September 2008

Committee on Homeland Security
Report Prepared by the Majority Staff:

Giving a Voice to Open Source Stakeholders: A Survey of State, Local & Tribal Law Enforcement

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
REP. BENNIE G. THOMPSON, CHAIRMAN

Executive Summary

In today's complex and dangerous world, U.S. law enforcement officials, first responders, and the private sector need timely, relevant, and actionable intelligence to secure the Nation against potential threats. Some of this intelligence can be produced with open source information – publicly-available information that can be disseminated quickly to an appropriate audience to meet a specific intelligence requirement. These unclassified intelligence products, derived from aggregated and analyzed information available from sources such as newspapers, periodicals, the Internet, scientific journals, and others can provide law enforcement with the actionable intelligence they need to enhance their capabilities and make tactical decisions about where to deploy their limited resources.

Congress and the President established the Department of Homeland Security (DHS), in part, to improve the sharing of information among Federal, State, and local government agencies and the private sector. Effective information sharing can enhance our Nation's ability to detect, identify, understand, and assess terrorist threats; to better protect our Nation's critical infrastructure; to integrate our emergency response networks; and to link the Federal and State governments.[1] Yet, seven years after the attacks of September 11, 2001, information sharing remains a major homeland security challenge. The DHS approach to this challenge has primarily been focused on providing security clearances to an ever-increasing number of law enforcement personnel and private sector representatives to assure access to classified homeland security information.[2] This approach, all too often, prevents information from being shared with the cops on the beat – the people best-positioned to detect suspicious activities or uncover a terrorist cell. To reach this critical audience, DHS should disseminate open source intelligence because this type of unclassified product can be shared with law enforcement and appropriate partners in the private sector, regardless of whether they have security clearances. Given that the Federal government has at its disposal a nearly limitless amount of unclassified open source information, the potential value of open source intelligence products is enormous. Congress recognized the value of open source information in section 201(d)(21) of the Homeland Security Act of 2002 which requires DHS, whenever possible, to produce and disseminate unclassified reports and analytic products based on open source information.[3]

Open source intelligence products can and should be shared with appropriate Federal, State, local and tribal law enforcement, and the private sector because of their unclassified nature. Unfortunately, DHS has not effectively exploited this type of information to provide essential analytical products. In fact, DHS' efforts have lagged behind the rest of the Federal government. While the Office of the Director of National Intelligence (DNI) and the Central Intelligence Agency (CIA) have each established robust open source programs, DHS – the lead Federal agency responsible for sharing terrorism threat and vulnerability information with State and local law enforcement – has yet to articulate a vision for how it will collect, analyze and disseminate open source information. Seeking to bring about change at DHS, the House of

[1] National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism Related Information Sharing, October 2007, 7.
[2] See *Security Clearances: FBI Has Enhanced Its Process for State and Local Law Enforcement Officials*, GAO-04-596, April 30, 2004.
[3] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

Representatives, on July 30, 2008, approved H.R. 3815, the Homeland Security Open Source Information Enhancement Act of 2008, a bill introduced by Representative Ed Perlmutter (D-CO) and a bipartisan group of Committee Members. This legislation requires the Secretary of Homeland Security to establish an open source program.

The Committee on Homeland Security Open Source Survey ("CHS Open Source Survey") and this report were undertaken at the direction of Chairman Bennie G. Thompson. Specifically, Chairman Thompson charged the majority staff of the Committee on Homeland Security to survey over 350 State, local, and tribal law enforcement officials to better understand their intelligence needs and the potential benefits of an open source program at DHS, in light of other open source activities underway across the U.S. Intelligence Community (IC).

The survey results underscore the need for DHS action to harness open source information to enhance information sharing. Fully 82% of respondents reported that they collect and analyze open source information, with a majority expressing a desire to raise their situational awareness of "all hazards" and an interest in receiving DHS open source products providing that information.[4] Only 50% of respondents, however, reported that DHS open source products met that need.[5] Moreover, 60% of respondents reported that in order to improve matters, DHS needs to establish a robust training program in addition to producing open source intelligence products with actionable recommendations.[6]

The end state that DHS should be striving for is a robust open source program extending across its intelligence components, State, local and tribal law enforcement, fusion centers, and the private sector. Among the program's goals should be to:

- Establish and maintain a baseline of open source capabilities throughout DHS;

- Enable State and local fusion centers to build and develop open source exploitation capabilities and give full access to relevant DHS and IC open source data;

- Leverage the full range of open source information sources to expand and inform analysis and reporting.

[4] CHS Open Source Survey, questions 2 & 3 (February 2008).
[5] Id.
[6] CHS Open Source Survey, questions 15 & 16, (February 2008).

TABLE OF CONTENTS

What is Open Source?

The Intelligence Community (IC) under Intelligence Community Directive 301 defines "open source information" as information that is publicly available and that anyone can lawfully obtain by request, purchase, or observation.[7] Open source information generally falls into four categories: (1) information that is widely available to anyone; (2) commercial data; (3) the expertise of individual experts; and (4) "gray" literature, consisting of written information produced by the private sector, government sources, and academia that is available on only a limited basis.[8] So-called gray literature is typically limited because few copies are produced, the existence of the material is largely unknown, or access to information is not readily available via the Internet.[9] Within these four categories, open source information can include:

- Media sources such as newspapers, magazines, radio, television, and the Internet;
- Public data such as government reports, budgets, demographics, hearing materials, legislative history, press conferences, and speeches;
- Information derived from professional and academic sources such as conferences, symposia, professional associations, academic papers, dissertations and theses, and experts;[10]
- Commercial data such as commercial imagery; and
- So-called "gray literature" such as working papers, discussion papers, unofficial government documents, proceedings, research reports, studies, and market surveys.[11]

Intelligence is generally defined as the finished product that is produced after information is collected, processed, and analyzed.[12] Open source information becomes open source intelligence when available information is collected, analyzed, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence need or requirement.[13]

While there has been progress on defining what open source is and is not within the IC, the findings of the CHS Open Source Survey reflect a growing appreciation and acceptance of open source information and intelligence by State, local, and tribal law enforcement as an important tool to help inform community safety efforts. In fact, when asked if their organization collected and analyzed open source information, 81% of survey participants responded in the

[7] Director of National Intelligence, National Open Source Enterprise, Intelligence Community Directive, Number 301, (July 11, 2006).

[8] Amy Sands, "*Integrating Open Sources into Transnational Threat Assessments*," in Jennifer E. Sims and Burton Gerber, *Transforming U.S. Intelligence*, Washington: Georgetown University Press, 65 (2005).

[9] Id.

[10] See Mark M. Lowenthal, Intelligence, From Secrets to Policy 79, (CQ Press, 2nd Edition 2003).

[11] Sands, *supra* note 8.

[12] Director of National Intelligence, *supra* note 7.

[13] Id.

affirmative.[14] The CHS Open Source Survey found that respondents are using open source information to raise situational awareness and assist in criminal investigations, reflecting a move towards an all-hazards approach to policing.[15] This approach recognizes that the same competencies serve both counterterrorism and the prevention of ordinary crimes; in other words, the response to a terrorist attack often requires the same resources as industrial accidents or natural disasters.[16] Arguing for this approach to policing, the Seattle Chief of Police, R. Gil Kerlikowske, said, "[I]f the law enforcement focus at the local level is only on counterterrorism, you will be unable as a local entity to sustain it unless you are an all-crimes operation, and you may be missing some very significant issues that could be related to terrorism."[17]

As the all-hazards approach to policing gains acceptance among State, local, and tribal law enforcement, there is a corresponding need for more and better open source intelligence products. According to 107 law enforcement officials that responded to the CHS Open Source Survey, open source information is being used as a means to support criminal investigations that are not limited to either their intelligence or counterterrorism activities.[18] The relationship between all-hazards policing and open source intelligence was acknowledged by an official from the Tennessee Fusion Center who said:

> Open source information serves a critical role in State and local fusion center analysis activities. We all rely on the fusing of all sources of information, both open and classified, to conduct analysis and reach judgments as to the various threats to our States and the best means to address the threats. The more advanced our capabilities, the greater our pool of quality information to produce credible products of value for our State leaders, law enforcement and first responder communities as well as our federal partners.[19]

[14] CHS Open Source Survey, question 2, (February 2008).
[15] Id., question 3, (February 2008).
[16] See Eben Kaplan, *Fusion Centers*, Council on Foreign Relations (2007), available at http://www.cfr.org/publication/12689/.
[17] Eric Schmitt and David Johnston, *States Chafing at U.S. Focus on Terrorism*, N.Y. Times, May 26, 2008.
[18] CHS Open Source Survey, *supra* note 14.
[19] Comments of Supervisory Intelligence Officer Steven Hewitt, Tennessee Fusion Center, June 24, 2008 (interview notes on file with author).

