WRITTEN TESTIMONY OF ELIOT A. JARDINES
President of Open Source Publishing, Incorporated

Before

THE HOUSE COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM
RISK ASSESSMENT

Hearing on
"Using Open-Source Information Effectively"

June 21, 2005

Chairman Simmons, Congresswoman Lofgren, and members of the Subcommittee, I thank you for the opportunity to participate in this hearing. I am Eliot Jardines, President of Open Source Publishing, Incorporated, a private firm which specializes in providing open source intelligence support to the US military, the intelligence community and federal law enforcement. Open Source Publishing has provided open source exploitation, analysis and training for federal agencies since its inception in 1996.

Over the past fourteen years, my career as an open source intelligence practitioner and educator has provided me with an opportunity to understand the significant contributions which the open source intelligence discipline, or OSINT, can bring to the all-source intelligence analysis process. With that said, I am also keenly aware of the limitations of this discipline which should not be viewed as a panacea, but rather a highly effective component of the intelligence toolkit.

The Value of OSINT for Homeland Security

From Pearl Harbor to the September 11th terrorist attacks, intelligence failures have largely resulted not from a lack of information, but rather the inability to effectively disseminate that information or intelligence. In 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, OSINT can be shared extensively without compromising national security.

The flexibility and timeliness of open source intelligence is particularly salient for the Department of Homeland Security because it provides a means by which critical intelligence can be acquired and disseminated without the encumbrances imposed by classification. As an example, during the mid-1990's I was a member of a team which conducted an assessment of how the US Customs Service collected, analyzed and disseminated intelligence. We soon discovered that it was incredibly difficult to disseminate classified information to the tactical level.

Highly classified messages or analytical products underwent a sanitation process which tended to remove important details. The end result was intelligence reports which were too general or broad to be of much use. An attempt to disseminate highly classified documents down to the port of entry level, resulted in the discovery that few if any personnel at that level had the requisite clearances. In other instances, the necessary security infrastructure was unavailable. In one memorable instance, we discovered that a port of entry was able to receive classified faxes, but did not have approved facilities for storage of classified data. The net result was that the classified fax was generally left off. In the rare instances classified faxes were received, they were promptly shredded as no approved means of classified storage was available. With that said, the Customs Service, now the Bureau of Customs and Border Protection, has made dramatic improvements regarding disseminating intelligence. The CPB's Office of Intelligence under the leadership of Roy Surrett, has in many ways set the standard for responsive intelligence support.

However, given the largely unclassified nature of open source intelligence products, the aforementioned issues of clearances and security infrastructure are irrelevant. Not only can these OSINT products be disseminated to inspectors at a port of entry, they can also be provided to state and local law enforcement. In fact, OSINT products could be disseminated to the full

compliment of first responders such as firefighters, EMTs, university police departments, hospitals and private security firms. Consider for a moment what a paradigm sift that would represent.

Intelligence community support to the homeland security community below the federal level is largely non-existent due to classification issues. The way I see it, either we provide Top Secret security clearances and the necessary communications and storage capabilities for every single chief of police, sheriff and fire chief in the country, or we invest a far smaller amount to establish a robust OSINT capability. In the event, God-forbid, of another terrorist attack upon the homeland, it will be the local first responders who will be called upon to put their lives on the line. Do we not owe it to them to at least provide some intelligence support?

Integrating OSINT into the DHS analytical process

How then, do we go about providing this open source intelligence support? First of all, OSINT must be effectively incorporated into the DHS all-source analysis process. This can only be achieved by changing the prevailing mindset that classification is a measure of quality. A highly classified intelligence report is no better or more important than one of lower classification, it is only indicative of the degree of damage done to national security should its inherent sources and methods be compromised.

Secondly, we must establish OSINT as an equal partner with human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT) and measurement and signatures intelligence (MASINT). This is achieved by providing the infrastructure necessary to acquire, process, analyze and disseminate open source intelligence. It is essential that a formalized means exist for the exploitation of OSINT. Of particular importance is the establishment of an open source intelligence requirements management system. Having a requirements management system in place would allow DHS to identify its standing and ad hoc intelligence collection requirements, as well as what entity or activity would be responsible for fulfilling those needs.

For too long, open source exploitation has been delegated as merely an additional duty for intelligence analysts. This is simply a ridiculous notion. No one would seriously propose that intelligence analysts be required to collect their own signals or imagery intelligence. However, that is precisely what we do with open source intelligence. The third recommendation for effective integration of OSINT, is to develop a cadre of highly skilled open source analysts and library professionals to work along side traditional intelligence analysts in order to provide tailored OSINT support to the DHS analytical process. Likewise, these analysts could fulfill an analyst helpdesk function fulfilling ad hoc requirements for DHS entities and the first responder community. It is vital that these OSINT positions be given the importance they deserve and that they not devolve into convenient placeholders for personnel awaiting security clearances.

Fourthly, in order to effectively incorporate OSINT into the DHS analytical process, we must redefine that process. We must begin by redefining the traditional linear intelligence cycle which is more a manifestation of the bureaucratic structure of the intelligence community than a description of the intelligence exploitation process. In his recent seminal work on the issue, *Intelligence Analysis: A Target Centric Approach* Dr. Robert M. Clark describes the traditional intelligence cycle as one that, "defines an *antisocial* series of steps that constrains the flow of

information. It separates collectors from processors from analysts and too often results in 'throwing information over the wall' to become the next person's responsibility. Everyone neatly avoids responsibility for the quality of the final product. Because this compartmentalized process results in formalized and relatively inflexible requirements at each stage, it is more predictable and therefore more vulnerable to an opponent's countermeasures."[1]

Dr. Clark goes on to propose a more target-centric, iterative and collaborative approach which is far more effective than the traditional intelligence cycle. In Clark's target-centric approach, the process is a resilient one in which collectors, analysts and customers are integral and accountable. Redefining the analytical process is a lengthy discussion which exceeds the time constraints of this hearing. I would however, commend Dr. Clark's book to the Subcommittee for further consideration.

