Coast Guard Publication 2-0

Intelligence

May 2010

THE COMMANDANT OF THE UNITED STATES COAST GUARD

Washington, D.C. 20593-0001
May 2010

Commandant's Letter of Promulgation

Coast Guard Publication 2-0 (CG Pub 2), *Intelligence,* describes the theory and philosophy of intelligence as practiced by the Coast Guard. It provides a conceptual framework for understanding and conducting effective intelligence activities. The Coast Guard's view of intelligence is based on our unique role as a military, multi-mission, and maritime force as described in Coast Guard Publication 1, *U.S. Coast Guard: America's Maritime Guardian.*

CG Pub 2, *Intelligence,* discusses the nature and principles of the Coast Guard's use of intelligence. A proper understanding of the capabilities and limitations of intelligence supports the effective execution of Coast Guard missions and ensures the Coast Guard is *Always Ready* for all threats and all hazards.

CG Pub 2, *Intelligence,* does not supersede any current doctrinal publication. It provides the authoritative basis for the subsequent development of intelligence doctrine, education, training, equipment, procedures, and organization. CG Pub 2, *Intelligence,* affords no specific techniques or procedures for intelligence activities; rather, it offers broad guidance which requires judgment in its application. Other Coast Guard intelligence publications and manuals provide specific tactics, techniques, and procedures.

Coast Guard Intelligence doctrine applies across the full mission spectrum, from maritime safety to maritime stewardship to maritime security. Since intelligence is an essential component of any successful mission, this publication is meant to guide Guardians at all levels of command, in both the operating forces and the supporting establishment.

Semper Paratus!

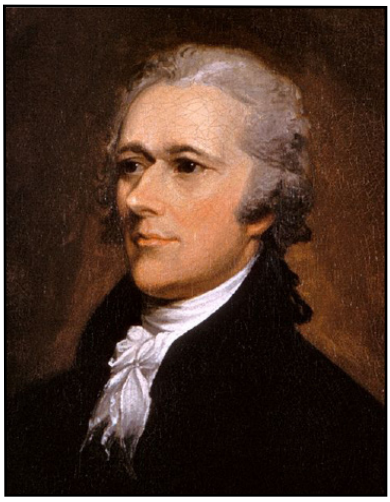
THAD W. ALLEN
Admiral, U.S. Coast Guard

TABLE OF CONTENTS

Chapter One

Overview of Intelligence

Decision Advantage



Alexander Hamilton handled intelligence duties as George Washington's aide-de-camp during the Revolutionary War.

For more than two centuries, the Coast Guard has relied on intelligence information to execute its missions. In fact, an intelligence assessment of the maritime domain contributed to the establishment of the Revenue Marine in 1790. Alexander Hamilton evaluated the extent and recent history of maritime smuggling, appraised the opportunities the American coastline provided to merchants determined to avoid taxes collected in ports, and predicted the rapid growth of foreign trade and maritime shipping interests. In today's language, he employed an Intelligence Preparation of the Maritime Domain (IPMD) to inform his determination that a fleet of cutters with the mission of collecting revenue and combating smuggling would benefit the nation. His mission decision, enhanced by intelligence, proved greatly advantageous to the United States. Since then, the Coast Guard has continued its use of intelligence to create this "Decision Advantage."

Definition of Intelligence

Intelligence is the development and analysis of raw material in order to determine what the information means and to identify the implications for decision making. In other words, intelligence is the analysis and synthesis of information into

knowledge. It is knowledge about an adversary, threat, or the surrounding environment needed for decision making. It is important to recognize that intelligence is not simply another term for information. Information is unevaluated material of any kind, such as documents found onboard a vessel, photographs, radio intercepts, patrol reports, and reports of interviews. Information is the raw material from which intelligence is ultimately derived. Few pieces of information speak conclusively for themselves. They must be combined and compared with other pieces of information, analyzed, evaluated, and finally given meaning. Intelligence does not just repeat what a source reveals. The end result is not more information, but knowledge that provides a meaningful assessment of the situation.

Objective of Intelligence

The purpose of intelligence, therefore, is to inform commanders and decision makers by providing accurate, timely, and relevant knowledge about adversaries, threats, and the surrounding environment. In the Coast Guard, this surrounding environment includes the maritime domain and the cyber domain. Many Coast Guard members often narrowly interpret this as providing tactically-actionable intelligence to operational forces and, as a result, measure the effectiveness of intelligence support accordingly. Although developing the key piece of intelligence that cues the interdiction of an adversary is a laudable goal, it is by no means the only support required by Coast Guard commanders and decision makers. In fact, one of the most effective ways intelligence can provide support is through an IPMD. An IPMD involves identifying and evaluating existing capabilities and limitations of an adversary, hypothesizing possible adversary courses of action based upon these capabilities and limitations, and assisting in the development and evaluation of practical Coast Guard (and other agency) courses of action to counter the adversary. The IPMD process is further described in Section 4.B.2 of the Coast Guard Field Intelligence Support to Operations (FISO) Manual, COMDTINST M3800.5 (series).

Nature of Intelligence

The nature of intelligence presents numerous challenges. Intelligence is a fluid commodity. It is perishable. It may be incomplete, sometimes confusing, and often contradictory. More gaps exist in what is known about an adversary than what is known about friendly forces. Moreover, the reliability of everything known about an adversary is subject to greater scrutiny and doubt. It is important to remember that intelligence produces assessments, estimates, and hypotheses. It does not produce certainties.

Command Expectations

Commanders measure intelligence against a high standard. They require intelligence to describe in detail unfamiliar places, to identify customs and attitudes of fundamentally different societies, to assess the capabilities of unique and unfamiliar adversaries, and to forecast how these societies and adversaries will act in the future. Most notably, commanders want intelligence to assist them in understanding the thought process of adversaries and predict, with certainty, what course of action they intend to pursue, possibly even before they know themselves. Commanders and decision makers desire a depth and degree of accuracy which approaches perfection. This is as it should be because the price of failure in intelligence is high. Inadequacies in intelligence can lead directly to loss of life, destruction of equipment and facilities, and mission failure.

Commanders need quality intelligence.

May Appear to Invalidate Itself

The challenges and expectations facing intelligence are further complicated by the irony that good intelligence may actually appear to invalidate itself. Consider the following example: An intelligence staff reports that a maritime smuggling organization has planned a vessel-to-vessel drug transfer at a specific rendezvous. Acting quickly, the commander sorties patrol aircraft to conduct surveillance of the location. The adversary, however, detects the aircraft and aborts the transfer. As a result, the initial intelligence report, which accurately predicted the smuggling event, appears wrong. Accordingly, the effects of intelligence are extremely difficult to isolate and measure.