Why is Open Source so Important?

> **The need for exploiting open-source material is greater now than ever before…[T]he ever-shifting nature of our intelligence needs compels the IC to quickly and easily understand a wide range of foreign countries and cultures…information often detailed in open source.[20]**
>
> ***-- The Commission on the Intelligence Capabilities of the U.S. Regarding Weapons of Mass Destruction***

Within the Intelligence Community (IC), there is wide recognition of the intelligence value of open source information. In fact, "[t]he collection of foreign intelligence is accomplished in a variety of ways, not all of them either mysterious or secret. This is particularly true of overt intelligence, which is information derived from newspapers, books, learned and technical publications, official reports of government proceedings, radio and television. Even a novel or play may contain useful information about the state of a nation."[21] For example, Soviet newspaper articles were often viewed as intelligence by Central Intelligence Agency (CIA) operatives in the 1950s.[22] By 2005, the RAND Corporation, a non-profit think tank, reported that about 70 to 80 percent of the Nation's intelligence about terrorism and other threats to national security was attributable to open sources – such as the newspaper, media, Internet, public, and [the] community.[23] The remaining 20 to 30 percent was derived from operations-based activities including undercover surveillance, informants, and Federal databases.[24]

Utilization of open source information in intelligence products is supported by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) which states that "[o]pen-source intelligence is a valuable source that must be integrated into the intelligence cycle to ensure that United States policymakers are fully and completely informed."[25] To achieve the full integration of open source information into the intelligence cycle, there needs to be a fundamental change in the way open source information is used. Open source information should be used not simply as a supplement to classified data, but rather as a potential source of valuable intelligence.[26]

There is growing recognition among State, local, and tribal law enforcement officials that open source information can help them keep their communities more secure. In the words of one

[20] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Report, (2005).
[21] Allen Dulles, The Craft of Intelligence, New York: Harper & Row (1963), 55.
[22] See Evan Thomas, The Very Best Men: Four Who Dared: The Early Years of the CIA (New York: Simon & Schuster, 1995), 154.
[23] K. Jack Riley, Gregory F. Treverton, Jeremy M. Wilson, Lois M. Davis, *State and Local Intelligence in the War Terrorism*, RAND Corporation (2005), 41.
[24] Id at 41.
[25] Intelligence Reform and Terrorism Prevention Act (IRTPA), Pub. L. No. 108-458, § 1052, 118 Stat. 3638, (2004).
[26] Congressional Research Service, Report on Open Source Intelligence (OSINT): Issues for Congress, (January 28, 2008), 2.

CHS Open Source Survey respondent, “[o]pen source is often our only resource; the flow of classified information is so restricted that we don’t consider it.”[27] While there will always be a need for products that are based upon classified sources, the proliferation of Internet use and other advanced forms of communication is rapidly leading to an information revolution among terrorists groups – including al-Qaeda, which has demonstrated its ability to use virtual space to recruit, radicalize, plot, and plan.[28] According to former CENTCOM Commander General John Abiziad, “we have to master virtual space where al-Qaeda now operates with impunity in recruiting, proselytizing and plotting and planning. Al-Qaeda's organizing ability in cyberspace is unprecedented.”[29] The sooner the Department of Homeland Security (DHS) recognizes the value in this type of unclassified information, the sooner DHS analysts can analyze it and provide useful open source intelligence to State, local and tribal law partners.

A DHS-led program to analyze open source information could bring a great deal of value to the intelligence products that are passed along to State, local and tribal law enforcement. For instance, DHS could bring to bear the foreign language expertise of its analysts, largely unavailable at the local level, to provide valuable intelligence on potential terrorist activity that may be planned or coordinated online in a virtual environment. Intelligence reports to State, local, and tribal law enforcement agencies, however, need to be based on their intelligence requirements. The reports produced by DHS do not appear to meet this standard. About half of respondents to the CHS Open Source Survey said the classified intelligence reports that they receive from DHS were either “not at all useful” or were “never used,” as illustrated in Figure 1.[30] The vast majority of police and sheriff’s offices around the country do not have security clearances. Doling out such clearances, moreover, would not solve the problem. According to one respondent, “[A]lthough some of our analysts have security clearances, they do not have routine access to classified data systems.”[31] When asked about the DHS’ unclassified products, including the Chief Intelligence Officer’s (CINT) Notes, close to 50% stated that they were either “not at all useful” or they were “never used.”[32] At the same time, there is dissatisfaction about the timeliness of information that is transmitted by DHS. Specifically, the National Governor’s Association (NGA) 2007 Survey of 56 State homeland security advisors found that 44% of respondents were dissatisfied with the timeliness of information coming from DHS.[33] Moreover, only 47% said DHS provided intelligence that was specific enough for their needs.[34] The NGA survey underscores the findings of CHS Open Source Survey – accurate timely and actionable intelligence is not getting to our nation’s first preventers.

[27] Comments of a senior State law enforcement official, (May 2008) (interview notes on file with author).
[28] Arnaud de Borchgrave, “*Networked and Lethal*,” The Washington Times, 18 (September 25, 2007).
[29] Id.
[30] CHS Open Source Survey, questions 19(a) and 19(b), (February 2008).
[31] Id.
[32] Id.
[33] National Governor’s Association, 2007 Homeland Security Directors CHS Open Source Survey (2007).
[34] Id.

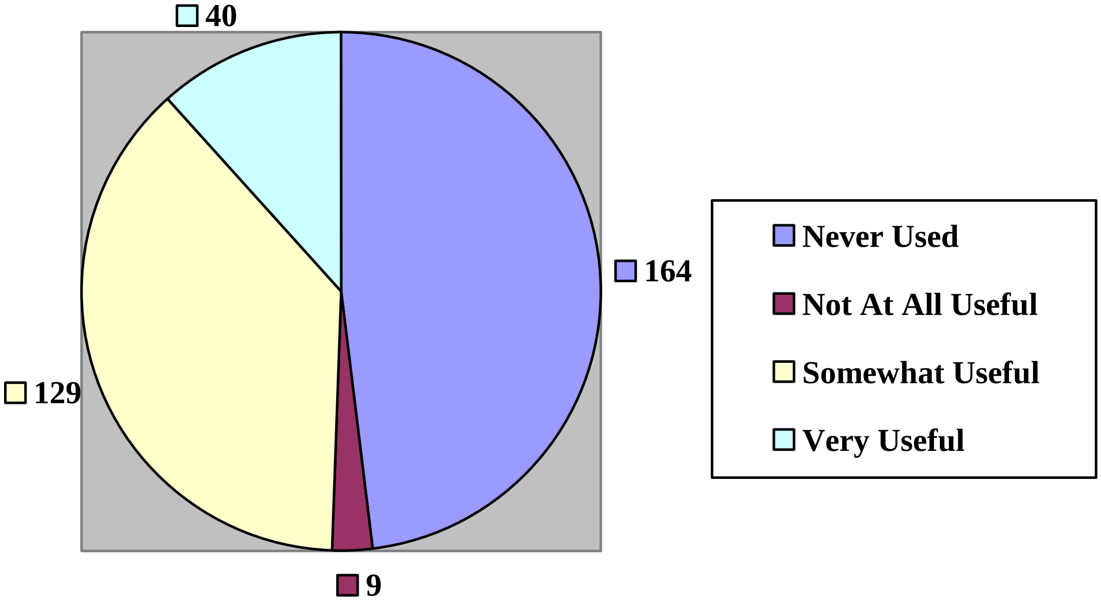

Figure 1: How Useful Are DHS Classified Reports? (Source: CHS Open Source Survey, February 2008)

There is no such thing as being “half safe”. If only 50% of respondents are finding DHS intelligence products useful – be they classified or unclassified – there is certainly room for improvement. The collection, analysis, and dissemination of open source information can help bridge the gap. According to Eliot Jardines, the former Assistant Deputy Director of National Intelligence for Open Source (ADDNIOS), “[I]n looking at the nature of the homeland security and first responder communities, it is apparent that open source intelligence is particularly useful. Due to its unclassified nature, open source intelligence can be shared extensively without compromising national security.”[35] By tapping into its extensive resources and rededicating itself to the development of unclassified intelligence products that communicate pertinent information to State, local, and tribal law enforcement, DHS can effectively execute its critical information-sharing mission.

