Lessons Learned
Information Sharing
www.LLIS.gov

LLIS Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process

December 2005

Background

The Homeland Security Advisory Council's (HSAC) Intelligence and Information Sharing Initiative's December 2004 Final Report (chaired by Governor Mitt Romney of Massachusetts) identified the lack of a formal intelligence requirements process as a missing critical component within the Nation's domestic intelligence sharing framework. Intelligence requirements are the specific gaps in on-hand intelligence that need to be filled for an agency or entity to conduct its prevention and preparedness efforts effectively. Agencies within the federal-level intelligence community (IC) have long used formal requirements processes to identify these gaps, define their intelligence collection needs, and develop and execute operational plans.

However, even in the wake of September 11th, 2001 terrorist attacks and the President's requirement for the construct of an "Information Sharing Environment," this foundational federal intelligence requirements process has not been formally extended from the Department of Homeland Security (DHS) and the IC to its state, local, tribal, and private sector partners, even as these partners have assumed a greater role and responsibility within the Nation's intelligence sharing structure. Currently, no formal process exists for state, local, tribal, and private sector entities to task federal agencies with specific intelligence requirements. Failing to understand these entities' requirements inhibits the federal government's ability to understand the threats facing the Nation, much less provide actionable, timely, preferably UNCLASSIFIED, and frequently updated homeland security information and intelligence to those on the front lines of the domestic War on Terrorism.

Purpose and Methodology

To gain a better understanding of current state, local, tribal, and private sector information and intelligence sharing capabilities and requirements, *Lessons Learned Information Sharing* (*LLIS.gov*), DHS's network for lessons learned and best practices, solicited feedback from relevant subject-matter experts (SME) from across the country. The *LLIS.gov* program's experience in working with the emergency response and homeland security communities, sustained research into the subject of information/intelligence sharing, and extensive network of more than 18,000 public safety officials made it well-suited to undertake this endeavor.

LLIS.gov held a series of four SME meetings in Boston, Chicago, Los Angeles, and Dallas to gather input on state, local, tribal, and private sector intelligence requirements processes. Meeting participants discussed public and private sector processes, mechanisms, and organizational structures for sharing homeland security information and intelligence. In addition, *LLIS.gov* established a message board on its homepage for members to submit their comments and questions regarding the topic of intelligence requirements.

The following report presents the principal findings and recommendations gathered through this initiative. Of note, these findings and recommendations were developed through a "bottom-up" approach. They are the product of the direct input of more than 60 emergency response and homeland security professionals from both the public and private sectors and from multiple disciplines, including state and local executive offices, law enforcement, fire, public health, emergency management, emergency medical services, critical infrastructure security, and public works.

The report is intended to complement and expand upon the recent findings and recommendations of the HSAC's Intelligence and Information Sharing Working Group and the Fusion Center Guidelines Initiative of the Department of Justice's (DOJ's) Global Justice Information Sharing Working Group. Together, these initiatives represent a cooperative effort among DHS, DOJ, and state, local, tribal, and private sector responders and homeland security officials to identify specific gaps and shortfalls within our Nation's information and intelligence sharing environment and develop clear recommendations to address them.

Finding: *In the absence of a clear, consistent system for homeland security intelligence requirements management, state, local, tribal, and private sector entities have developed their own informal and formal structures and networks to share information and intelligence.*

Discussion in the SME meetings demonstrated that state, local, tribal, and private sector entities have established a variety of innovative and effective organizational structures and processes for gathering, analyzing, and sharing terrorism-related information and intelligence. Several states have established fusion centers to serve as central nodes for performing these intelligence sharing functions. Many municipalities and jurisdictions have created their own networks, such as Terrorism Early Warning Groups (TEWs), to perform similar functions at a local level. The private sector, either through sector-specific, regional, or national associations and organizations and private sector intelligence activities, has also developed mechanisms for gathering and sharing threat information and intelligence.

Discussion among the SMEs also revealed the disparate levels of development and sophistication of these state, local, tribal, and private sector structures around the country. Certain states, such as California, New York, Illinois, and Massachusetts, have mature fusion centers with well-developed information and intelligence sharing processes with their federal, tribal, local, and private sector partners. Others are just beginning to develop these structures and processes and are seeking guidance, training, and resources to establish their intelligence sharing programs.

