Sharing the wealth—Coast Guard Law Enforcement Information Valuable to the National Intelligence Effort or How the Coast Guard Defeats the Wall

*Commander Peter J. Clemens**

The 9/11 Commission Report identified information sharing paucity within and between agencies of the federal government as a critical gap in the "back office" side of government operations.[1] Other commissions have identified the need to improve information sharing,[2] and Congress has passed several provisions that enable greater sharing of specific types of information.[3] Recognizing that information sharing is sometimes challenging but always rewarding, the Coast Guard has provided clear guidance enabling the sharing of information obtained during law enforcement and other operations with the national intelligence community. Likewise, this guidance enables intelligence originating from the intelligence community to be shared with operational commanders engaged in law enforcement.

The Coast Guard intelligence program has established a process to systematically review information reported from the field for national intelligence value. This process is designed to implement statutory requirements and improve the information's availability across the intelligence community. Unique among the nation's armed forces, the Coast Guard relies on a variety of statutory authorities to obtain information. The authority relied on, and the regulations specific to the information management system, dictate the authorized dissemination of the collected information. This article is narrowly focused on the legal basis for information sharing between the law enforcement and intelligence programs. This separation was often referred to as a "wall"[4] perceived to exist between intelligence activity and law enforcement activity. Although a wider world of information sharing exists within the rubric of maritime domain awareness, that wider world is not the focus here.

Background

The Coast Guard intelligence element became part of the intelligence community when President Bush signed the Intelligence Authorization Act of 2002 into law.[5] The authority to conduct intelligence activities, as contemplated by the National Security Act of 1947,[6] was added to the tool box of Coast Guard authorities enabling maritime missions that protect the nation from all hazards and threats found in the maritime environment. As the Coast Guard was developing its policies and procedures in 2002 and 2003 to guide the use of its newly acquired intelligence authorities,[7] the "wall,"[8] erected by court opinions[9] and related U.S. Department of Justice (DOJ) practice and opinions,[10] retained some vitality in at least confusing if

---

* Currently assigned as Chief, Legal division, Maintenance and Logistics Command Pacific–MLCPAC(1), Coast Guard Island, Cal.. The author would like to thank Lieutenant J. Trent Warner, Center for Law and Military Operations, The Judge Advocate General's Legal Ctr. and Sch., for his footnoting assistance and editing of this article.

[1] FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES § 13.3 "Unity of Effort in Information Sharing" (2004) [hereinafter FINAL REPORT].

[2] *See, e.g.*, THE COMMISSION ON THE INTELLIGENCE CAPABILITIES OF THE UNITED STATES REGARDING WEAPONS OF MASS DESTRUCTION, REPORT TO THE PRESIDENT OF THE UNITED STATES, Conclusion 20 (2005), *available at* http://www.wmd.gov/report/wmd_report.pdf.

[3] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) of 2001, Pub. L. No. 107-296, § 905, 115 Stat. 272 [hereinafter USA PATRIOT ACT]; Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135; Intelligence Reform and Terrorism Prevention Act (Intelligence Reform Act) of 2004, Pub. L. No. 108-458, 118 Stat. 3638 [hereinafter 2004 Intelligence Reform Act].

[4] *See* A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS, at 26 (Nov. 2004 – Released June 19, 2006 by the Office of the Inspector General, DOJ) [hereinafter FBI'S INTELLIGENCE HANDLING REVIEW] (quoting a memorandum by Richard Scruggs, Head of the DOJ's Office of Intelligence Policy and Review (OIPR), *available at* http://www.fas.org/irp/agency/doj/oig/fbi-911/chap2.pdf. Apparently, it was Scruggs who first used the phrase "Chinese Wall" to describe the separation between the Intelligence and Law Enforcement communities. *Id.*

[5] Intelligence Authorization Act (IAA) for Fiscal Year 2002, Pub. L. No. 107-108, 115 Stat. 1394 (2001) [hereinafter 2002 IAA].

[6] National Security Act (NSA) of 1947, Pub. L. No. 253, 61 Stat. 496 (1947) [hereinafter 1947 NSA]. Specifically, section 105 of the 2002 IAA amended the 1947 NSA to include the Coast Guard within the intelligence community, (50 U.S.C. § 401a(4)(H)), and section 1073 of 2004 INTELLIGENCE REFORM ACT amended 50 U.S.C. § 401a(4)(H) to § 401a(4)(K).