Law enforcement officials responding to the CHS Open Source Survey reported that they are looking for intelligence products that not only provide information to assist them in their efforts to keep their communities safe and secure but also that provide actionable recommendations about what to do with the information. According to one respondent, “[F]ederal agencies don’t do a good job of providing actionable counterterrorism information.”[36] In testimony before the Intelligence, Information Sharing and Terrorism Risk Assessment Subcommittee of the Committee on Homeland Security, Michael Battista, Deputy Chief of the Denver Police Department, likewise noted that law enforcement needs “greater specificity of

[35] *Using Open Source Information Effectively, Hearing Before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment*, (June 21, 2005) (written statement of Eliot A. Jardines).

[36] CHS Open Source Survey, question 22 comments, (February 2008).

information that allows local law enforcement the ability to take preventative steps in addressing the topic of the [intelligence product]”.[37]

[37] *Information Sharing and National Special Security Events: Preparing for the 2008 Presidential Conventions, Hearing Before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment*, (August 10, 2007) (written statement of Michael H. Battista).

What Efforts are Underway Across the Federal Government?

In 2005, the Director of National Intelligence (DNI) established the Open Source Center (OSC), which is designed to "to advance the Intelligence Community's (IC) exploitation of open source material and enable all IC analysts to access and use relevant open source materials."[38] The Center, which is managed by the Director of the Central Intelligence Agency (CIA), has become a distribution point for unclassified open source products via its website, www.opensource.gov.[39] Users from across the Federal government as well as State, local and tribal law enforcement have access to its products. Of particular relevance is a feature on the OSC website that includes a comprehensive sub-section on terrorism populated with reports from foreign media as well as analytical reports on terrorist groups and activities.[40] It has become an important resource for analysts across the IC; however, as Figure 2 illustrates, 76% of the respondents to the CHS Open Source Survey stated that they were either unfamiliar or unaware of the types of product and support offered by the OSC.[41]

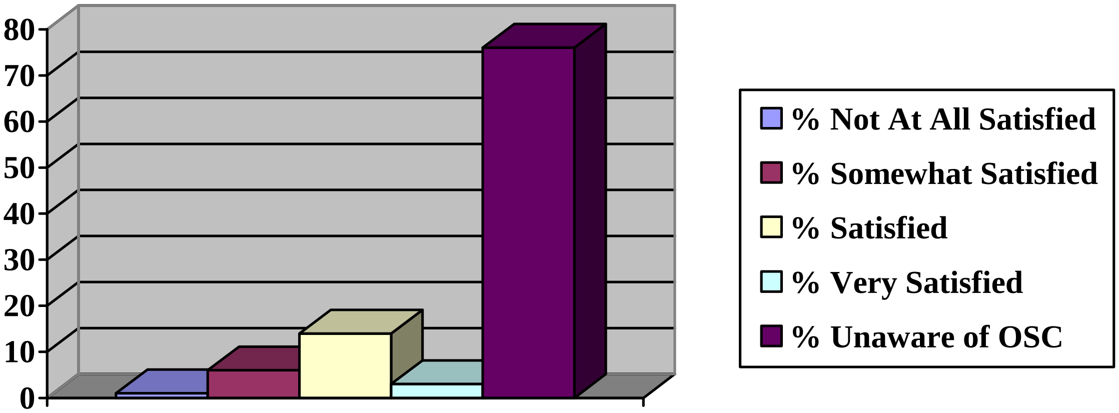

Figure 2: How Satisfied Are You With Open Source Center Products? (Source: CHS Open Source Survey, February 2008)

These results come as no surprise. The OSC's efforts have been centered on supporting the foreign focused elements of the IC, consistent with its mission and legal authorities. In July 2006, the DNI issued Intelligence Community Directive 301, committing the IC to "ensuring the active and efficient use of open source intelligence, information, and analysis by the IC through the establishment and maintenance of an effective, reliable, and collaborative capability that provides maximum availability of open source information to all consumers."[42] In that directive, the DNI also delegated authority for open source strategy development, programmatic oversight,

[38] Memorandum of Agreement for the Establishment and Operation of the Director of National Intelligence OSC, signed between the Director of National Intelligence and the Director of the Central Intelligence Agency, (October 2005).

[39] Id.

[40] See Donna O'Harren, *Opportunity Knocking: Open Source Intelligence for the War on Terrorism*, Naval Post Graduate School, December 2006 at 51.

[41] CHS Open Source Survey, question 14, (February 2008).

[42] Intelligence Community Directive 301, *supra* note 7 (emphasis added).

and evaluation to the Assistant Deputy Director of National Intelligence for Open Source (ADDNIOS).[43] According to former ADDNIOS Eliot Jardines,

> In the open source world, it is neither feasible nor desirable to have a centralized end-to-end solution. A single entity cannot be all things to all people. We should not be centralizing open source capabilities or taking over mission analytical functions better accomplished elsewhere. Rather, we will have visibility into best practices, capabilities, source background, and data stores. We must leverage and share for the greater benefit.[44]

The DNI set out to provide assistance to the Department of Homeland Security (DHS) so that it could develop a robust open source program of its own that served the needs of State, local, and tribal law enforcement. In fact, according to the DNI, the Office of Intelligence & Analysis (I&A) at DHS was allocated approximately $2 million between 2006 and 2008 to establish an open source program that would be aligned with the National Open Source Enterprise – coordinated by the DNI on behalf of the IC.[45] For 2009, the DNI proposed that I&A be provided an additional $1 million in funding to support DHS' open source efforts.[46] As of August 2008, however, DHS was unable to identify with any degree of certainty how monies earmarked for open source activities have been allocated.[47] A senior I&A official advised the Committee in April 2008 that DHS has had difficulty in determining how best to use open source funding.[48]

In addition to funding support, the DNI has offered DHS access to its open source distribution systems including opensource.gov and Intelink-U, the IC's unclassified intelligence distribution network.[49]. According to a senior I&A official, DHS declined the DNI's offer to use Intelink-U as its primary open source dissemination vehicle for its Federal, State and local customers at no cost, in order to focus instead on distributing its intelligence products via the Homeland Security Information Network (HSIN).[50] As of June 2008, however, no action has been taken by DHS to post its unclassified intelligence products to these DNI-hosted systems. While the DNI has made a great deal of progress in building a coordinated National Open Source Enterprise across the IC, its work has been stymied by DHS' inability and apparent unwillingness to take advantage of the guidance and funding that has been provided.

In the absence of a robust DHS program, the disparity in where law enforcement officers go to access open source intelligence could not be starker – most tellingly revealed when respondents were asked which Federal agency they relied upon most for actionable unclassified

[43] Intelligence Community Directive 301, *supra* note 7.

[44] Assistant Deputy Director of National Intelligence for Open Source Eliot Jardines, National Open Source Enterprise, (April 2006).

[45] Interview with senior ranking intelligence official (April 2008) (Specific numbers cannot by provided due to their classified nature, notes on file with author).

[46] Id.

[47] Id.

[48] Id.

[49] Id.

[50] Id.

intelligence. Out of 329 respondents, 227 or 69% said the Department of Justice and the Federal Bureau of Investigation (FBI) met their needs. Just 58 law enforcement officials or 17% of the respondents stated that they relied mostly on DHS.[51] Notably, the CHS Open Source Survey strongly suggests dissatisfaction with DHS' open source intelligence products is directly related to frustration with DHS for not acting to consolidate its HSIN system with other Federal systems.[52] The president of a prominent emergency response association said, "DHS needs to outline how it intends to combine information from all of the HSIN portals into a common operating picture for State and locals, as well as the private sector."[53]

As a result of DHS' inability to lead on open source, the OSC is rapidly becoming the de facto center of gravity for open source intelligence products. While only 27% of CHS Open Source Survey respondents accessed opensource.gov, of those respondents, a large percentage stated that they did so in order to raise their situational awareness of threats.[54] The OSC is a valuable resource for the IC, but the IC is its primary customer and the products they disseminate are designed with that customer in mind. DHS, on the other hand, is uniquely positioned to develop unclassified open source products that complement the work of the OSC and produce intelligence products based on open source information for underserved State, local and tribal stakeholders. DHS' failure to become a center for open source products for these first preventers represents a missed opportunity that should not continue.

[51] CHS Open Source Survey, question 22, (February 2008).
[52] Id., question 11, (February 2008).
[53] Comments of Ian Hay, President, Southeast Emergency Response Network (SEERN), June 25, 2008 (interview notes on file with author).
[54] CHS Open Source Survey, questions 4 and 5, (February 2008).

Is the Department of Homeland Security Using Open Source?