Need Exceeds Capability

Finally, it should be emphasized that the need for intelligence usually greatly exceeds the ability to produce it. Despite the existence of extensive specialized capabilities designed to collect information about the adversary, the availability of the capability and the resulting collection will normally be less than what is desired. Furthermore, collecting information does not by itself provide the needed intelligence. Even when friendly forces obtain information directly from the adversary (such as from informants, cooperating defendants, tactical questioning, wiretaps, or exploited documents), intelligence components must

still confirm, evaluate, interpret, validate, and analyze that information. Follow-on collection, processing, and production activities are normally needed. Throughout the process, available intelligence resources to provide answers are often limited.

What Intelligence Can and Cannot Do

Intelligence information can be an extremely powerful tool. It is most useful when the consumer has a clear understanding of what intelligence can and cannot do. While laws, policies, capabilities, and standards are constantly changing, these general guidelines can help consumers make the most of this resource.

Intelligence can provide valuable services, such as:

- Warning of potential threats.
- Decision advantage, by improving the decision making of consumers and partners while hindering that of enemies.
- Insight into key current events.
- Descriptions of adversary modus operandi, including tactics, techniques, and procedures likely to be used in the future.
- Situational awareness.
- Long-term strategic assessments on issues of ongoing interest.
- Assistance in preparation for senior-level meetings that include national security-related subjects.
- Pre-travel security overview and support.
- Reports on specific topics, either as part of ongoing reporting or upon request for short-term needs.
- Enhanced knowledge on persons of interest.
- Pre and post-travel support.

Realistic expectations will help the consumer fill their intelligence needs. Some things that ***intelligence cannot*** do include:

- ***Predict the future -*** Intelligence can provide assessments of likely scenarios or developments, but there is no way to predict what will happen with certainty.
- ***Violate the U.S. Constitution or U.S. law -*** Intelligence activities and law enforcement operations must be conducted consistent with all applicable laws. All intelligence activities and law enforcement operations are subject to extensive and rigorous oversight both within the Executive Branch and by the Legislative Branch.

The Intelligence Cycle/Process

An effective way to organize, develop, and manage intelligence activities is to use the intelligence cycle (also called the intelligence process) as a guide. It consists of the following six interrelated steps.

1. ***Planning and Direction -*** Planning and Direction is the leadership and management of the entire intelligence effort, from promulgating intelligence requirements to tasking collection to acquiring exploitation tools to prioritizing production requirements.

2. ***Collection and Reporting -*** Collection is the gathering of raw data from which finished intelligence is produced. It also includes reporting of the collected information. Because all Coast Guard personnel can be involved in obtaining information of potential intelligence value (thereby leading to the phrase "Every Guardian a Sensor"), a critical function of intelligence staffs is to sensitize personnel to collection requirements and intelligence needs.

Seventh District Intelligence Specialists perform digital forensics on a GPS receiver to help the Florida Fish and Wildlife Conservation Commission in a boating fatality accident investigation.

3. ***Processing and Exploitation -*** Processing and Exploitation is the conversion of collected information into a form suitable for analysis. It includes translating, transcribing, preparing images, and transforming data stored in electronics and other media into text, tables, graphics, or charts.

4. ***Analysis and Production -*** Analysis and Production is the process of evaluating, interpreting, and integrating raw, processed, and exploited data and information into intelligence products for known or anticipated purposes and applications. In the Coast Guard, intelligence staffs perform analysis and develop products for their supported commanders. In addition, the Intelligence Coordination Center and the Maritime Intelligence Fusion Centers serve as a reach back capability for analysis and production in support of those staffs.

5. ***Dissemination and Utilization -*** Dissemination is the conveyance of intelligence to the consumer in a usable form. The Coast Guard has added "Utilization" to this step because intelligence that is disseminated but not utilized has little value.

6. ***Evaluation and Feedback -*** Evaluation and Feedback involve actions to improve the performance of intelligence operations and the overall functioning of the intelligence cycle.

Intelligence Disciplines

Intelligence disciplines are well defined areas of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. The following are examples of intelligence disciplines.

Open Source Intelligence (OSINT) - Open Source Intelligence is intelligence derived from information publicly available from print or electronic forms, including radio, television, newspapers, journals, the Internet, commercial databases, videos, graphics, and drawings.

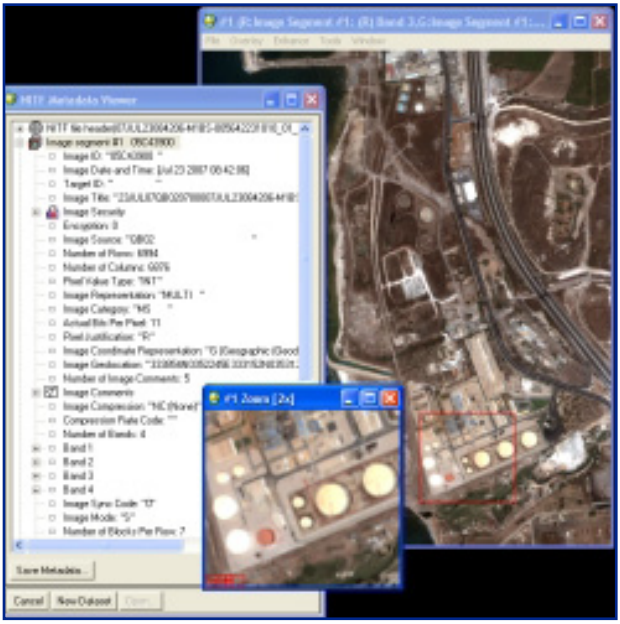
Human Intelligence (HUMINT) - Human Intelligence is intelligence derived from information collected and provided by human sources. It includes overt data collected by personnel in diplomatic and consular posts. It also includes information collected via clandestine sources of information, debriefings of foreign nationals and U.S. citizens who travel abroad, official contacts with foreign governments, and direct observation. As a military service, a law enforcement and regulatory agency, and a member of the Intelligence Community, the Coast Guard has unique authorities, access, and abilities for conducting a wide variety of HUMINT activities. For example, Coast Guard HUMINT activities include domestic information gathering for situational awareness and against criminal adversaries. The vast majority of these activities involve overt observations and interactions made under Coast Guard law enforcement and regulatory authority, activities which align under a

Sector Boston intelligence staff conduct a consent-based interview on a visiting motor vessel.

subset of HUMINT called Law Enforcement Intelligence Collection (LEIC). Interagency partners frequently associate the term HUMINT with collecting foreign intelligence, maintaining confidential sources, possessing specialized foreign intelligence HUMINT training, employing particular tradecraft, and operating under different authorities than the Coast Guard. Due to the Coast Guard's law enforcement and regulatory authorities, Coast Guard law enforcement intelligence element personnel use the term LEIC rather than HUMINT when describing their collection activities.