[7] *See* 2002 IAA, *supra* note 5.

[8] *See* FBI'S INTELLIGENCE HANDLING REVIEW, *supra* note 4.

[9] *See id.* at 22–24 (quoting United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980) (articulating that the "primary purpose test" when it construed the FISA warrant application "purpose" certification requirement. The original test required only that the government certify that the information sought

not actually limiting information sharing between law enforcement and intelligence personnel.[11] The Coast Guard was challenged to construct a process that recognized the differences in authority and the related rules associated with those authorities without creating an impassible or restrictive barrier. Information is a necessary ingredient in planning and performing enforcement operations. Additionally, due to the nature of the maritime environment, information obtained during routine Coast Guard operations is often uniquely valuable to the intelligence community. This information can support intelligence community analysis of a number of national security challenges. Information sharing is critical to the efficiency and efficacy of both the recipe to plan and conduct enforcement operations as well as the national intelligence effort.

Intelligence "Collection"

Collection as a verb must be understood in the context of an intelligence discipline. Collection is associated with reliance on intelligence authority, describing the conduct of intelligence activity with the objective to obtain information (e.g. collect intelligence) about the operating environment, the adversary, and the adversary's plans and intentions.[12] The term "collection" also refers to the narrower arena of human intelligence (HUMINT) collection. Although collection occurs via other means, the Coast Guard process discussed in this article does not affect other technology reliant collection disciplines. Collection in this sense can be contrasted against traditional law enforcement questioning which generally relies on seizure analysis under the Fourth Amendment.[13] The Coast Guard has the authority to conduct intelligence collection[14] as well as the authority to perform law enforcement questioning.[15] The collection legal analysis requires a two step inquiry: (1) is the information physically possessed, and (2) is continued possession intended to further an intelligence purpose?[16] Limitations on this authority are found in Executive Order 12,333, guidelines that implement Executive Order 12,333 within the agency,[17] as well as the Fourth Amendment, related case law, and other applicable law.[18] This two step analysis is critical to ensure that the limitations on intelligence authority do not become a barrier to conducting legitimate review of the material.

---

was foreign intelligence. However, the *Truong* court added the additional requirement that the information sought be for the "primary purpose" of collecting foreign intelligence.)) "However, the court ruled that the government's primary purpose in conducting an intelligence investigation could be called into question when prosecutors had begun to assemble a prosecution and had led or taken on a central role in the investigation." *Id.* at 23; *see also* United States v. Johnson, 952 F.2d 565 (1st Cir. 1991) (applying the "primary purpose test" language in its decision).

[10] *See, e.g.*, Memorandum from Janet Reno, U.S. Att'y Gen., DOJ, to Asst. Att'y Gen. Criminal Div. et al., subject: Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations (July 19, 1995) (setting forth the policy that no information collected regarding foreign intelligence or foreign counterintelligence maybe shared for criminal investigative purposes without first being vetted by the OIPR), *available at* http://www.fas.org/irp/agency/doj/fisa/1995procs.html; *see also* Memorandum from Larry D. Thompson, U.S. Att'y Gen., DOJ, to Michael Chertoff, Asst. Att'y Gen. et al., subject: Intelligence Sharing, (Aug. 6, 2001) (reconfirming the DOJ's 1995 policies and procedures regarding information sharing between the intelligence and law enforcement communities), *available at* http://www.fas.org/irp/agency/doj/fisa/dag080601.html.

[11] Kate Martin, *Domestic Intelligence and Civil Liberties*, 24 SAIS REV. (Winter-Spring 2004).

[12] *See generally* U.S. COAST GUARD, COMMANDANT INSTRUCTION MANUAL 3820.12, COAST GUARD INTELLIGENCE ACTIVITIES glossary of terms (28 Aug. 2003) [hereinafter CIM 3820.12] (defining "collection" as "[t]he gathering or receipt of information, regardless of source, by a Coast Guard national intelligence component, coupled with an affirmative act by that component demonstrating intent to use or retain that information for intelligence purposes." CIM 3820.12 also defines "national intelligence" to include "foreign intelligence" which in turn defines "foreign intelligence" as "[i]information relating to the capabilities, intentions, or activities of foreign governments, or elements thereof, or foreign organizations or foreign persons, or international terrorist activities").