Within the Department of Homeland Security (DHS), the Office of Intelligence and Analysis (I&A) is responsible for assessing the nations vulnerabilities to terrorist attacks.[55] Under the Implementing Recommendations of the 9/11 Commission Act of 2007, moreover, the Under Secretary for Intelligence and Analysis also known as the Chief Intelligence Officer (CINT) is responsible for producing and disseminating unclassified reports and analytic products based on open source information.[56] As described previously, the collection, production, evaluation, and dissemination of these reports to State and local governments as well as the private sector is central to this task. To date, despite extensive support from the Director of National Intelligence (DNI) and a statutory imperative to act, DHS has yet to stand up a robust open source program to share information with law enforcement and other appropriate domestic partners. While DHS produces a number of unclassified intelligence products, to date none of them is identified as having been produced from open source information. In addition, unclassified intelligence products often do not contain the actionable recommendations that law enforcement is seeking that can help direct their day-to-day activities. This determination is supported by the CHS Open Source Survey which found that 37% of respondents were either "not at all satisfied" with or were "completely unaware" of any open source intelligence support provided by I&A.[57] According to one respondent, "[T]he quantity of reports is very good. Open source products tend to be more information than intelligence, however, and quality analysis of open source reporting is lacking."[58]

Unfulfilled Promises

Time and time again, DHS has insisted that it is moving forward with building an open source capability, as envisioned by the Intelligence Reform and Terrorism Prevention Act of 2004. For example, on May 24, 2006, testifying before the Committee on Homeland Security, the CINT, Charles Allen, stated:

> We're looking at putting together a cadre of governmental specialists, as well as contractors from my office, to work as a virtual satellite bureau of the OSC that is run by the CIA to ensure that we meet the requirements not only of the federal government for homeland security open-source information but that we also make available this information and we push it down to the states. The states also . . . have open-source things publicly and lawfully acquired that we hope to have pushed back to us.[59]

[55] See Department of Homeland Security Information Sharing Strategy, April 18, 2008.

[56] Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 531, 121 Stat.333, (2007).

[57] CHS Open Source Survey, question 11, (February 2008).

[58] Id.

[59] *The Progress of the DHS Chief Intelligence Officer, Before the House Committee on Homeland Security*, 109th Cong. 109-80 (May 24, 2006) (testimony of Assistant Secretary Charles Allen, Department of Homeland Security).

Most recently, on February 26, 2008, CINT Charles Allen testified before the Committee’s Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment that:

> The President’s budget will also provide increases for the Office of Intelligence and Analysis’ open source (OSINT) research and analytic capabilities, recognizing the intelligence value of information that is freely found in the public domain. This increased capability will allow the Office of Intelligence and Analysis to conduct OSINT research, acquisition, collection management, content management, and knowledge management to increase the quantity of relevant OSINT provided to our customers. Exploiting this type of information complements the broader IC’s open source investments and allows DHS to better serve Federal, State, and local customers. These new initiatives – along with the maturation of DHS’ Integrated Collections Strategy and fused approach to intelligence, surveillance, and reconnaissance – will improve the Department’s responsiveness to the needs of our internal and external partners.[60]

As of August 2008, however, more than two years after CINT Charles Allen first testified before the Committee about his open source plans, DHS had not formally stood up an open source capability within I&A. Despite assurances from I&A to Congress, the open source program at DHS in fact has suffered from a lack of leadership and strategic direction. Specifically, DHS for the past year has assigned exactly one employee to the task of producing unclassified intelligence products based on open source information.[61] Committee staff, moreover, has learned that as of April 14, 2008, one employee was on duty doing open source work, and a new hire was awaiting a security clearance.[62] An I&A official told Committee staff that there were seven remaining vacancies and expressed the view that within approximately two to three months, the application, review, interview, and selection process could be completed for all seven vacancies.[63] In September 2008, Committee staff received an update on the status of these vacancies. “Of the 8 DNI billets, 2 positions have been filled and 3 were sent to DHS Human Resources for hiring.”[64] In addition, “of the 3 DHS billets, 2 are filled and one is conditionally hired awaiting security clearance.”[65]

[60] *Homeland Security Intelligence at a Crossroads: The Office of Intelligence and Analysis’ Vision for 2008, Before the House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment*, 110th Cong. (February 26, 2008) (testimony of Charles Allen, Under Secretary for the Office of Intelligence and Analysis, Department of Homeland Security).

[61] Briefing by Department of Homeland Security official on I&A open source efforts, January 23, 2008 (notes on file with author).

[62] Briefing by Department of Homeland Security official on I&A open source efforts, April 29, 2008 (notes on file with author).

[63] Id.

[64] Briefing by Department of Homeland Security official on I&A open source efforts, September 8, 2008 (notes on file with author).

[65] Id.

CHS Open Source Survey respondents overwhelmingly reported that DHS was providing intelligence products that were not taking full advantage of the open source materials readily available, including information that was available on the Internet, weblogs, and chat rooms.[66] As Figure 3 illustrates, the large majority of respondents were either unaware that DHS produced open source products or were completely unsatisfied with them. CHS Open Source Survey respondents were unable to identify which products were in fact prepared using open source material and information.[67] Moreover, the few DHS products actually identified as "open source products," including the DHS *Daily Open Source Infrastructure Report*[68], have included only news summaries without any threat analysis or actionable recommendations.

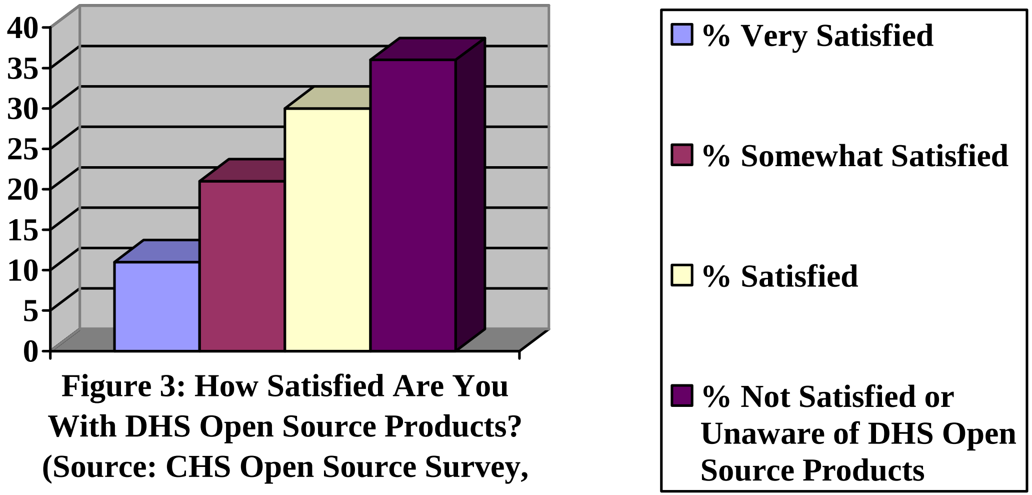

Figure 3: How Satisfied Are You With DHS Open Source Products? (Source: CHS Open Source Survey, February 2008)

Within I&A, the Director of the Collection Requirements Management Division (CR) is responsible for the collection, analysis, and dissemination of open source information. The few so-called open source intelligence products produced by CR are summaries of news stories readily available on Google News or CNN. None contain the additional analysis that would make them actionable for State, local, and tribal law enforcement. DHS' plans to address these issues are well-intentioned; however, it is unclear if they are well-supported with appropriate resources. On June 10, 2008, the CR provided a preliminary draft of a vision for a Domestic Open Source Enterprise (DOSE) to Committee staff.[69] The document sets forth a strategy for building a comprehensive open source capability at DHS. However, without adequate staffing and a commitment by senior leadership, unclassified open source products in all likelihood will continue to be produced and distributed haphazardly by DHS. As a result, what law enforcement is likely to get is information that is anything but actionable.

[66] CHS Open Source Survey, General Comments (February 2008).
[67] Id.
[68] The DHS Daily Open Source Infrastructure Report (Daily Report) is collected each week day as a summary of open-source published information concerning significant critical infrastructure issues. Each Daily Report is divided by the critical infrastructure sectors and key assets defined in the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, available at http://www.dhs.gov/xinfoshare/programs/editorial_0542.shtm.
[69] Briefing by Barbara Alexander on I&A open source efforts, June 10, 2008 (notes on file with author).