Signals Intelligence (SIGINT) - Signals Intelligence is information gathered from data transmissions, including communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT). As a law enforcement agency, the Coast Guard also collects signals using law enforcement and regulatory authorities. Although functionally similar to SIGINT, this type of law enforcement function is more appropriately termed Law Enforcement Technical Collection and is further described in COMDTINST C3221.1 (series), Law Enforcement Technical Collection (LETC) Activities.

Geospatial Intelligence (GEOINT) - Geospatial Intelligence is information describing, visually depicting, and accurately locating physical features and human activities on the Earth. Examples of GEOINT products include imagery, analyses, maps, and navigation charts. Imagery intelligence (IMINT) is a subset of GEOINT.



An example of imagery used for intelligence planning purposes.

Measurement and Signature Intelligence (MASINT) - Measurement and Signature Intelligence is information produced by quantitative and qualitative analysis of physical attributes of targets and events in order to characterize and identify them.

Chapter Two

The Intelligence Community

Intelligence Community Overview

The Intelligence Community (IC) is a group of 17 Executive Branch departments and agencies that work together and separately to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States. The roles and responsibilities of the IC and its members are laid out in Executive Order 12333, United States Intelligence Activities, as amended (hereafter referred to as EO 12333).

Intelligence Community Responsibilities

Under EO 12333, all departments and agencies in the IC cooperate fully to provide the President, the National Security Council (NSC), and the Homeland Security Council (HSC) with the necessary information to base decisions concerning foreign, defense, and economic policies, and to protect U.S. national interests from foreign security threats. EO 12333 requires IC members to:

- Use all means, consistent with Federal law and EO 12333, and with full consideration of the rights of U.S. persons, to obtain reliable intelligence information to protect the U.S. and its interests.
- Protect the legal rights of all U.S. persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law.
- Give special emphasis to detecting and countering espionage, and other threats and activities directed by foreign powers or their intelligence services against the U.S. and its interests; threats to the U.S. and its interests from terrorism; and threats to the U.S. and its interests from

the development, possession, proliferation, or use of weapons of mass destruction.

- Prepare and provide intelligence in a manner that allows the full and free exchange of information, consistent with legal and presidential guidance.
- Report possible violations of Federal criminal laws by employees and other persons in a manner consistent with the protection of intelligence sources and methods.
- Report activities that may be unlawful or contrary to Executive Order or presidential directive.
- Protect intelligence and intelligence sources, methods, and activities from unauthorized disclosure.
- Facilitate the sharing of information or intelligence to state, local, tribal, and private sector entities.
- Disseminate information or intelligence to foreign governments and international organizations under approved arrangements or agreements.

Intelligence Community Members

The members of the IC serve the information and intelligence needs of their respective heads of departments and also operate as part of the integrated IC. The following are summaries of each member.

Director of National Intelligence (DNI) - The IC is led by the DNI, who is subject to the authority, direction, and control of the President. The DNI is the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to national security. The DNI oversees and directs the implementation of the National Intelligence Program (NIP) and execution of the NIP budget. The DNI heads the Office of the Director of National Intelligence (ODNI), whose duty is to organize and coordinate the other 16 IC members based on intelligence consumers' needs. Included within the ODNI are the National Counterterrorism Center (NCTC), the National Counterproliferation Center (NCPC), the Open Source Center (OSC), and the National Media Exploitation Center (NMEC).

Central Intelligence Agency (CIA) - The CIA is the largest producer of all-source national security intelligence for senior U.S. policymakers. The CIA's intelligence analysis on overseas developments feeds into the informed decisions by policymakers and other senior decision makers in the national security and defense arenas. The Director of the CIA is the national authority for coordination, de-confliction, and evaluation of clandestine HUMINT operations across the IC, consistent with existing laws, Executive Orders, and interagency agreements.

Included within the CIA is the National Clandestine Service (NCS) which conducts clandestine collection (primarily human source collection) of foreign intelligence that is not obtainable through other means. The NCS also carries out covert action in support of U.S. policy goals when legally and properly directed and authorized by the President. Moreover, the NCS performs counterintelligence activities to protect classified U.S. activities and institutions from penetration by hostile foreign organizations and individuals.

Defense Intelligence Agency (DIA) - The DIA collects, produces, and manages foreign military intelligence for policymakers and military commanders. The DIA Director is a senior military advisor to the Secretary of Defense and the DNI, and is the program manager for the General Defense Intelligence Program. Within the DIA is the Defense Intelligence Analysis Center (DIAC), the Missile and Space Intelligence Center (MSIC), the National Center for Medical Intelligence (NCMI), the National Defense Intelligence College (NDIC), and the Defense Attaché System (DAS), which conducts representational duties on behalf of the Department of Defense and advises U.S. Ambassadors on military matters.

Federal Bureau of Investigation (FBI) - The FBI, as an intelligence and law enforcement agency, is responsible for understanding threats to national security and penetrating national and transnational networks that have a desire and capability to harm the U.S. It focuses on terrorist organizations, foreign intelligence services, Weapon of Mass Destruction (WMD) proliferators, and criminal enterprises. Within the FBI are the National Security Branch (NSB), Counterterrorism Division (CTD), Counterintelligence Division (CD), Directorate of Intelligence (DI), Weapons of Mass Destruction Directorate (WMDD), and the Terrorist Screening Center (TSC).

National Security Agency (NSA) - The NSA is the nation's cryptologic organization, with responsibility for protecting U.S. national security information systems, and collecting and disseminating foreign signals intelligence. It is part of the Department of Defense and is staffed by experts in cryptanalysis, cryptography, mathematics, computer science, and foreign language analysis. Within the NSA are the Signals Intelligence Directorate, the Central Security Service (CSS), the NSA/CSS Threat Operations Center (NTOC), the Information Assurance Directorate (IAD), and the National Security Operations Center (NSOC).