Recommendation: *DHS should nurture the existing and new structures that these jurisdictions, agencies, and entities have established and support them in building their intelligence capabilities and in integrating their efforts with those of the IC.*

Meeting participants agreed that the most effective information and intelligence sharing structures and mechanisms were those that were flexible and built from the "bottom-up" to reflect the particular needs and capabilities of their state, jurisdiction, region, or sector. DHS should focus on leveraging existing programs and seek to integrate those programs into a cohesive, national information and intelligence sharing architecture that is flexible enough to incorporate different state, jurisdictional, or private sector approaches. To that end, DHS should bolster its support to efforts like the HSAC/Global Justice Information Sharing Initiative and the TEW Expansion Project, which are providing guidance and training to states, local jurisdictions, and regions to assist them in establishing intelligence sharing and fusion processes.

Recommendation: *Using its existent policy guidelines (e.g. the National Incident Management System), DHS should focus on building and integrating intelligence sharing* ***functions*** *within each state, as opposed to promoting particular organizational/bureaucratic structures.*

DHS should assess whether or not those state, local, tribal, and private sector structures are fulfilling the certain essential functions (e.g. "collection management" or "analysis and synthesis") necessary for information and intelligence sharing processes to be effective. In those jurisdictions or sectors where these functions are not being performed or only performed incompletely, DHS should provide training and support to assist relevant agencies and entities in fulfilling these functional requirements.

Finding: *State, local, tribal, and private sector entities are unclear as to whom within DHS and the IC they should task with their information and intelligence requirements.*

SME meeting participants consistently stated that the roles and responsibilities of the different federal intelligence agencies and entities were unclear. For state, local, tribal, and private sector officials, simply delineating the multitude of new entities within the domestic information and intelligence sharing arena is a major challenge. Without a clear sense of who to task with their requirements, these officials frequently issue their requirements to as many agencies as possible in order to ensure that they receive the desired information. This approach inevitably leads to redundancy of effort and inefficient use of resources, with multiple agencies receiving the same request and disseminating the same information or intelligence in response.

Not knowing whom to task with their requirements, several meeting participants stated that their entities could not even begin to establish a formal requirements process. Many expressed a desire for a more streamlined approach, with a main point of contact within the IC (e.g. the Homeland Security Operations Center (HSOC)) to process or coordinate their intelligence requirements.

> **Recommendation**: *DHS, in cooperation with its partners within the DNI and IC, should quickly develop and implement a coherent domestic intelligence requirements process. DHS should use the HSOC and the growing network of state fusion centers as the foundation of an architecture for information sharing and intelligence requirements coordination.*

Finding: *State, local, tribal, and private sector entities lack a standard training program for homeland security intelligence analysts. This lack of standard training creates disparities in analyst capabilities, terminology, and approach to homeland security analysis.*

Currently, state, local, tribal, and private sector entities possess intelligence analysts with widely differing skill sets, operational experience, and backgrounds. Some have adopted training and terminology from military intelligence, others from criminal intelligence, and still others from the myriad training programs offered by government agencies, private companies, and academic institutions. Consequently, analyst capabilities, lexicons, and analytical approaches differ widely from state to state and jurisdiction to jurisdiction. For an integrated, national intelligence requirements process to be effective, analysts should possess a common terminology and a fundamental, shared approach to analyzing threat information.

> **Recommendation**: *DHS should establish a uniform training curriculum and standards for homeland security intelligence analysts (as distinct from criminal intelligence, military intelligence, etc.).*
>
> By doing so, DHS would build and strengthen state, local, tribal, and private sector intelligence sharing capabilities, while fostering the consistent language and analytical approach necessary to promote an integrated, national intelligence sharing framework. This training curriculum should include a standard homeland security lexicon, as proposed by the HSAC in March 2004.

Finding: *Domestic intelligence sharing is currently a predominantly law-enforcement function; whereas state, local, tribal, and private sector entities would prefer a broader, more inclusive homeland security intelligence sharing framework.*

Law enforcement agencies should naturally play a central role within any domestic homeland security information and intelligence sharing framework. However, public safety disciplines such as public health, fire, emergency medical services, and private sector security provide different types of information and different perspectives that are essential for this framework to be effective. Several SMEs cited the overall lack of inclusion of these other disciplines at all levels as a critical shortcoming in the development of comprehensive, effective information and intelligence sharing processes.

> **Recommendation**: *DHS should support the expansion of homeland security intelligence sharing and analyst training to include all public safety and works disciplines, including critical private sector entities. The Department should continue to encourage initiatives that promote a multidisciplinary approach to information and intelligence sharing and fusion, such as the HSAC, Global Justice Information Sharing Initiative, and the Terrorism Early Warning (TEW) Expansion Projects.*

Finding: *There is a perception within State, local, tribal, and private sector entities that they are receiving information from the federal government without being asked for information in return.*

Meeting participants repeatedly cited a lack of two-way communication between themselves and the federal government. They stated that, too often, DHS and other federal agencies transmit non-specific threat information that in many cases does not meet their requirements. Several stated that they were not even aware that DHS has any specific information and intelligence requirements from them; few had even heard of or seen DHS's Terrorist Threat Reporting Guide.

