INFORMATION SHARING MECHANISMS TO IMPROVE HOMELAND SECURITY

Focus Areas: Program/Project Management, Standardized Data Reporting, Standard Business Processes.

Sponsoring Executive: Charles Allen, Under Secretary for Intelligence and Analysis and Chief Intelligence Officer

Lead Executive: Carter Morris, Director, Information Sharing & Knowledge Management Intelligence and Analysis, (202-282-8248)

Supporting Organization(s): Office of Intelligence and Analysis, Office of the Under Secretary for Management (OUSM), Office of the Chief Information Officer (OCIO), National Protection and Programs Directorate (NPPD)

Description

Responsible for assessing the nation's vulnerabilities, DHS takes the lead in evaluating vulnerabilities and coordinating with other federal, state, local, and private entities to ensure the most effective response. The collection, protection, evaluation and dissemination of information to the American public, other federal agencies, state, local, and tribal governments, and the private sector is central to this task.

Maintaining a comprehensive yet cohesive information network that enhances inter- and intra-Department information sharing is complicated by geographical, infrastructural, and technical challenges. Therefore, the Department has developed three mechanisms that complement each other and enable federal, state, and local partners to collaborate and coordinate efforts.

First, the Homeland Security Advisory System targets our protective measures when specific information to a specific sector or geographic region is received. It combines threat information with vulnerability assessments and provides communications to public safety officials and the public. Second, the Protected Critical Infrastructure Information (PCII) Program facilitates greater sharing of critical infrastructure information between private sector and government entities by protecting the information from public disclosure. Third, secure communication networks, including the Homeland Security Information Network (HSIN) for SBU/CUI information and the Homeland Secure Data Network (HSDN) for classified (collateral Secret) information, provide nation-wide platforms to share essential intelligence and other homeland security information with the proper stakeholders. This information sharing is accomplished both horizontally across the government and vertically among state, local, and tribal governments, the private sector, and citizens as outlined in the President's National Strategy for Homeland Security. HSAS, PCII, HSIN and HSDN are crucial towards meeting the Department's most daunting challenge to communicate across distances and technologies.

In support of DHS' critical information sharing mechanisms, the Department has implemented multiple activities and programs that are dedicated towards working with particular federal, state, and local partners that may require various levels of clearance, types of information, and means of communication. First, the Constellation/Automated Critical Asset Management System (C/ACAMS) allows state and local government users to collect and use asset data and protection information to develop incident response and recovery plans to protect infrastructure assets. The Homeland Security Advisory System targets protective measures when specific information to a specific sector or geographic region is received. It combines threat information with vulnerability assessments and provides communications to public safety officials and the public. Second, HSIN, a computer-based collaboration system connecting all 50 states, five territories, Washington, D.C., and 50 major urban areas, provides a medium in which sensitive but unclassified information may be communicated to multiple stakeholders within a secure environment. Third, HSDN is the Department's strategic capability for sharing intelligence and other classified (Secret/collateral) or highly sensitive information among federal agencies with homeland security missions and key State and local partner installations, particularly Fusion Centers.

In order to assure that proper representation is considered and stakeholder concerns are heard, DHS has formed committees and working groups that meet on a regular and frequent basis with Department membership, enabling cross group discussions, best practice implementation, and a bridge of communication from DHS and other federal leadership to first responders and local emergency event support structures. During 2007, the Department established the information sharing governance framework, which operates through a three-tiered structure to represent all DHS components and enable the Department to speak with "one voice" to our external partners. The Information Sharing Governance Board (ISGB) is the decision-making body for all DHS information sharing and collaboration issues[1]. The Information Sharing Coordinating Council (ISCC) is the implementing body for information sharing issues and is comprised of information sharing action officers representing all 22 components and offices within the Department. Shared Mission Communities (SMCs) complement the governance structure, and are comprised of members of a shared mission. The SMC fosters a culture of information sharing and supports the ISCC and ISGB in gathering information sharing requirements and implementing solutions. A SMC begins as an ISCC Integrated Project Team to complete its charter and design its strategic vision, and as a community, propose their establishment to the ISCC & ISGB for approval. Through this structure, the Department is implementing the Secretary's One DHS[2] information sharing policy and executing towards the milestones detailed in the information sharing goal outlined in the Secretary's Priority Tracker.