National Reconnaissance Office (NRO) - The NRO is a joint organization engaged in the research and development, acquisition, launch, and operation of overhead reconnaissance systems necessary to meet the needs of the IC and the Department of Defense.

National Geospatial-Intelligence Agency (NGA) - The NGA collects and creates information about the Earth for navigation, national security, U.S. military operations, and humanitarian aid efforts.

The Office of Intelligence and Counterintelligence (IN), Department of Energy (DOE) - The IN assesses worldwide nuclear terrorism threats and nuclear proliferation, and evaluates foreign technology threats. IN protects vital national security capabilities ranging from nuclear weapons to energy research and development projects. It also conducts counterintelligence operations to protect nuclear weapons secrets and other sensitive scientific endeavors.

The Bureau of Intelligence and Research (INR), Department of State (DOS) - INR provides all-source intelligence support to the Secretary of State and other DOS policymakers including ambassadors, special negotiators, country directors, and desk officers. The INR Assistant Secretary is responsible for intelligence analysis, policy, and coordination of intelligence activities in support of diplomacy.

The Office of Intelligence and Analysis (OIA), Department of the Treasury - The OIA is responsible for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information related to the operation and responsibilities of the Department of the Treasury. OIA's focus includes financing for terrorism, insurgency, rogue regimes, and WMD proliferation.

The Office of National Security Intelligence (ONSI), Drug Enforcement Administration (DEA) - ONSI facilitates intelligence coordination and information sharing with the IC to reduce the supply of drugs, protect national security, and combat global terrorism. Additionally, it collects and produces intelligence in support of the DEA and other federal, state, local and tribal entities.

The Office of Intelligence and Analysis (I&A), Department of Homeland Security (DHS) - I&A uses multi-source information and intelligence to identify and assess current and future threats to the U.S. I&A provides actionable intelligence to support national and DHS decision makers while working closely with state, local, tribal, and private sector entities. I&A focuses on threats to border security; chemical, biological, radiological, and nuclear issues, to include explosives and infectious diseases; critical infrastructure protection; extremists within the homeland; and travelers entering the homeland. Although they are not part of the IC, several of DHS's components have

extensive interactions with the IC, including U.S. Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), Transportation Security Administration (TSA), Secret Service (USSS), and Citizenship and Immigration Services (CIS).

Army, Navy, Air Force, and Marine Corps - The intelligence components of the Army, Navy, Air Force, and Marine Corps collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence to support departmental requirements, and, as appropriate, national requirements.

They also conduct counterintelligence activities; monitor the development, procurement, and management of tactical intelligence systems and equipment, and conduct related research, development, and test and evaluation activities.

They maintain military intelligence liaison relationships and military intelligence exchange programs with selected cooperative foreign defense establishments and international organizations.

Coast Guard - The intelligence elements of the Coast Guard support Coast Guard tactical and operational commanders, strategic planners, and decision makers. In addition, the Coast Guard supports the IC, Department of Homeland Security, and federal, state, local, tribal, and foreign partner agencies by providing objective, thorough, accurate, timely, usable, relevant intelligence about the maritime domain, potential threats, and adversaries' capabilities, limitations, and intentions.

EO 12333 includes direction specific to the Coast Guard, stating its national intelligence element shall:

- Collect (including through clandestine means), process, analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support departmental and national missions.
- Conduct counterintelligence activities.
- Monitor the development, procurement, and management of tactical intelligence systems and equipment, and conduct related research, development, and test and evaluation activities.
- Conduct foreign intelligence liaison relationships and intelligence exchange programs with foreign intelligence services, security services or international organizations.

The Coast Guard's Separation of National Intelligence and Law Enforcement Intelligence Elements

In addition to the authority prescribed in EO 12333 described earlier, the Coast Guard collects information of potential intelligence value using its law enforcement and regulatory authorities. The uniqueness of these separate types of authorities necessitates the division of Coast Guard intelligence personnel into two elements: the National Intelligence Element (NIE) and the Law Enforcement Intelligence Element (LEIE). Coast Guard personnel assigned to each of these elements provide intelligence support to the Coast Guard, the Department of Homeland Security, and the IC. Using proper classification and handling procedures, intelligence from one element can be shared with the other.

The Coast Guard's National Intelligence Element - The National Intelligence Element (NIE) consists of ONLY those intelligence components and billets designated by the Assistant Commandant for Intelligence and Criminal Investigations, Commandant (CG-2), as IC resources as established under the National Security Act of 1947, as amended (50 U.S.C. 401 et seq.), and are subject to Executive Order 12333, United States Intelligence Activities, as amended. Included in the NIE are Coast Guard Cryptologic Group personnel who operate in accordance with authorities, policies, and procedures of the U.S. Signals Intelligence System and Coast Guard Counterintelligence Service personnel. Commandant (CG-21) maintains a listing of Coast Guard NIE billets.

The crew of Coast Guard Cryptologic Unit Texas during commissioning ceremony at the Alamo.

The Coast Guard's Law Enforcement Intelligence Element - The Law Enforcement Intelligence Element (LEIE) consists of intelligence personnel who plan, direct, collect, report, process, exploit, analyze, produce, and disseminate information pursuant to Coast Guard law enforcement and regulatory authorities. Most Coast Guard intelligence personnel are in the LEIE. Because LEIE

personnel operate pursuant to Coast Guard law enforcement and regulatory authorities, they follow policies and procedures mandated in U.S. Coast Guard Maritime Law Enforcement Manual (MLEM), COMDTINST M16247.1 (series) and the Marine Safety Manual (MSM), COMDTINST M16000.12 (series). All intelligence personnel should have a working knowledge of these manuals. Properly operating pursuant to law enforcement and regulatory authorities, LEIE personnel may obtain information which has value to U.S. intelligence agencies (including the Coast Guard National Intelligence Element). This type of information is forwarded to the IC through appropriate and timely dissemination.

Other Intelligence Partners

In addition to working with other members of the IC to meet national intelligence requirements, Coast Guard intelligence personnel also interact regularly with other national, regional, state, local, and tribal law enforcement and intelligence entities. These include Joint Terrorism Task Forces (JTTFs), and State and Local Fusion Centers.

Sector Detroit intelligence staff host a conference for international, national, state, local, and tribal intelligence and law enforcement partners.

