Homeland Security Presidential Directive 13: Maritime security policy. Washington, D.C.: Government Printing Office.

Agreements

- Agreement between the Government of the United States of America and the Government of Canada on the North American Aerospace Defense Command. (2006, April 28). Retrieved August 18, 2010, from <http://www.treaty-accord.gc.ca/text-texte.asp?id=105060>
- International Convention for the Safety of Life at Sea (SOLAS). (1974, with amendments). Retrieved September 12, 2010 from <http://www.imo.org/>

Rush-Bagot Agreement of 1817. (1817). Exchange of notes relative to naval forces on the American lakes signed at Washington April 28 and 29, 1817, submitted to the Senate April 6, 1818. Resolution of approval and consent April 16, 1818. Proclaimed April 28, 1818. Retrieved January 22, 2007, from <http://www.yale.edu/lawweb/avalon/diplomacy/britain/conv1817.htm>

US–Canada Framework Agreement on Integrated Cross-Border Maritime Law Enforcement Operations Between the Government of the United States of America and the Government of Canada (2009, May 26). Retrieved August 18, 2010, from <http://www.hsdl.org/?view&doc=110229&coll=limited on 18 August 2010>

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Commandant (CG-7)
U.S. Coast Guard
Washington, D.C.
4. Commandant (CG-9)
U.S. Coast Guard
Washington, D.C.
5. Commander, Ninth Coast Guard District
U.S. Coast Guard
Cleveland, Ohio