[13] *See* Katz v. United States, 389 U.S. 347, 357 (1967) (reviewing the general rule that warrantless searches are unreasonable except for ". . . specifically established and well-delineated exceptions"); *see also* Terry v. Ohio, 392 U.S. 1, 29 (1968) (discussing the fact that law enforcement personnel may, ". . . in light of his experience that criminal activity may be afoot . . ." make inquiries into such conduct). Both cases stand for the basic proposition that law enforcement conduct must conform to the requirements of the 4th amendment, i.e., searches and seizures must be affected by warrant, unless a lawful exception exists, and the search or seizure is reasonable under the circumstances.

[14] *See* 2002 IAA, *supra* note 5.

[15] *See* 14 U.S.C § 2 (2000) ("The Coast Guard shall enforce or assist in the enforcement of all applicable Federal laws, on, under, and over the high seas and waters subject to the jurisdiction of the United States . . ."); *see also* 14 U.S.C. § 89 ("The Coast Guard may make inquiries, examinations, inspections, searches, seizures, and arrests upon the high seas and waters over which the United States has jurisdiction, for the prevention, detection, and suppression of violations of laws of the United States.").

[16] Exec. Order No. 12,333 § 2.3, 3 C.F.R. 200, *amended by* Exec. Order No. 13,355, 69 Fed. Reg, 53,593 (Aug. 27, 2004). *See generally* CIM 3820.12, *supra* note 12, glossary of terms.

[17] Coast Guard Intelligence Activities implement Executive Order 12,333 for the Coast Guard, other IC members must rely on their agency implementing policy for this analysis. *See* CIM 3820.12, *supra* note 12 (setting forth the Coast Guard's implementing instructions of Executive Order 12,333). Other applicable laws include the Foreign Intelligence Surveillance Act (FISA) of 1978, 50 U.S.C. § 1801–1871 (2000) [hereinafter FISA].

[18] *See* FISA, *supra* note 17.

By analogy, intelligence collectors may read the newspaper without limitation; however, if an intelligence collector wants to continue possession of the newspaper to further an intelligence purpose then further evaluation must be conducted to ensure that the authority limitations are complied with prior to actually retaining the information from the newspaper. In this way intelligence collectors may read, or review, information about a U.S. person[19] without violating a proscription from Executive Order 12,333.[20] However, they may not collect that information unless authorized to do so.[21]

Obtaining Law Enforcement Information

The Coast Guard has defined law enforcement intelligence as "information collected, stored, and used by Law Enforcement Intelligence Program personnel or non-intelligence components of the Coast Guard pursuant to Coast Guard law enforcement and/or regulatory authority."[22] In short hand, any information obtained while relying on an authority other than intelligence activity authority qualifies as law enforcement intelligence in the Coast Guard. Routine Coast Guard operations require interaction with a large number of foreign nationals and international travelers who are able to provide information on port conditions and operations. Any information obtained while conducting these routine Coast Guard operations is categorized as law enforcement intelligence.

Navigating the Channel between Law Enforcement and the Intelligence Community

The Coast Guard has the authority to operate in the information paradigms of both the law enforcement and intelligence communities.[23] It is critical to any analysis to recognize, in the first instance, which paradigm you are starting from when attempting to determine how information may be shared with the other paradigm. Knowing the starting point enables application of the necessary legal standards and ensures compliance with related policy requirements. The interface between these communities exists in the Coast Guard at Maritime Intelligence Fusion Centers (MIFC) located both in the Atlantic and Pacific area of operations, as well as at the Intelligence Coordination Center (ICC) located at the National Maritime Intelligence Center (collectively Coast Guard intelligence production centers). The production centers apply law and policy to ensure that the Coast Guard stays in "good water" while navigating this well marked channel. For law enforcement intelligence support personnel, information sharing and the subsequent intelligence derived from that information is focused on supporting Coast Guard enforcement personnel conducting operations. Analysts at the Coast Guard productions centers are challenged to navigate this interface and ensure information is shared between both communities. Analysts review information obtained by Coast Guard field personnel to determine if it may be responsive to national level intelligence requirements. Similarly they are in a position to review products from the intelligence community and bring them to the attention of field commanders who may benefit from those products.