The Department Pilot Project

On June 6, 2007, CINT Charles Allen announced a pilot program that has implications for DHS' interaction with State and local authorities and includes a major open source component.[70] The State and Local Fusion Center (SLFC) Pilot Project Team was led by CENTRA Technology, Inc., to work with fusion centers in five States (California, Florida, Illinois, Massachusetts, and New York) to enhance DHS support in three critical areas: (1) responding to State and Local Fusion Center requests for information (RFIs); (2) providing State and Local Fusion Centers with reporting and analysis that responds to their mission-critical information needs; and (3) assisting State and Local Fusion Centers with *their* open source information exploitation capabilities.[71]

The State and Local Fusion Center Pilot Project Team had two goals: (1) to put in place measures to immediately improve DHS support at the pilot sites; and (2) to develop a set of actions that would enable DHS to better meet the needs of State and Local Fusion Center partners nationwide.[72] In February 2008, a report summarizing the findings of the pilot project – including findings on open source – was provided to the CINT Charles Allen. The Project Team found "that the ability of pilot site analysts to exploit open source is limited by the lack of training on state-of-the-art exploitation techniques, by restricted access to relevant federal databases, and by the enormous volume of open source products they receive."[73]

The CHS Open Source Survey supported these conclusions. When asked if I&A developed unclassified products with the open source intelligence requirements of State, local, and tribal law enforcement in mind, 56% of respondents stated that they were unaware of any such effort to understand their requirements.[74] Another 36% stated that DHS had never contacted them to ask if their open source needs were being addressed.[75] In addition, 71% of respondents stated that over the previous month, they obtained less than five open source products from DHS.[76] Just 5% of respondents reported obtaining over 50 open source products from DHS over that same period.[77]

The results of the CENTRA report and the CHS Open Source Survey point to a deficiency at DHS and at I&A. Put simply, while I&A must provide valuable and actionable open source products; it cannot do so until it has a firm grasp of State, local, and tribal open source intelligence requirements. The CENTRA Report can serve as a starting point. Once DHS has such a capability, it could then take on training State, local and tribal intelligence analysts on how to exploit open source information. "While we understand that classified information is important in many cases," said Sergeant William Wickers of the Phoenix Police Department,

[70] See Charles Allen, State and Local Fusion Center (SLFC) Pilot Project email, (June 6, 2007) (on file with author).
[71] See generally CENTRA Technology, Inc., Enhancing DHS Information Support to State and Local Fusion Centers: Results of the Chief Intelligence Officer's Pilot Project and Next Steps, (February 20, 2008).
[72] Id.
[73] CENTRA Technology, Inc., Enhancing DHS Information Support to State and Local Fusion Centers: Results of the Chief Intelligence Officer's Pilot Project and Next Steps, (February 20, 2008).
[74] CHS Open Source Survey, question 12, (February 2008).
[75] Id.
[76] CHS Open Source Survey, question 21, (February 2008).
[77] Id.

"the more information that is derived from open sources and used to develop products helps us out a great deal."[78]

More than two years have passed since CINT Charles Allen stated his intentions to stand-up a DHS open source program. Congress, the Secretary of Homeland Security, and the DNI have given him the authority to carry out this effort. In advance of the presidential transition, he and his team should – at the very least – put the DOSE in place to addresses this glaring deficiency.

[78] Comments of Sergeant William Wickers, Phoenix Police Department, June 3, 2008 (interview notes on file with author)

Obstacles to a Department Open Source Capability

> **We need to rethink the distinction between open sources and secrets…[79] Too many policymakers and intelligence officers mistake secrecy for intelligence and assume that information covertly acquired is superior to that obtained openly.[80]**
>
> ***-- Stephen Mercado, Noted Intelligence Expert***

Access and Distribution

One of the largest obstacles to the creation of a robust open source capability at the Department of Homeland Security (DHS) is the lack of access to open source databases and the lack of a coherent distribution system for intelligence products. The Office of Intelligence and Analysis (I&A) has provided its analysts with connectivity to the numerous classified systems available to similarly situated analysts throughout the Intelligence Community (IC). On the other hand, I&A analysts have not generally been provided access to open source databases beyond those available for free on the Internet. According to the Congressional Research Service, "[A]lthough open [source] information can be collected, certainly at less expense than, for example, that collected by satellite, the Department, like any other consumer of various media, still must pay for access. The Department also must purchase analytic tools that enable analysts to more effectively sift open source information."[81] Analysts within I&A should be able to access classified networks such as the SIPRNet as easily as other fee-based open source portals.

Private companies with large databases of open source information have described I&A as "indifferent" to their offerings despite their proven utility.[82] A senior official with a major corporation that works with large amounts of publicly available data stated that after 18 months of dialogue with the I&A, DHS is no closer to implementing a data management plan to allow for the collection, analysis, and dissemination of open source information.[83] Without access to these types of databases, intelligence analysts at I&A are left producing products primarily from classified sources. As a result, I&A is often forced to remove so much information to create unclassified products that the context and utility of the product becomes unclear.

Moreover, while at least some of I&A's intelligence products are reaching State, local, and tribal law enforcement, distribution is uneven and scattered across too many systems. For example, classified and unclassified products are often available and distributed to State, local and tribal law enforcement on networks via:

[79] Stephen Mercado, *Reexamining the Distinction Between Open Information and Secrets,* (2005), at http://www.cia.gov/csi/studies/Vol49no2/reexamining_the_distinction_3.htm.

[80] Id.

[81] Congressional Research Service, *supra* note 26.

[82] Interviews with various private sector companies (list maintained by the Committee on Homeland Security staff), (Winter 2007-08).

[83] Interview with senior corporate official (January 1, 2008) (notes on file with author).

- Department of Homeland Security Interactive (Classified);

- Department of Homeland Security Intelink on the Joint Worldwide Intelligence Communications System (JWICS) (Classified);

- Homeland Secure Data Network (HSDN) (Classified);

- Homeland Security Information Network (HSIN) Secret (Classified);

- National Counterterrorism Center Online (Classified);

- Homeland Security Information Network (HSIN) for Law Enforcement (LE) (Unclassified);

- Homeland Security Information Network (HSIN) for Intelligence (INTEL) (Unclassified);

- Homeland Security Information Network (HSIN) for Government (GOV) (Unclassified);

- Homeland Security Information Network (HSIN) for Emergency Management (EM) (Unclassified).[84]

In addition, I&A continues to use an email distribution system based upon lists of State, local, and tribal law enforcement personnel.[85] The lack of a coordinated information sharing system with a single sign-on or a federated search means that analysts waste valuable time logging on and off different systems and must maintain too many different usernames and passwords. In the long-term, this wastes valuable resources and may very well be a security risk.

Finally, CHS Open Source Survey results show that while many State, local, and tribal law enforcement officers have access to the Internet and to unclassified DHS systems, the lack of "actionable" information is hindering the utility of that information. A CHS Open Source Survey respondent stated that DHS unclassified reports, including the Chief Intelligence Officer (CINT) Notes were, "low on recommendations for State and locals."[86] With a comprehensive strategy, and in coordination with the DNI, DHS would be poised to create a more robust open source capability. To get there, DHS must invest in providing its analysts with access to all available sources of open source information – including private databases – and begin to limit the number of distribution systems for its unclassified and classified products.

Subject Matter Expertise

According to a recent Congressional Research Service report, intelligence analysts at DHS face several obstacles in making more effective use of open source information, including a

[84] For Official Use Only (FOUO) Intelligence Reports from the Department of Homeland Service indicate that distribution of classified and unclassified products continues via these channels, (April 3, 2008).
[85] Committee staff is regularly copied on the unclassified intelligence products distributed by I&A.
[86] Comments of a senior State law enforcement official, (May 2008) (notes on file with author).

lack of sufficient subject matter expertise. "[O]pen source proponents assert that open source intelligence is as much about such expertise – foreign language and cultural understanding – as it is about the underlying data itself," the report notes. "[I]t would be misleading to assume that the value of such intelligence exists mostly, or solely, in the information itself," the authors conclude.[87]

DHS' efforts to date might lead some to believe that senior leadership has a bias against open source information – especially when one considers the vigor with which it has approached other programs that traffic in classified information such as the National Applications Office (NAO) and the Homeland Security Data Network (HSDN). As one of the newer members of the IC, DHS should able to shed old ways of thinking and embrace a robust unclassified intelligence mission. If the CENTRA Report is any guide, DHS will and should look to State, local and tribal law enforcement for the way forward with open source. Fortunately, a bias against open source information does not appear to exist within the State, local and tribal law enforcement community. According to CHS Open Source Survey results, fully 80% of respondents used private and public open source databases.[88] 326 survey respondents stated that they access these systems as needed to facilitate pending investigations, and 27% stated that they did so several times a day.[89]

Other Obstacles

Training: Intelligence analysts at State and local fusion centers often lack the training necessary to make the most effective use of open sources. According to one survey respondent, "[C]urrently there is a surplus of information available and a serious lack of trained persons to analyze it. There are a lot of analysts without much more than 1 week of analytical training."[90] Oftentimes, the analysts are trained on how to use any number of classified intelligence systems, but they lack access to databases such or cannot take advantage of the Internet's search capabilities.[91] As a result of the pilot project initiated by CINT Charles Allen, an open source training program is being developed.[92] The Committee recently received testimony from the Executive Director of the California Office of Homeland Security, indicating that the Sacramento Fusion Center has received initial open source training from DHS. He stated, "[I]t was very useful, it was well received."[93] This training largely consists of educating State and local intelligence analysts on how to access open sources via the Internet and how they can be used to tailor open source products for their use. The development of this program is ongoing.