Chapter Three

Coast Guard Intelligence

History of Coast Guard Intelligence

Coast Guard intelligence has its formal roots in the 1915 assignment of a Chief Intelligence Officer at Coast Guard Headquarters. According to Coast Guard Regulations of the time, the duties of that officer included the securing of information which was essential to the Coast Guard in carrying out its duties; disseminating this information to responsible officers, operating units of the Coast Guard, the Treasury Department and other collaborating agencies; and maintaining adequate files and records of law enforcement activities.

During the 1920s and 1930s, a combination of novel use of human sources, cryptology, and dedicated investigative tactics brought about tremendous operational success in the battle to interdict illegal rum runners and other smuggling activities. Known as the "Father of Coast Guard Intelligence," Admiral Frederick C. Billard, Commandant of the Coast Guard from 1924 to 1932, grew the nascent office to approximately 50 billets and established an intelligence center and intelligence stations. Coast Guard intelligence provided direct support to operations including equipping a Coast Guard patrol boat as the first U.S. signals intercept ship, innovatively fusing human-source intelligence and imagery, and employing an aggressive counter-intelligence campaign against smugglers. Coast Guard intelligence was the core of the Coast Guard's successful reduction by 60 percent of a massive flow of illegal smuggling along the 12,000-mile coastline from 1927 to 1928 to a mere trickle by the end of Prohibition. Elizebeth and William Friedman, both renowned cryptologists and pioneers of early U.S. efforts in this field, were critical in this endeavor. Elizebeth Friedman and one assistant clerk decrypted over 12,000 rum-runner messages in a three-year span, while also contributing to several other legal and law enforcement successes.

William and Elizebeth Friedman, Coast Guard cryptography pioneers.

After a short lull in activity following the repeal of Prohibition, Coast Guard intelligence again made significant homeland security contributions during World War II. Using expertise gained during the Rum War successes, Coast Guard intelligence leaders refocused their cryptologic efforts. While working as part of a U.S. Navy code breaking effort, 23 Coast Guardsmen, led by Lieutenant Commander Leonard T. Jones, independently solved the cipher of the German high command's intelligence service, the *Abwehr*, primarily from transmissions in Latin America, North Africa, and the Far East. This small unit, designated "CG Unit 387" included Elizebeth Friedman and 12 SPARs (the name for the Coast Guard Women's Reserve during World War II, taken from the Coast Guard Latin motto "Semper Paratus" and its English translation "Always Ready"). Between 1941 and 1943, CG Unit 387 intercepted more than 10,000 encrypted messages from 65 different German clandestine circuits, of which approximately 8,500 were cracked. These accomplishments were critical to Allied operational success in the war. Their assignments were also a reflection of the viewpoint of the senior officer of the group, Captain Joseph Farley (a future Coast Guard Commandant). Captain Farley felt that those with maritime expertise were best suited to lead the maritime-related code breaking efforts rather than the FBI, which had attempted to take over the endeavor. His perspective reflects the thinking in the Service then, like now, that the missions the Coast Guard conducts during war or other crises require little or no adapting from its peacetime operations, as they draw from centuries of experience in those missions.

In the Pacific Theater, Coast Guard code breaking skills and overall knowledge of Japanese *maru* (merchant) ships similarly led to deciphering the codes used by those vessels, and ultimately the codes used by the Japanese military. These phenomenal successes were the result of pre-war and wartime Coast Guard intercepts and deciphering of Japanese *maru* weather and position reports, and the contributions of specialists such as USCG Lieutenant Commander Henry M. Anthony. As an expert on merchant ship communications, he was instrumental in aiding the U.S. Navy's Fleet Radio Unit, Pacific (FRUPac) with its major code breaking gains. Such communications intelligence directly contributed to half of the U.S. submarine sinkings of Japanese ships in the Pacific Theater,

and again demonstrated the relevance of Coast Guard peacetime expertise and competencies in times of national crisis.

Other Coast Guard intelligence contributions during World War II similarly drew from the Service's strengths and missions. Domestically, Coast Guard investigators and members of a newly created Intelligence Specialist rating (which was given the designator X to identify it) screened potential service members and merchant mariners, and worked closely with Captains of the Port to monitor suspicious and high threat merchant vessels. Intelligence personnel led human-source intelligence and counterintelligence efforts to prevent port sabotage and espionage, while also disseminating intelligence on port and coastal threats posed by U-boats and their landing parties. Despite many attempts by German saboteurs, Coast Guard intelligence and related port security efforts foiled all such attacks.

The Coast Guard also established a close relationship with maritime special operations forces. A great majority of the Office of Strategic Services (OSS – predecessor to the CIA) Maritime Unit and Operational Swimmer Detachments consisted of Coast Guard personnel, and several of the U.S. Navy's first frogmen (predecessors to U.S. Navy SEALs) were Coast Guardsmen assigned to Underwater Demolition Team X in the Pacific. Coast Guard experts in the maritime domain such as small boat coxswains were also in high demand. During the war, these groups conducted intelligence, surveillance, reconnaissance, sabotage, and espionage operations in the maritime domains of the European, Mediterranean, Chinese, Burmese, Indian, and Pacific Theaters.

Following World War II, Coast Guard intelligence contracted until the late 1970s. At that time, growing intelligence requirements to counter marijuana and cocaine maritime smuggling to the U.S. and the 1980 *Mariel* Boatlift from Cuba dictated the need for a more robust and structured effort. During the 1970s and 1980s, the Coast Guard established a program management office at headquarters; a national all-source analysis and indications and warning center (the Intelligence Coordination Center); theater-level intelligence staffs at both the Atlantic and Pacific Area commands; and tactically-focused district intelligence staffs, including the Maritime Intelligence Center in Miami, Florida. Other liaison, Joint Task Force, El Paso Intelligence Center, and accredited Defense Attaché System positions were created to facilitate information sharing and the contributions of Coast Guard maritime expertise. More robust intelligence support to Coast Guard

Former Coast Guard Commandant Thad Allen, then Lt. Allen, receives an award after serving at the El Paso Intelligence Center.

operations was further warranted as drug smugglers employed increasingly sophisticated methods to transport their products, and as other threats expanded, such as alien smuggling from Haiti, Cuba, the Dominican Republic, China, and Ecuador, and foreign fishing vessel incursions into U.S. fishing grounds.