Field personnel report unevaluated intelligence information to the Coast Guard production centers with a field intelligence report (FIR).[24] Field intelligence reports were created specifically to enable units to submit information of potential intelligence value to support Coast Guard missions. Field intelligence reports reflect the full range of Coast Guard maritime activity. These reports can provide domain awareness for port level activity. They can also report responses to questions asked by field personnel during enforcement operations, routine patrols, or other routine interactions with mariners. Field intelligence reports are analyzed to respond to Coast Guard information requirements. Concurrently, they are reviewed at each Coast Guard production center to determine if they meet national level intelligence needs. Intelligence analysts ensure that appropriate field level reports are available to the intelligence community, navigating this interface requires

---

[19] *See* Exec. Order No. 12,333 § 3.4(i) (defining a "U.S. Person" as a "United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.").

[20] *Id*. § 2.3(a).

[21] *See id.* § 2.3 ("Agencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned. . . ."). Subsequently, the Coast Guard implemented CIM 3820.12 Procedure 2.B.2, *supra* note 12, which states, "[c]ollection of information shall meet the following criteria: . . . [b]e based on a function assigned to that Coast Guard national intelligence component."

[22] U.S. COAST GUARD, COMMANDANT INSTRUCTION 3820.14, POLICY FOR DISSEMINATION AND USE OF INTELLIGENCE INFORMATION (26 Feb. 2003) [hereinafter CI 3820.14].

[23] *See supra* notes 14, 15 and accompanying text.

[24] *See* U.S. COAST GUARD, COMMANDANT INSTRUCTION 3821.15, FIELD INTELLIGENCE REPORTS (20 Feb. 2004) (discussing policies and procedures for the use of FIRs).

knowledge of both the information handling rules associated with Coast Guard law enforcement information and knowledge of the intelligence collection inquiry required to ensure compliance with those policies.

Intelligence Collection

Field intelligence reports that are identified as being responsive to national level intelligence requirements can be collected within the constraints of Executive Order 12,333 guidance.[25] In this analysis the Coast Guard production center analyst acts as a collector and applies the two step collection review to determine if the FIR should be translated into an intelligence information report (IIR). The IIR is the vehicle to share information with the intelligence community. Intelligence information report's are transmitted to a variety of Defense intelligence partners and are available throughout the intelligence community for use within those intelligence production processes.

Practical Application

The narcotics smuggling trade has a long history of innovation.[26] Cocaine originating from South America is transported across, under, and over the maritime separation between North and South America.[27] Recently the narco-traffickers have demonstrated the utility of semi-submersible vessels to transport large amounts of cocaine.[28] This developing capability represents a set of new information requirements for both Coast Guard enforcement operations and Coast Guard intelligence.

Preventing the illegal importation of controlled substances is both a law enforcement challenge and a challenge for the intelligence community. The "war on drugs" has been and will likely continue to be a national priority.[29]

Coast Guard units that have interdicted shipments by semi-submersible have been able to provide information to the intelligence program with FIRs. The FIRs are reviewed at the production centers and, those that contain information responsive to national collection requirements, may be translated into IIR. Additionally, interviews of the suspects operating the semi-submersible vessels have resulted in numerous FIRs, some of which were translated into IIRs.

In an area of operations unrelated to narcotics smuggling, Coast Guard Field Intelligence Support Team (FIST) personnel interview foreign nationals that arrive in domestic ports on foreign flagged vessels.[30] These interviews often result in increased awareness of foreign port conditions. The FIRs originated by these FIST personnel enable focused enforcement efforts by Coast Guard boarding teams as the intelligence program identifies potential risk in the commercial fleets.

Responsive to Legal and Policy Mandates

The mandated information sharing requirements found in the USA PATRIOT ACT,[31] and the Homeland Security Act of 2002[32] are at the core of the memorandum of understanding (MOU) between the intelligence community, the federal law enforcement agencies, and the Department of Homeland Security.[33] This MOU also relies on two attorney general

---

[25] *See* CIM 3820.12, *supra* note 12.