Volume: In searching open sources, State, local, and tribal law enforcement officers encounter an enormous volume of information. One CHS Open Source Survey respondent stated

[87] Congressional Research Service, *supra* note 26.
[88] CHS Open Source Survey, question 7, (February 2008).
[89] Id., questions 8 & 9, (February 2008).
[90] CHS Open Source Survey, question 23 comments, (February 2008).
[91] Congressional Research Service *supra* note 26.
[92] See Briefing *supra* note 69.
[93] *Moving Beyond the First Five Years: Evolving the Office of Intelligence and Analysis to Better Serve State, Local and Tribal Needs, Hearing Before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment*, (April 24, 2008) (testimony of Matthew Bettenhausen).

that he often experiences "information overload."[94] In order to create open source products that are relevant to State, local and tribal law enforcement, DHS needs to define specific intelligence requirements and tailor the collection, analysis and dissemination of unclassified open source products to those requirements. Otherwise, analysts will quickly become overwhelmed with the volume of potentially pertinent open source information.

Tools: The search for more effective analytic tools remains a challenge. While private databases can provide some open source information, a better way to tackle the enormous amount of information available on the Internet needs to be created. For example, the private sector has created a number of different search tools that can find and organize large amounts of data but they must be tailored to DHS' mission. The lessons that DHS learns from the process of creating new tools need to be passed along to DHS' customers – State, local, and tribal law enforcement. In addition, DHS either needs to reduce the number of distribution systems or it needs to create an entirely new way to collaborate.

The "Echo" Effect: Open source products that are distributed to a very broad audience due to their unclassified nature tend to re-circulate, oftentimes causing information to become recycled several times without additional analysis. In addition, a particular news item with no credibility can circulate enough times to create a "sense" of credibility. DHS has sought ways to quell this phenomenon with its CINT Notes but much more work remains to be done. According to one senior law enforcement official, "[C]ircular reporting unfortunately results in the need to review the same material more than once in order to ensure you do not miss important information. Essentially it adds time and work to the business of analysis."[95]

Security: According to the Congressional Research Service, overly rigid IC security practices continue to limit the broader and more effective use of open source information.[96] This impacts the ability of State, local and tribal law enforcement to access information they need. An official from a prominent fusion center explains, "[P]olygraph requirements and classification reviews of subsequent publications – can discourage outside experts from collaborating with IC counterparts. Subsequently classifying information provided by outside collaborators can also undermine cooperation."[97] Moreover, according to Washington, D.C. Chief of Police Cathy Lanier, "[W]hile the security classification system that mandates security clearances helps to ensure that sensitive information is protected; it also hinders local homeland security efforts. Information collected by the Federal government is sometimes overly *classified*, causing valuable information that should be shared to remain concealed."[98]

[94] Comments of a senior State law enforcement official, (May 2008) (notes on file with author).
[95] Comments of Supervisory Intelligence Officer Steven Hewitt, Tennessee Fusion Center, June 24, 2008. (interview notes on file with author)
[96] Congressional Research Service *supra* note 26.
[97] Id.
[98] *Over-classification and Pseudo-classification: The Impact on Information Sharing, Before the House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment*, 110th Cong. (March 22, 2007) (testimony of Cathy Lanier, Acting Chief of Police, Metropolitan Police Department).

Towards a Homeland Security Open Source Capability

> **[O]pen source intelligence is the outer pieces of the jigsaw puzzle, without which one can neither begin nor complete the puzzle ... open source intelligence is the critical foundation for the all-source intelligence product.[99]**
>
> ***-- Joseph Nye, former head of the National Intelligence Council***

Mission

When it comes to threat information, State, local, and tribal law enforcement – the Nation's first preventers – should not be saying "we usually see it in the news first."[100] The Department of Homeland Security (DHS) instead must create a comprehensive open source capability that serves these primary customers. This program should be supervised and controlled by the DHS Chief Intelligence Officer (CINT) to conduct competitive unclassified analysis on selected topics of interest to both DHS analysts and those partners. This program should not duplicate the efforts of the Open Source Center (OSC) or any other element of the Intelligence Community (IC). The work of DHS should instead fill a more complementary role by providing strategic analysis that can only be accomplished using open sources specifically tailored to the intelligence requirements of State, local, and tribal law enforcement.

Doing so will first require DHS to recognize its shortcomings. When it comes to providing unclassified actionable intelligence to these partners, it has been largely ineffective. As the February 2008 CENTRA report produced for CINT Charles Allen indicated, "[S]tate and local fusion center leaders … do not believe that the raw reporting and finished intelligence they currently receive from DHS fully meets their mission-critical needs. The intelligence provided is not sufficiently focused on their unique requirements and the substantive issues that dominate the daily work of their fusion center personnel. Even products that do address the right substantive issues sometimes fail to bring out the operational implications for local and State law enforcement – a focus that is critical for their stakeholders."[101] Therefore, while there appears to be progress when it comes to creating intelligence products for these stakeholders, DHS' continuing lack of attention to open source and the apparent continuing disconnect between DHS and its primary customers on this issue, leaves it vulnerable to criticism that it adds little or no value on the intelligence front.

Without immediate action, this lack of understanding will continue to hamper DHS' ability to become a primary source for finished intelligence products for State, local, and tribal law enforcement. Despite increasing access to classified information and intelligence through the Homeland Secure Data Network (HSDN) and the proliferation of security clearances at all levels of government, there is a lack of collaboration between DHS intelligence analysts,

[99] Sands, *supra* note 8, at 64.
[100] CHS Open Source Survey comments to question 19(a), (February 2008) (notes on file with author).
[101] CENTRA Technology, Inc. *supra* note 73.

analysts at the non-Federal level, and non-Federal law enforcement. A real emphasis on providing unclassified open source products with actionable analysis and recommendations is needed.

The end state that DHS should be striving for is a robust open source program extending across all of its intelligence components, State, local, and tribal law enforcement, fusion centers, the IC and the private sector. It would be collaborative in nature – fostering research, experimentation, and capitalizing on opportunities to drive innovation in open source collection, analysis, and dissemination. Among the program's goals would be to:

- Establish and maintain a baseline of open source capabilities throughout DHS;

- Enable State and local fusion centers to build and develop open source exploitation capabilities and give full access to relevant DHS and IC open source data;

- Leverage the full range of open source information sources to expand and inform analysis and reporting.

The creation of a truly unclassified program requires that the open source capability, its systems and its analysts be separated from DHS' classified intelligence efforts. DHS must create a space for the open source program to operate in a completely unclassified environment, free from the restrictions associated with security and classification systems. Such an approach would reflect a marked change in how DHS develops unclassified materials. No longer will they simply be redacted versions of classified products. Under a new open source program, open source analysts would collaborate with State, local and tribal law enforcement, academia, and the private sector to create products that complement classified material and are not simply an afterthought. This approach is critical since any open source capability designed around a classified environment that collects, analyzes, and disseminates classified intelligence products will not satisfy the need for unclassified actionable intelligence based upon unclassified open sources.

Implementation at the Department of Homeland Security

Any open source capability at the Department of Homeland Security (DHS) must be harmonized with the Director of National Intelligence (DNI) National Open Source Enterprise in order to ensure that efforts are coordinated and information is shared in a timely fashion. Implementation of this capability will require a multi-year commitment from DHS and a sincere recognition that open sources serve a key role in providing State, local, and tribal law enforcement with timely, accurate and actionable unclassified open source intelligence products. Investments will be needed in the following areas: (1) policy issues and congressional oversight; (2) program guidance from State, local and tribal law enforcement; (3) leveraging innovation outside DHS; (4) training; (5) coordinating systems; (6) communicating across DHS intelligence components and to their external partners; and (7) protection of privacy, civil rights and liberties.