As its use of intelligence expanded during the 1980s and 1990s, the Coast Guard incorporated numerous aspects of the other military intelligence programs. Examples include use of the Intelligence Information Report (IIR) format for reporting, centralized collection management, use of Department of Defense training and professional education, and the acquisition of IC funding (General Defense Intelligence Program) in order to become more compatible with IC members. Even with this growth and maturing structure, the Coast Guard had only a little more than 200 full-time intelligence billets until the early 21st century. Nonetheless, Coast Guard intelligence professionals provided critical intelligence by warning of Haitian and Cuban mass migrations, tipping and cueing several high-profile Chinese migrant smuggling attempts, and supporting the detection and interdictions of foreign fishing vessels in the U.S. Exclusive Economic Zone and those in violation of international fishing protocols.

Graduates of the first Intelligence Specialist 'A' School at TRACEN Yorktown.

Following a multi-year planning endeavor by the Coast Guard, and members and staff on the House Permanent Select Committee on Intelligence, the Coast Guard became a formal member of the IC on 28 December 2001. In 2001, an amendment to the National Security Act of 1947 added the National Intelligence Element of the Coast Guard, bringing additional authorities, access to intelligence funding, influence within the IC, as well as numerous oversight requirements. Shortly thereafter, the Coast Guard created two Maritime Intelligence Fusion Centers, formed the Coast Guard Cryptologic Group, stood up the Coast Guard Counterintelligence Service, established intelligence staffs at Sectors, professionalized the intelligence workforce by instituting the Intelligence Specialist (IS) enlisted rating and the Intelligence Systems Specialist (ISS) Chief Warrant Officer specialty, initiated the COASTWATCH screening effort, and developed the Maritime Homeland Threat Analysis Division (MHTAD).

As of 2010, the Coast Guard has more than 1,000 intelligence billets.

Components of Coast Guard Intelligence

Coast Guard intelligence personnel are integrated into Coast Guard commands at every level. Groups of intelligence personnel attached to a unit comprise an "intelligence component." Intelligence components vary in size from the more than 100 members of the Intelligence Coordination Center, which is commanded by a Captain, to a two-person Sector Intelligence Staff led by a junior officer. Additionally, all Coast Guard intelligence personnel are divided into either the Law Enforcement Intelligence Element or the National Intelligence Element, described in the previous chapter. Regardless of their size, Coast Guard intelligence components bring three unique and critical characteristics to the intelligence and law enforcement communities: Maritime Access, Maritime Emphasis, and Maritime Expertise.

The following are descriptions of the Coast Guard major intelligence components.

Assistant Commandant for Intelligence and Criminal Investigations Directorate, Coast Guard Headquarters (CG-2) - Commandant (CG-2) supports the Assistant Commandant for Intelligence and Criminal Investigations* through planning, policy, programming, budgeting, training, security, and information systems support related to Coast Guard intelligence. Commandant (CG-2) also conducts oversight of Coast Guard intelligence components in conjunction with the Chief Counsel to ensure intelligence functions fully comply within the law. Commandant (CG-2) serves as the primary interface between the Coast Guard and the IC for policy, program, budget, planning, and oversight matters. Commandant (CG-2) manages all aspects of intelligence activities for force readiness. Commandant (CG-2) coordinates foreign disclosure of intelligence information, manages Sensitive Compartmented Information Facilities (SCIFs), and converts Coast Guard intelligence policies to doctrine, tactics, techniques, and procedures. The following components within Commandant (CG-2) are responsible for specific aspects of the Coast Guard's intelligence efforts.

** Operating under the authority delegated by the Commandant, the Assistant Commandant for Intelligence and Criminal Investigations is responsible for the overall function of Coast Guard intelligence. The Assistant Commandant also provides direction and management for Coast Guard intelligence components, serves as the principal advisor to the Commandant on intelligence matters, and acts as the Head of Element of the Intelligence Community, as set forth in EO 12333 and ODNI policy, for the Coast Guard National Intelligence Element.*

Coast Guard Investigative Service (CGIS) - CGIS is a federal investigative and protective program established to carry out the Coast Guard's internal and external criminal investigations, assist in providing personal security services, protect the welfare of Coast Guard people, aid in preserving the internal integrity of the Coast Guard, and support Coast Guard missions worldwide. Comprised of both civilian and military personnel, CGIS Special Agents can provide critical intelligence support to the Coast Guard through source information, undercover investigations, and through working relationships with other law enforcement investigators.

Coast Guard Counterintelligence Service (CGCIS) - CGCIS preserves the operational integrity of the Coast Guard by shielding its operations, personnel, systems, facilities and information from Foreign Intelligence and Security Services (FISS), and the intelligence efforts of terrorist organizations, drug trafficking elements and other organized crime groups, and adversaries, and insider threats. CGCIS supports the identification, understanding, neutralization, and exploitation of the operations of FISS and of non-state actors who employ intelligence tradecraft. CGCIS manages the Foreign Visitor Program, providing tailored foreign intelligence threat and awareness briefings specific to foreigners visiting Coast Guard commands. CGCIS also conducts foreign travel briefs and debriefs, providing tailored foreign intelligence threat and awareness briefings on FISS, terrorism, and criminal threats, and health concerns to educate Coast Guard personnel traveling to high-threat countries.

Coast Guard Cryptologic Group (CGCG) - CGCG provides a unique maritime cryptologic perspective within the SIGINT community, helping to satisfy validated national SIGINT requirements, which also support Coast Guard and DHS missions. CGCG brings cryptologic capabilities and full interoperability with U.S. Navy and U.S. Cryptologic assets to enhance Maritime Domain Awareness for operational commanders as they plan and execute Coast Guard missions.

Intelligence Coordination Center (ICC) - The ICC is the Coast Guard's strategic level intelligence analysis and production center. The ICC is responsible for analysis and production in response to the Commandant's Priority Intelligence Requirements and all headquarters-level intelligence requirements regarding the broadest aspects

of national and service policy and actions. The ICC manages all collection requirements, tasking, and requests for information that pass between the Coast Guard and IC partners.

Area Commander's Intelligence Divisions - The Atlantic and Pacific Area Commander's Intelligence Divisions manage all aspects of intelligence activities within their area of responsibility and of subordinate units. They direct the Area Commander's intelligence assets and the intelligence capabilities provided to the Area Commander in a supporting role, to achieve maximum support to Coast Guard mission execution. The Intelligence Divisions coordinate intelligence support to the Coast Guard's Standard Operations Planning Process (SOPP) for force allocation and Global Force Management (GFM), maintain an integrated, real-time, accurate Common Intelligence Picture in support of the Area Commander's Common Operational Picture, and provide optimal integration and coordination with interagency partners, the private sector, and international partners. They also coordinate headquarters, operational, and tactical intelligence component alignment with operational and contingency planning. The Intelligence Divisions oversee the following Coast Guard intelligence components.