[26] *See generally* Admiral Thad Allen, Commandant, U.S. Coast Guard, Address at the National Press Club (Feb. 8, 2008) (discussing the fact that the drug traffickers have historically moved back and forth from aviation to maritime trafficking as needed. Admiral Allen also recognized the recent rise in the use of semi-propelled, semi-submersibles used to transport narcotics, a trend due largely to the successful maritime drug interdiction efforts of many agencies, including the Coast Guard) (transcript available at http://www.uscg.mil/comdt/speeches/docs/NPC.8%20Feb%202008.pdf, video available at http://cgvi.uscg.mil/media/main.php?g2_itemId=220656).

[27] *Id*.

[28] *Id*.

[29] *Id*.

[30] *See generally* U.S. COAST GUARD, COMMANDANT INSTRUCTION 3831.10, FIELD INTELLIGENCE SUPPORT TEAMS (3 Nov 2006) (discussing policies and procedures governing FIST personnel).

[31] *See* USA PATRIOT ACT, *supra* note 3, §§ 203, 905.

[32] *See* Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 202, 221, 116 Stat. 2135.

[33] Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Homeland Security Information Sharing. This MOU was promulgated by a Director of Central Intelligence memorandum as cover to the MOU

memoranda[34] that implement sections of the USA PATRIOT Act. This tight web of policy guidance predated the National Security Intelligence Reform Act of 2004[35] which created the Information Sharing Environment (ISE).[36] Nonetheless it implements the statutes and forms a solid basis for what the Director of National Intelligence now has labeled the "responsibility to provide"[37] supporting the development of the ISE.

Establishing the FIR as a simple mechanism for field level personnel to report anything perceived to have some intelligence value has enabled the Coast Guard to meet these legal and policy mandates without unduly burdening operators. The Coast Guard production centers bear some of the burden to ensure that information responsive to national intelligence requirements is systematically evaluated and provided to the intelligence community. This process augments the Coast Guard's traditional focus on interagency cooperation at the field level through participation in joint task forces. Joint Interagency Task Forces (JIATF), as well as Joint Terrorism Task Forces (JTTF) and other task forces (e.g. Organized Crime Drug Enforcement Task Force), remain vital to the flow of information between and among federal and non-federal partners. These less formal mechanism continue to be supported by the Coast Guard and the Attorney General guidance makes it clear that formal sharing mechanisms should augment but not replace such arrangements.[38]

The Two Way Street

Coast Guard Commanders also benefit from intelligence information that the Coast Guard Intelligence Program receives from the intelligence community. The Coast Guard policy for use and dissemination of intelligence information guides practitioners in the rules for utilizing all source intelligence at the field level.[39] This policy guides all Coast Guard personnel to applicable legal and policy standards when handling intelligence information.[40] The policy is intended to provide a baseline of knowledge and enable field personnel to avoid unauthorized disclosures of sensitive information.[41]

Conclusion

Rather than focus on the prescriptive formulae represented by the reference to a wall, the Coast Guard program leverages all authorities available to navigate the narrow, but well marked, channel through the shoal waters of sensitive intelligence information use and dissemination. The well marked channel enhances the information flow available to national level decision makers while ensuring Coast Guard personnel adhere to applicable law and policy. Concurrently the Coast Guard extends the use of national intelligence products applicable to Coast Guard operations worldwide and thereby improves the planning and conduct of Coast Guard operations.

---

signed by Attorney General Ashcroft, 4 March 2003; Director of Central Intelligence Tenet, 4 March 2003; and Secretary of Homeland Security Ridge, 28 February 2003. The Department of Defense subsequently entered into the MOU. *Id.*

[34] Memorandum, Attorney General, to Heads of Department Components, subject: Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons (Sept. 23, 2002); Memorandum, Attorney General, subject: Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of Criminal Investigations (Sept. 23, 2002).

[35] 2004 Intelligence Reform Act, *supra* note 3.

[36] *See id.* § 1016a(2)(establishing the concept of ISE. Section 1016a(2) defines ISC as ". . . an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section").

[37] *See* Dir. Of Nat'l Intelligence, U.S. Intelligence Community Information Sharing Strategy 3 (22 Feb. 2008), *available at* http://www.fas.org/irp/dni/iss.pdf ("The DNI has called on the Intelligence Community to transform its culture to one where the 'responsibility to provide' information is a core tenet.").

[38] Memorandum, Attorney General, to Heads of Department of Justice et al., subject: Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation (Sept. 23, 2002).

[39] CI 3820.14, *supra* note 17.

[40] *Id.*

[41] *Id.*