Others participants stated that when they did transmit information to DHS and other federal agencies, they rarely received any feedback as to the utility of that information. Many stated that they had little contact with DHS officials in an operational capacity and suggested that DHS should have a more visible presence at the state, local, tribal, and private sector levels, preferably through the State Fusion Centers.

> **Recommendation**: *DHS should do more to foster a "transmit and receive" environment for information sharing that involves a greater two-way flow of intelligence/information–based upon state, local, tribal and private sector intelligence/information and operational requirements.*
>
> DHS should also make its state, local, tribal, and private sector partners more aware of its own information requirements. As is routine within the Intelligence Community, when DHS receives information from these entities, DHS should provide timely feedback to let them know the quality and utility of their information and make them feel directly involved in the homeland security effort. DHS should consider having permanent representatives, liaison officers, or trusted officials in state and local fusion centers to facilitate and coordinate information flow to and from DHS and to build professional and trusting relationships with these state and local partners.

Finding: *State, local, tribal, and private sector entities lack a clear understanding of the federal government's capabilities.*

Most state, local, tribal, and private sector entities are relatively new participants within the realm of homeland security, anti-terrorism, and intelligence. Consequently, many lack knowledge of the federal government's ability to fulfill their information and intelligence needs and requirements. This can lead to a redundancy of effort and a waste of scarce resources. For example, one state homeland security agency has a team of analysts researching a Middle Eastern country. At the same time, the Intelligence Community (IC) already has scores of analysts examining the same country with better access to information and more resources at its disposal. With better understanding and better connectivity between the state, DHS, and federal anti-terrorism agencies, the state could avoid this redundancy of effort and allocate its resources more effectively.

> **Recommendation**: *Through the state and local fusion centers, DHS should educate and inform its domestic partners of DHS and the IC's capabilities.*

Finding: S*tate, local, tribal, and private sector entities believe that inadequate attention has been paid to risk assessments for their jurisdictions/sectors/companies/regions.*

Comprehensive risk assessments including threat, vulnerability, and consequence are crucial to identifying specific intelligence requirements. A thorough assessment of the threats to, vulnerabilities of, and consequences of an attack on assets, infrastructure, and business and government continuity can reveal the key gaps in information and intelligence that should be filled to enable more effective prevention strategies. Meeting participants acknowledged that comprehensive risk assessments directed beyond traditional goals of protection toward resiliency and continuity of operations should drive the development of specific intelligence requirements.

Many participants also stated that inadequate resources and multiple and inconsistent risk assessment methodologies were all too often the norm. In particular, smaller or rural jurisdictions often lack the more obvious critical assets that would generate immediate interest in performing risk assessments. These jurisdictions nonetheless can serve as critical transit points for hazardous materials or as cross-border bottlenecks for the delivery of essential goods and services for the Nation. For example, an attack on a particular jurisdiction's chemical facilities could affect the security of the Nation's water supply, while one at a key border crossing could cripple large sectors of the U.S. economy. These jurisdictions frequently lack the requisite resources and expertise necessary to conduct these assessments.

> **Recommendation**: *DHS should accelerate its efforts to develop standard risk-based and operational continuity/resiliency-focused assessment methodologies and should assist in training public and private entities to conduct, use, and continually update these assessments.*

Finding: *State, local, tribal, and private sector entities believe there are too many technical systems for sharing threat information and intelligence, causing confusion and uncertainty as to where to go to obtain and/or disseminate threat information.*

"Not another DHS system!" was the frequent, repeated request from SMEs. The multitude of new technical and communication systems that have been developed by DHS and other federal agencies has led to confusion and frustration over their cost and effectiveness among state, local, tribal, and private sector entities. These entities are faced with frequent changes in reporting and communication systems, formats, passwords and security requirements, and have to undergo retraining to familiarize themselves with new systems.