The DHS open source capability should not only be able to distribute unclassified, timely, accurate, and actionable open source products but also should serve as a test-bed for new types of products, distribution systems and the exercise of CINT Charles Allen's authority under the Implementing Recommendations of the 9/11 Commission Act of 2007.[102]

I. Policy issues and congressional oversight

Significant challenges exist that must be overcome before a robust open source capability can be created at DHS, including resolution of issues regarding: (1) information sharing between public, private and international partners; (2) security; (3) legal requirements; (4) software licensing; and (5) intellectual property rights. There are currently only minimal guidelines in place that protect the personally identifiable information of Americans in the open source context. This information may include names, addresses, birthdates and even Social Security numbers. Processes and information flows to and from the Office of Intelligence and Analysis (I&A) and State, local and tribal law enforcement need to be established. This will require DHS to develop a legal charter, standard operating procedures, and a privacy impact assessment.

Effective congressional oversight will require:

- Close monitoring of the National Intelligence Program (NIP) to ensure that the I&A is receiving an appropriate amount of budget support;

- Empowering the DHS Privacy Office and the Office of Civil Rights and Civil Liberties and the Executive Branch's Privacy & Civil Liberties Oversight Board (PCLOB) to have a direct role in the establishment of an open source capability;

- Working with State, local, and tribal law enforcement, first responders and the private sector to determine if the open source capability is fulfilling its overall mission; and

[102] See generally Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, 121 Stat. 266, Title V (2007).

- Periodic GAO audits to determine how open source information is being collected, analyzed and disseminated.

II. Program guidance from State, local and tribal law enforcement

DHS needs to leverage existing distribution systems such as the Homeland Security Information Network (HSIN) in order to provide for the acquisition and dissemination of open source products to and from State, local and tribal law enforcement. In addition, DHS needs a full and complete understanding of the needs of State, local, and tribal law enforcement customers at the start of this endeavor, and those needs must be reflected in the types of open source products that are created and distributed. The more that these requirements are aligned, the more likely it is that a collaborative environment that allows information to flow in both directions will be created. The CENTRA report is an excellent first step at defining needs, but its lessons must be learned before a truly effective open source capability can be implemented.

III. Leveraging innovation outside the Department

DHS needs to work with individuals, entities and organizations that have built up expertise in collecting, analyzing and disseminating open source products. DHS should participate in the efforts of the DNI to create a functioning National Open Source Enterprise that brings the entire IC together to develop standards on the use of open source. In addition, it needs to work with the private sector to gain access to its vast pools of open source data and for lessons on how to build collaborative online environments. State and local law enforcement are already ahead of DHS on this front. According to CHS Open Source Survey respondents, State, local and tribal law enforcement currently use a variety of private sector open source offerings.[103] A mature open source capability will allow DHS analysts and State, local and tribal law enforcement analysts to draw from the best of the private sector, academia and international partners when needed. DHS should work towards pilot projects with the private sector, academia and international partners to demonstrate that it is serious about building a truly collaborative online environment.

IV. Training

The CHS Open Source Survey illustrated a very significant appetite among State, local, and tribal law enforcement for open source products. As Captain Douglas Keyer of the New York State Intelligence Center noted**,** "[T]he New York State Intelligence Center has taken advantage of OSC courses, as well as a recent DNI-DHS sponsored course featuring an OSC instructor. All courses received positive feedback. Also, the OSC sent a methodologist to New York to help us development a threat assessment capability."[104] He also noted, [T]his was a great benefit and will help us formulate state threat assessments well into the future. I appreciate the assistance provided by DHS and the OSC."[105] In coordination with the OSC and the DNI, DHS needs to expand its current training program with an emphasis on standing up an open

[103] CHS Open Source Survey, question 7 (February 2008).
[104] Comments of Captain Douglas Keyer of the New York State Intelligence Center (June 2008) (interview notes on file author).
[105] Id.

source capability that serves their needs. This will ultimately increase the effectiveness of all intelligence products including those that are classified. In the long-term, the creation of a collaborative online environment will make it easier to facilitate the training of State, local and tribal law enforcement in the effective use of open sources. Ultimately, any DHS open source program will succeed or fail based upon its ability to train DHS and State, local and tribal analysts on how to do open source right and by providing training in the protection of privacy and civil rights.

V. Coordinating Systems

As stated previously, DHS has a long way to go in streamlining the number of systems it uses for distributing intelligence products. An online collaborative environment that allows for the exchange of open source information will require building relationships between the DNI, the OSC, and the private sector. It may also require the development of new tools, processes, and systems that will also work within and in conjunction with existing systems. DHS will need to invest in systems, processes, and tools to be able to interact with all of the other IC components that collect data to solve intelligence problems.

VI. Communicating across the Department's Intelligence Components and to State, local and tribal law enforcement

Once DHS stands up an open source capability, it is critical that it provide information about its capabilities to State, local, and tribal law enforcement as well as the DNI, and the rest of the IC. The lessons learned by DHS will feed into and help to improve the National Open Source Enterprise with the goal of increasing the Federal government's investment in the creation of unclassified open source intelligence products based on open source information.

Protection of Privacy, Civil Rights and Civil Liberties of Americans

Any open source capability – at the Department of Homeland Security (DHS) or elsewhere – must include rigorous privacy, civil rights and civil liberties protections at its core. As one well-known intelligence expert noted:

> Until the mid-1970s, effective legal constraints on domestic intelligence collection were weak. Congressional investigation revealed abuses in targeting activists in the civil rights and anti–Vietnam War movements, or other questionable targeting of individuals under programs such as the Huston Plan, COINTELPRO, Operation Chaos, and others. Constraints were tightened, most notably in the Foreign Intelligence Surveillance Act of 1978, which institutionalized the special process for obtaining warrants for surveillance within the United States. There were also so-called attorney general procedures governing legally sensitive aspects of intelligence collection, including minimization procedures.[106]

Open source is no different; in fact, it is essential that DHS not be lulled into thinking that simply because information is readily available that it may not be protected. The Director of National Intelligence (DNI) has done a great deal of analysis into exactly what types of pitfalls the Office of Intelligence and Analysis (I&A) may face when this important capability is stood up.[107] The major privacy and civil liberties issue regarding the collection, analysis and dissemination of open source information hinges on the handling of U.S. person information. Specifically, DHS must develop processes covering:

1. Collection and use of publicly available information;

2. Accessing non-IC databases containing U.S. person information;

3. Presumptions on the status of U.S. persons (foreign/domestic);

4. How rules apply to new technologies such as chat rooms and blogs;

5. How to identify individuals without name identification.

DHS needs to address each of these issues before it can create an open source capability that is going to contribute significantly to the needs of State, local, and tribal law enforcement and the private sector. Working in consultation with the DHS Privacy Office, the Office of Civil Rights and Civil Liberties, and the Office of General Counsel, I&A should draft a legal framework and standard operating procedures to address these significant challenges. DHS

[106] Richard K. Betts, Enemies of Intelligence: Knowledge and Power in American National Security (Columbia University Press 2007).
[107] Briefing by a senior DNI Civil Liberties Protection officer on the work of the OSC (notes on file with author).

should also be prepared to partner with major privacy, civil rights and civil liberties organizations before any program is put into place.

Legal Issues Remain

Executive Order 12333, on United States Intelligence Activities, requires that all intelligence programs within the IC that are collecting, retaining, or disseminating information concerning U.S. persons be authorized by the Attorney General.[108] It is unclear; however, if DHS has taken the appropriate steps in this regard when it prepared its Domestic Open Source Enterprise (DOSE) that was briefed to Committee staff in June 2008. In addition, there are outstanding legal issues that potentially bear on the issue of how an I&A open source capability is structured and made operational. Among other things:

- It is not immediately clear that an open source capability within I&A directed solely at domestic open source would fall within the IC, subject to the Executive Order on United States Intelligence Activities.

- If I&A domestic open source capabilities are deemed to fall within the IC, how the Executive Order on United States Intelligence Activities should be interpreted on collection requirements against domestic threats is equally uncertain.

These remaining legal issues must be rigorously debated so I&A can learn from the IC's mistakes of the past when it comes to privacy and civil liberties and build in protections needed in the field of open source intelligence now. In designing an open source capability, DHS must keep these lessons in mind by involving the Privacy Office and the Office of Civil Rights and Liberties from the outset. This will ensure that appropriate measures are put in place that restrict potential violations and provide detailed procedures for analysts working with open source information.