The Traditional Intelligence Cycle: Where is the Target?

Image courtesy of the Central Intelligence Agency's Factbook on Intelligence, 2002.

The final way to integrate OSINT into analytical activities at DHS is to establish a streamlined and specialized contracting process to enable outsourcing of OSINT requirements and commercial content procurement. Centralizing the procurement of commercial content such as

[1] Clark, Robert M. (2004). *Intelligence Analysis: A Target-Centric Approach*. Washington, DC: Congressional Quarterly Press, 15.

databases, periodicals or commercial imagery for all of DHS would result in a dramatic cost savings which could in turn, be used to fund further OSINT efforts or content procurement. While centralizing content procurement, DHS must ensure the process is flexible and responsive enough to meet time sensitive or "unusual" requirements.

At Open Source Publishing, we are frequently asked by our customers to acquire individual books or maps which typically do not exceed $50.00 in cost. The conventional government procurement process for such small purchases requires a disproportionate outlay of personnel resources and the death of innumerable trees. In particular, the restrictions and paperwork surrounding the use of government credit cards (IMPAC cards) deserves much attention. Very useful in supporting OSINT efforts would be the establishment of a DHS blanket purchase agreement (BPA) to allow any DHS entity to acquire OSINT related products and services in a simple and cost effective manner.

If such a blanket purchase agreement becomes reality, particular care should be given to insure that the standard practice among the large government contractors of charging exorbitant pass-through fees be kept to a minimum. One particularly effective approach is to award the BPA to a number of prime contractors who would be required to disclose all pass-through percentages and "management fees" upfront to subcontractors interested in using the contract vehicle. In order to insure the success of such an effort, it is essential that the all too common "raping and pillaging" by prime contractors be minimized. The procurement of a $50.00 book should not require a $10.00 pass-through fee and $200.00 in management and administrative charges by the prime.

Disseminating OSINT

The effective dissemination of open source intelligence within the Department of Homeland Security and the first responder community is essential to our national security. As mentioned previously, many intelligence failures are a result, not of faulty analysis, but rather the inability to disseminate intelligence or information in a timely manner. No other department in our government is more reliant on effective information dissemination to fulfill its mission than DHS. Therefore, the unclassified nature of open source intelligence greatly enhances its prospects for wide distribution, and as such should be regarded as a key within DHS.

One recommendation to assist DHS in improving its OSINT dissemination efforts, is to provide all DHS entities with access to the Open Source Information System (OSIS). Operating at the *For Official Use Only* level, OSIS has provided the intelligence community with access to open source analytical products and commercial content since 1994. Rather than re-inventing the wheel, DHS should be encouraged to coordinate its efforts with the Intelink Management Office which manages OSIS. Another recommendation would be to allow <u>all</u> police and fire chiefs access to the homeland security related resources on OSIS. This dramatic expansion of access for first responders can be accomplished by simply leveraging the OSIS network's existing infrastructure. While additional OSIS funding would be required, the cost would be dramatically less than creating such a network from scratch. This arrangement also facilitates collaboration among the first responder community via the OSIS network's collaboration tools and training resources, again at little additional cost.

Should DHS Establish an OSINT Agency?

I understand the Subcommittee has a particular interest in examining whether the Department should establish its own open source intelligence agency. Both the 9/11 Commission and the Weapons of Mass Destruction Commission have recommended that the Director of National Intelligence consider establishing an OSINT agency or center. It is my feeling that it would be a mistake for DHS to rely solely on a DNI OSINT center to fulfill homeland security related OSINT requirements. While capable of providing some degree of support, the DNI's OSINT center could not be as responsive to the unique needs of DHS and the first responder community as a specialized OSINT agency or center would be.

Indicative of the need for specialized OSINT support, the Department of Defense's Open Source Council recently recommended the establishment of a DoD OSINT Program Office to better support the unique needs of warfighters and Defense decision makers. While in general I am no fan of establishing new agencies or centers, in this case the unique requirements of the homeland security community warrants just such an action. I think just about anyone would agree that it is a stretch to think that a single OSINT agency or center could adequately provide for all the needs of such widely divergent agencies like DHS, DoD and the Department of State.

Conclusion

In summation, I believe open source exploitation can provide timely, accurate and actionable intelligence to the Department of Homeland Security as well as the first responder community, particularly at the state and local level. Effective use of OSINT at DHS requires first of all, a change of perspective regarding the value of intelligence – which is *not* determined by its classification level. Secondly, it requires viewing OSINT as an equal partner in the all-source analysis process. Thirdly, OSINT should be conducted by highly skilled analysts and practitioners, not merely the uncleared. Fourthly, effective OSINT exploitation requires a complete reevaluation of the traditional intelligence cycle which is largely ill-suited to the demands of the Global War on Terror. Lastly, effective OSINT requires a flexible means of outsourcing and content procurement.

In terms of effective dissemination of OSINT within DHS and the first responder community, it is imperative that DHS not reinvent the wheel but rather leverage existing capabilities such as the Open Source Information System. Finally, it is my belief that the Department of Homeland Security should establish its own OSINT agency or center to meet the unique needs of its constituents. I thank the Subcommittee for its consideration of my testimony.