Recommendation: *DHS should consolidate its myriad of systems for disseminating threat information and use its Homeland Security Information Network (HSIN) as the principal information sharing system.*

LLIS Intelligence Requirements Initiative Subject-Matter Experts

Glenn Aga, Public Safety Commissioner, City of Laguna Niguel, California
Richard Andrews, Senior Director, Homeland Security Project, National Center for Crisis and Continuity Coordination
Caroline Barnes, Assistant Director, New Jersey Office of Counterterrorism
Roy Barnes, Manager, Global Intelligence, General Motors Corporation
Robert Belfiore, Chief, Port Authority of New York and New Jersey
Dennis Beyer, Chief of Homeland Security, Tulsa, Oklahoma Fire Department
Carlo Boccia, Director, Mayor's Office of Homeland Security, Boston, Massachusetts
Ken Bouche, Colonel, Illinois State Police
M. Doug Cain, Sergeant, Louisiana State Police
John Cohen, Office of the Governor, Commonwealth of Massachusetts
Mark D. Cohen, Deputy Director and Chief Counsel, New York State Office of Homeland Security
Michael Cohen, Security Director, Citigroup-New Jersey
Dan Collier, Investigator/Analyst, Minnesota Joint Analysis Center
Roy Condon, Executive Vice President of Operations, Homeland Security Information Network-Critical Infrastructure (HSIN-CI)
George Cummings, Director of Homeland Security, Port of Los Angeles
John Daley, Intelligence Supervisor, Boston Police Department
Raymond DeMichiei, Deputy Director of Emergency Management and Homeland Security, Office of the Mayor, Pittsburgh, Pennsylvania
Jack Faer, President, Fidelity Security Services, Inc.
Shawna French-Lind, Homeland Security Manager, Wal-Mart Stores, Inc.
Jeff Friedland, Emergency Services Manager, St. Clair County, Michigan
Daniel Garcia, Deputy Chief, Dallas Police Department
Van Godsey, Intelligence Unit Supervisor, Missouri State Highway Patrol
Michael Grossman, Commander, Office of Homeland Security, Los Angeles County Sheriff's Department
Kevin Hacker, Officer, Counter-Terrorism Section, Chicago Police Department
Robert Hass, Under Secretary for Homeland Security, Commonwealth of Massachusetts
William Hipsley, Deputy Director, California Office of Homeland Security
Bart R. Johnson, Lieutenant Colonel, New York State Police
Robert Keane, Assistant Vice President for Safety and Regulatory Affairs and Police Chief, Canadian National Railway
Ted Kilpatrick, Manager, Dallas Water Utilities
Fred LaMontagne, Fire Chief, Portland, Maine
Grant Lappin, Public Safety Director, Baylor HealthCare-Texas
Monte McKee, Major, Indiana State Police
Laurence Mulcrone, Senior Director of Security, McCormick Place/Navy Pier, Chicago, Illinois
Russell Porter, Assistant Director and Chief-Intelligence Bureau, Iowa Department of Public Safety
Daniel Rattner, Founder and Principal, D.M. Rattner & Associates
Richard Rawlins, Deputy Director of Operations, Ohio Homeland Security

Thomas J. Richardson, Captain, Seattle Fire Department
Alexander Rokowetz, Manager, National Security & Emergency Preparedness, Verizon
Paul Schieck, Director of Security, Seattle Mariners Baseball Club
Joel Schrader, Deputy Director, Kentucky Office of Homeland Security
Dave Smith, Security Manager, Shell Oil Company
Robert Smith, Major, Massachusetts State Police
Rick Stephens, Senior Vice President Internal Services, Boeing Corporation
John Sullivan, Lieutenant, Los Angeles County Sheriff's Department/Terrorism Early Warning Group
Rick Velazquez, Deputy Chief of Staff to Don Knabe, Los Angeles County Board of Supervisors
Steve Wheeler, Director of Security, Lockheed Martin Corporation
Jeff Witte, Director, Agriculture Biosecurity, New Mexico Department of Agriculture

Lessons Learned Information Sharing Staff

John Rabin, Program Director, *Lessons Learned Information Sharing*
Peter Roman, Research Director, *Lessons Learned Information Sharing*
Bill Moore, Project Manager, *Lessons Learned Information Sharing*

Federal Participants

Art Fierro, Chief Operating Officer, Homeland Security Information Network-Critical Infrastructure (HSIN-CI)
William Dawson, Deputy Intelligence Community CIO and Special Assistant for Information Sharing, Office of the Deputy Director of Central Intelligence for Community Management

Special Acknowledgements

Dan Ostergaard, Executive Director, Homeland Security Advisory Council
Jeff Gaynor, Director, Emergency Response Senior Advisory Committee
Mike Miron, Director, State and Local Officials Senior Advisory Committee
Candace Stoltz, Director, Private Sector Senior Advisory Committee