Maritime Intelligence Fusion Centers (MIFCs) - MIFCs serve as the central hub for fusion, analysis, and dissemination of maritime intelligence and information at the operational and tactical level. They provide tactical intelligence support to the District and Sector Intelligence Staffs, and to Command Intelligence Officers in their area. MIFCs specifically focus on intelligence support to targeting, technical intelligence capabilities, and analytical reach back. Field level commands determine the periodicity, level of detail, and topics for MIFC intelligence analysis and production. MIFCs also provide the Operational Commander's Intelligence Division with analysis and production that supports the Standard Operations Planning Process. By serving as the conduit for production and requirements flowing in and out of their commands, they provide timely response for supported components.

District Intelligence Staff (di/dri) - The District Intelligence Staff performs each phase of the intelligence cycle to varying degrees. It supports the District Commander, provides value-added information for reports produced within the District, sensitizes operations personnel to intelligence priorities and collections requirements, performs law enforcement intelligence collection, and serves as collection manager for assets in the District.

It defines and meets the District Commander's intelligence needs, provides guidance and oversight to Sector intelligence staffs, serves as the conduit for production and requirements flowing in and out of the District. In addition, the District Intelligence Staff is comprised of subject matter experts on maritime adversaries and the means in which they exploit the maritime domain. The Chief of the District Intelligence Staff is the primary intelligence advisor to the District Commander and is a subject matter expert in the integration of intelligence into Coast Guard operations and the application of Coast Guard intelligence policy, doctrine, and tactics, techniques, and procedures within the District.

Sector Intelligence Staff (Si) - The Sector Intelligence Staff performs each phase of the intelligence cycle to varying degrees. It supports the Sector Commander, provides value added information for reports produced within the Sector, sensitizes operations personnel to intelligence priorities and collections requirements, performs law enforcement intelligence collection, and serves as collection manager for the assets in the Sector. It defines and meets the Sector Commander's intelligence needs, provides guidance and oversight to Command Intelligence Officers, serves as the conduit for production and requirements flowing in and out of the Sector, and consists of subject matter experts on maritime adversaries and the means in which they exploit the maritime domain. The Chief of the Sector Intelligence Staff is the primary intelligence advisor to the Sector Commander.

Intelligence staff in front of a seized 41 foot "super *yola*" in San Juan, Puerto Rico, after the vessel was interdicted in the Mona Pass with 245 nationals from the Dominican Republic on board.

Command Intelligence Officer (CIO) - CIOs are collateral duty law enforcement intelligence personnel who are responsible for all phases of the intelligence process that apply to the member's command. The CIO works for the unit commander but may receive guidance, advice, and support from the servicing intelligence staff. The Commanding Officer or Officer-in-Charge is ultimately responsible for the unit's intelligence efforts.

Chapter Four

Principles of Coast Guard Intelligence Operations

Intelligence Alignment with Operations

The Principles of Coast Guard Intelligence Operations derive from the Principles of Coast Guard Operations contained in *U.S. Coast Guard: America's Maritime Guardian, Publication 1.*

The Principles

- ***Clear Objective***
- ***Effective Presence***
- ***Unity of Effort***
- ***On Scene Initiative***
- ***Flexibility***
- ***Managed Risk***
- ***Restraint***

The Principle of Clear Objective

Direct every intelligence operation or activity toward a clearly defined and obtainable objective or requirement. The principal objectives of Coast Guard intelligence are to:

Drive Coast Guard mission execution. This includes providing timely, actionable, and relevant intelligence to Coast Guard commanders and operating forces. Coast Guard intelligence components exist to provide decision advantage to Coast Guard commanders, operating forces, and senior leaders to drive mission execution across the spectrum of operations. The end result of a Coast Guard intelligence operation or activity is a decision or action by Coast Guard personnel.

Provide timely, actionable, and relevant intelligence to Department of Homeland Security components to prepare, prevent, and respond to threats and accomplish the mission. The Coast Guard collaborates with other Department of Homeland Security (DHS) intelligence components to provide the same decision advantage to DHS leadership and operating elements to achieve homeland security missions.

Provide timely and relevant intelligence in response to national intelligence requirements in support of national security objectives. National security objectives are set by the President and National Security Council, and translated by the Director of National Intelligence and IC into national intelligence requirements. The Coast Guard provides timely intelligence gathered by Coast Guard forces in response to national intelligence requirements in support of national security objectives.

The Principle of Effective Presence

Deliver the right information to the right customer at the right time.

Intelligence is responsive to requirements. Precise knowledge and understanding of customer requirements are essential to developing and achieving the objective. Coast Guard intelligence personnel must actively engage, communicate, and educate Coast Guard and other consumers about the intelligence profession, the intelligence cycle, and their role in the requirements process.

Intelligence must not only answer the substance, but be delivered in the form and at the appropriate classification for use by the customer. Where possible, Coast Guard commands will appropriately sanitize, downgrade, or declassify intelligence to ensure broadest dissemination to customers, while at all times protecting intelligence sources and methods from compromise.

Coast Guard personnel from the Defense Attache Office Bogota prepare to depart on the embassy's C-12.

Coast Guard intelligence components represent Coast Guard interests within the IC, and on intelligence matters within the Department of Homeland Security,

Department of Defense, and other agencies, through liaison officers and detailees, the Coast Guard Cryptologic Group, the Coast Guard Counterintelligence Service, and other NIE billets. The Coast Guard leverages those personnel to forge stronger alliances with other departments and agencies to communicate Coast Guard requirements, promote cooperation, and share information.

Intelligence must have an effective presence in the field. The Coast Guard maintains this through District and Sector Intelligence Staffs, Command Intelligence Officers, Coast Guard Investigative Service Special Agents, and deployed intelligence officers and specialists. Coast Guard commands collect and report intelligence and other information in the port and coastal areas, where other organizations have limited capability.

The National Maritime Intelligence Center, located in Suitland, Md.

Effective management of intelligence resources ensures intelligence is delivered at the right cost. The Coast Guard plans, programs, and budgets Coast Guard intelligence operations using IC, Department, and Coast Guard resources. The Coast Guard actively engages the Department, Director of National Intelligence, and congressional intelligence committees on intelligence issues.