[108] Executive Order 12333 of Dec. 4, 1981, appear at 46 FR 59941, 3 CFR, 1981 Comp., p. 200.

Conclusion

On April 1, 2008, USA TODAY published a story entitled *Today's Spies Find Secrets in Plain Sight*. In that story, CINT Charles Allen, "[O]pen source is the world of the future."[109] The Department of Homeland Security (DHS) must take a bold step toward that future. This report gives voice to 350 State, local and tribal law enforcement officials who are seeking a Federal partner that is capable of providing timely and actionable open source intelligence products. DHS is responsible under the Implementing Recommendations of the 9/11 Commission Act of 2007 to be that partner. This report also provides a roadmap for how it can move towards building a collaborative open source capability that serves the needs of State, local and tribal law enforcement while respecting the rights of all Americans.

[109] Peter Eisler, *Today's Spies Find Secrets in Plain Sight*, USA TODAY, April 1, 2008.

APPENDIX

OPEN SOURCE INTELLIGENCE (OSINT) SURVEY

February 2008

Thank you for completing this open source information and intelligence survey. Your responses will help the U.S. House of Representatives Committee on Homeland Security better evaluate and respond to the needs of State, local and tribal law enforcement. Your answers and any comments that may contain identifying information will be kept strictly confidential.

BACKGROUND

The federal Intelligence Community defines open source information as information that is publicly available material that anyone can lawfully obtain by request, purchase, or observation. Open source information generally falls into four categories: information that is widely available to anyone; targeted commercial data; individual experts; and "gray" literature, which consists of written information produced by the private sector, government sources, and academia that is available on only a limited basis – either because few copies are produced, the existence of the material is largely unknown, or access to information is constrained. Within these four categories, open source information can include:

- Media sources such as newspapers, magazines, radio, television, and computer-based information;
- Public data such as government reports and other official data such as budgets and demographics, hearings, legislative debates, press conferences, and speeches;
- Information derived from professional and academic sources such as conferences, symposia, professional associations, academic papers, dissertations and theses, and experts;
- Commercial data such as commercial imagery; and
- "Gray" literature such as trip reports, working papers, discussion papers, unofficial government documents, proceedings, preprints, research reports, studies, and market surveys.

Open source information becomes open source "intelligence" when it is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. Intelligence, moreover, is generally defined as the finished product that is produced after information is collected, processed and analyzed. For example, a newspaper article detailing critical infrastructure in a particular city is information. When that information is analyzed and combined with additional sources, it is possible to deduce what critical infrastructure may be a potential terrorist target. The finished product is considered intelligence.

1. How would you describe your organization?

○ Local Police Department
○ State Homeland Security Agency
○ State or Local Fusion Center
○ Joint Terrorism Task Force (JTTF)
○ Other: ____________________

2. Does your organization collect and analyze open source information?

○ Yes
○ No
○ Not Sure

3. For what purpose do you collect and analyze open source information? Please check all that apply:

□ Produce intelligence products
□ Raise situational awareness
□ Personnel deployment decisions
□ Research requirement
□ Supplement classified intelligence
□ Other (please explain): ______________________________

4. Which information sharing systems do you access? Please check all that apply:

□ Law Enforcement Online (LEO)
□ Regional Information Sharing System Network (RISSNet)
□ Homeland Security Information Network (HSIN)
□ OpenSource.gov
□ Homeland Secure Data Network (HSDN)
□ Intelink-U
□ Other: ______________________
□ I do not access information sharing systems.

5. For what purpose do you access any of these information sharing systems? Please check all that apply:

□ Access intelligence products produced by the Federal government
□ Share intelligence products or relevant information
□ Raise situational awareness
□ Locate subject matter experts
□ No access to these systems is provided where I work
□ I have access to these systems but I do not access them

6. How often do you access these information sharing systems?

○ Several times a day
○ Once a day
○ Several times a week
○ Once a week
○ Once a month
○ Never
○ Other: ____________________

7. Which commercial information systems do you access? Please check all that apply:

□ Lexis-Nexis
□ Oxford Analytica
□ EBSCOhost
□ Autotrack
□ ProQuest
□ Other: ____________________

8. For what purpose do you access these commercial systems? Please check all that apply:

□ Access information to facilitate a pending investigation
□ Raise situational awareness
□ Locate subject matter experts
□ Access commercial intelligence products
□ No access to these systems is provided where I work
□ I have access to these systems but I do not access them

9. How often do you access these commercial systems?

○ Several times a day
○ Once a day
○ Several times a week
○ Once a week
○ Once a month
○ Never
○ Other: ____________________

10. Do you have Internet access on your desktop?

○ Yes
○ No
○ Not Sure

DHS has stated that they provide open source intelligence support to State and local partners. For questions 11 & 12 please describe your level of satisfaction with the support provided:

11. How satisfied are you with the open source intelligence support provided by the DHS Office of Intelligence and Analysis?

○ Not At All Satisfied
○ Somewhat Satisfied
○ Satisfied
○ Very Satisfied
○ I am unfamiliar with or unaware of a DHS open source program

Additional Comments:

12. Has the DHS Office of Intelligence & Analysis asked your organization what its open source intelligence requirements are?

○ Yes
○ No
○ Not Sure

* * *

The National Open Source Center (NOSC) provides foreign media reporting and analysis to policymakers, government institutions and strategic partners. It delivers targeted, timely and authoritative open source intelligence for analysis, operations and policymaking.

13. Are you familiar with the work of the National Open Source Center (NOSC) and its website opensource.gov?

○ Yes
○ No
○ Not Sure

14. How satisfied are you with the open source intelligence support provided by the National Open Source Center (NOSC)?

○ Not At All Satisfied
○ Somewhat Satisfied
○ Satisfied
○ Very Satisfied
○ I am unfamiliar or unaware of the support provided by the National Open Source Center

Additional Comments:

15. Does DHS provide your organization with training on how to collect, analyze and disseminate open source information and/or intelligence?

○ Yes
○ No
○ Not Sure
○ I am unfamiliar or unaware of the training offered by DHS

16. If you answered "YES" to question 15, how satisfied were you with the training?

○ Not At All Satisfied
○ Somewhat Satisfied
○ Satisfied
○ Very Satisfied

Additional Comments:

17. Has your organization taken advantage of training courses offered by the National Open Source Center (NOSC)?

○ Yes
○ No
○ Not Sure
○ I am unfamiliar or unaware of the training offered by the National Open Source Center (NOSC)

18. Do the intelligence analysts or personnel who analyze information in your organization have security clearances?

○ Yes
○ No
○ Not Sure
○ Our organization does not have intelligence analysts

19. Please describe the usefulness of the following information sources:

a. DHS Classified Reports (For example: terrorist threat analysis)

○ Never Used
○ Not At All Useful
○ Somewhat Useful
○ Very Useful

Additional Comments:

b. DHS Unclassified Reports (For example: CINT notes)

○ Never Used
○ Not At All Useful
○ Somewhat Useful
○ Very Useful

Additional Comments:

c. Internet (For example: news websites, blogs or Google Earth)

○ Never Used
○ Not At All Useful
○ Somewhat Useful
○ Very Useful

Additional Comments:

d. Media (For example: pamphlets, newspapers, magazines, television)

○ Never Used
○ Not At All Useful
○ Somewhat Useful
○ Very Useful

Additional Comments:

e. Other State Agency Information (For example: reports distributed by a State Department of Health)

○ Never Used
○ Not At All Useful
○ Somewhat Useful
○ Very Useful

Additional Comments:

20. How satisfied are you with the open source products provided by the DHS Office of Intelligence & Analysis?

○ Not At All Satisfied
○ Somewhat Satisfied
○ Satisfied
○ Very Satisfied
○ I am unfamiliar with any of the DHS open source products

Additional Comments:

21. Over the past month, how many open source products have you received from DHS?

○ 0 to 5
○ 10 to 25
○ 26 to 50
○ Over 50

22. What federal agency does your organization most rely upon for actionable unclassified intelligence?

○ Department of Homeland Security (DHS)
○ Department of Justice (DOJ) including the FBI, DEA &ATF
○ Department of Defense (DOD)
○ National Open Source Center (NOSC)
○ None of the above
○ Other ______

Additional Comments:

______

23. If your organization does not use open source information or intelligence on a regular basis, what are the reasons? Please check all that apply:

□ Lack of software
□ Lack of training
□ Too time-consuming
□ Open source information is not helpful
□ Information not suited to my organization's needs
□ None of the above, my department actively uses open source information.
□ Other ______

Additional Comments:

______

Additional Comments on the Survey:

______

Submit by Email