The Principle of Unity of Effort

Describes cooperative effort among different units, under positive leadership, to achieve the objective. This requires leadership to provide a clear understanding of the objective and the role each individual, unit, or organization is expected to play in meeting the objective and embodies the concept of "chain of command."

Unity of effort requires the assignment of specific roles and responsibilities among Coast Guard commands to ensure focused effort to achieve the objective.

The Assistant Commandant for Intelligence and Criminal Investigations is accountable to the Commandant for achieving the Coast Guard's intelligence objectives, and is also accountable to the DNI for the activities of the Coast Guard's National Intelligence Element. The Coast Guard establishes performance standards, measures success and effectiveness in meeting objectives against those standards, and strives to improve.

Coast Guard commands should align tactics, techniques, and procedures under an umbrella of policy and doctrine to ensure standardization of best practices.

Coast Guard commands should rapidly and appropriately share information within the Coast Guard, Department of Homeland Security, Department of Defense, IC, and other departments and agencies to the greatest extent possible, with due regard for protection of intelligence sources and methods from unauthorized disclosure. In addition, the Coast Guard's unique position as the primary executor of U.S. military, law enforcement, and regulatory authorities along the nation's maritime boundaries, Coast Guard commands should endeavor to produce unclassified or sensitive-but-unclassified reports which operators can easily share, to the greatest extent possible and within the law, with their mission partners in state, local, and tribal law enforcement, as well as those in the international community and private sector.

An Intelligence Officer from the Fourteenth District meets foreign dignitaries in Pohnpei, Federated States of Micronesia, during a Law Enforcement Roundup.

Coast Guard operating forces, especially those assigned to response and prevention functions, have unique access and expertise in the maritime domain. Typically, these operating forces are better positioned to collect information of potential intelligence value than are the comparatively smaller number of intelligence personnel. Therefore, a primary responsibility of intelligence staffs is to sensitize their operational counterparts to collection opportunities and requirements. Armed with this knowledge, every single Guardian is capable of observing and reporting information that may be valuable to executing the Coast Guard's missions: "Every Guardian is a sensor."

The Principle of On Scene Initiative

Allows Coast Guard intelligence personnel to take the initiative on matters (guided by a firm understanding of the desired objectives, national interests at stake, and scope of authority) without waiting for specific direction from higher levels in the chain of command. This concept requires communication of the commander's intent, which conveys the objective and desired course of action, and communication of a concept of operations. This details the commander's estimated sequence of actions to achieve the objective and contains essential

elements of a plan (i.e., what is to be done and how the commander plans to do it).

The Coast Guard deploys intelligence forces forward, whenever possible, directly to support the customer to shape Coast Guard decisions and operations to achieve mission execution.

The Coast Guard encourages innovation and development of new practices, and adopts as standards those ideas which improve mission success.

The Assistant Commandant for Intelligence and Criminal Investigations designates intelligence components as executive agents to represent the Coast Guard on specific issues.

The Principle of Flexibility

The ability to respond in a timely manner to a wide variety of circumstances and mission requirements.

The Coast Guard rapidly responds to meet changes in objective or intelligence requirements. This includes maintaining the agility to prioritize new or changing requirements and to surge capability when necessary to ensure mission success.

Sustainability demands flexibility. The Coast Guard evaluates the impact of changes in mission on existing demands and resources, plans for sustainability of effort, and takes necessary actions to ensure achievement of priority objectives.

The Principle of Managed Risk

USCG Attache instructing international partners on Risk Management.

The obligation to ensure that personnel engaged in intelligence duties or activities are properly trained, equipped, and sustained for the mission, and that appropriate security measures are implemented to protect classified information, sensitive-but-unclassified information, and intelligence sources and methods from unauthorized disclosure.

Intelligence is a profession with unique competencies which requires a highly-trained workforce. The Coast Guard strives to deliver the best training and

performance improvement solutions to ensure personnel possess the knowledge, skills, and ability to achieve the objective.

The protection of intelligence sources and methods from unauthorized disclosure is an overriding imperative. Coast Guard commands should produce intelligence in a way that balances the need for maximum utility of the information to the intended recipient with certain protection of intelligence sources and methods. The Coast Guard develops policy and procedures for use of intelligence to ensure security of classified and sensitive information, and protection of intelligence sources and methods.

Coast Guard commands actively assist in the management of personnel security to ensure only appropriate personnel have access to classified and sensitive information. The Coast Guard manages the special security function consistent with Director of National Intelligence policy.

Coast Guard commands should actively participate in Coast Guard information assurance (including information, operations, and communications security) operations to ensure security of information systems.

Coast Guard commands should actively participate in Coast Guard cyberspace activities, including Computer Network Operations, in coordination with Department of Homeland Security and IC efforts.

The Principle of Restraint

The special obligation to exercise power and authority prudently and with restraint.

Coast Guard commands should exercise authority with restraint and in full compliance with the law, IC directives, and Coast Guard policy. This typically includes ensuring the full participation of Coast Guard legal advisors in the planning and execution of intelligence activities to achieve the objective with due regard for the law.

The Coast Guard National Intelligence Element strictly adheres to the letter and spirit of laws and regulations governing the conduct of intelligence activities, including Coast Guard implementing procedures approved by the Attorney General and Director of National Intelligence.

All Coast Guard Law Enforcement Intelligence Element activities and functions strictly adhere to the letter and spirit of the laws and regulations governing authority, jurisdiction and operations.

The Coast Guard creates and maintains a rigorous oversight function to ensure compliance. Coast Guard commands should conduct regular internal review and welcome external oversight.

USCGC Waesche (WMSL-751), one of the new National Security Class cutters, has organic intelligence components.

Coast Guard Publication 2-0 is not intended to, and does not, create any right, benefit, or standard, substantive or procedural, enforceable at law or in equity, by any party against the Coast Guard or the United States of America, its officers, employees, or agents, or any other person. The high expectations of performance contained in Coast Guard Publication 2-0 are intended to encourage public service above and beyond the minimum threshold of due care that might apply in a non-governmental context. Any requirements or obligations created by Coast Guard Publication 2-0 flow only from Coast Guard personnel to the Coast Guard, and the Coast Guard retains the discretion to deviate or authorize deviations from these requirements. Coast Guard Publication 2-0 creates no duties or obligations to the public to comply with procedures described herein, and no member of the public should rely on Coast Guard Publication 2-0 as a representation by the Coast Guard as to the manner of performance of our missions.