The Department is also actively engaged in the Director of National Intelligence (DNI) Intelligence Community Information Sharing Steering Committee (IC-ISSC). The Director for Information Sharing & Knowledge Management is the DHS representative to the IC-ISSC. DHS consistently participates in the working group meetings and development of IC information sharing policy memoranda and directives, to ensure that DHS stakeholder needs are advocated and considered.

[1] The ISGB is comprised of the Under Secretary for Intelligence & Analysis, the Chief Information Officer, the Assistant Secretary for Policy, the Director of Current Operations, the Assistant Secretary for Infrastructure Protection, the General Counsel and the Lead, Law Enforcement Shared Mission Community (currently the Assistant Secretary for Immigration & Customs Enforcement).

[2] The Secretary's Memorandum to all DHS components on the policy for *DHS Internal Information Exchange and Sharing* issued February 1, 2007.

Other influential committees and working groups exist to support the Department. First, the Homeland Security Advisory Council provides advice and recommendations to the Secretary on matters related to homeland security. The Council is comprised of leaders from state and local government, first responder communities, the private sector, and academia. Second, the Critical Infrastructure Sector Partnership ensures that, coordinated approaches and plans are agreed upon and documented by all appropriate stakeholders, since critical infrastructure protection is a shared responsibility among Federal, State, local, and tribal governments and the owners and operators of the nation's critical infrastructure and key resources. Third, the DHS Data Privacy and Integrity Advisory Committee advises the Secretary and Chief Privacy Officer on program, policy, operations, administrative, and technology issues relevant to DHS that affect individuals' privacy, data integrity, data interoperability, and other privacy-related issues.

Although mechanisms, activities, and programs are essential for critical information sharing to be effective, trust is the most important variable for success. It has been noted that many local and private sector institutions are concerned that the Department is ill-equipped to adequately protect and effectively use the information that it provides. The Department is concerned that this interpretation may be in part due to the difficulty of communicating through third parties such as other government agencies and municipalities. Therefore, DHS has developed State & Local Fusion Centers that blend relevant law enforcement and intelligence information analysis and coordinate security measures in order to reduce threats to local communities.

In addition, the DHS National Protection and Programs Directorate's Office of Intergovernmental Programs promotes an integrated national approach to homeland security by ensuring, coordinating, and advancing federal interaction with state, local, and tribal governments. The purpose of the office's operations is multi-faceted and includes facilitating communication between the Department's expert resources and the expert resources of the nation's autonomous governments, providing advocacy for state, local, tribal, and territorial governments within the Department, and coordinating and maintaining constant awareness of the various multi-lateral communications occurring regularly throughout the Department.

By providing timely and meaningful consultation with our state, local, tribal, and territorial partners, DHS improves not only its capacity to share information with capable mechanisms and programs but also builds trust in both public and private sectors.

Expected Outcomes

- Standard set of policies and processes allowing timely inter- and intra- Department sharing of Homeland Security information
- Enhanced operational coordination and collaboration of Homeland Security elements from the local to the federal levels, via compatible information technology architecture and infrastructure
- Improved capacity and capability to collect, integrate and analyze data, identify trends, and disseminate intelligence and LE information

Accomplishments

- DHS has established and is operating a three-tiered governance structure for information sharing. At the executive level, the Information Sharing Governance Board (ISGB) meets quarterly to decide Department-wide information sharing issues. At the management level, the Information Sharing Coordinating Council (ISCC), comprised of representatives from all DHS components and offices, meets semi-monthly to discuss information sharing issues and formulate recommendations for the ISGB. At the execution level, the Shared Mission Communities (SMCs) and Integrated Project Teams (IPTs) meet regularly to develop solutions for information sharing issues.

- The Secretary of Homeland Security issued a DHS-wide policy on information sharing, the *DHS Policy for Internal Information Exchange and Sharing*, which provides guidance for all Departmental information sharing activities. To supplement this memorandum, the ISGB issued an Information Sharing and Access Agreement (ISAA) Guidebook to provide additional policy guidance for components in creating information sharing agreements.
- DHS completed deployment of HSDN to a total of 17 State Fusion Centers in 2007, with work in progress to reach a total of 40 Centers by the end of 2008. Using HSDN, DHS officers deployed to Fusion Centers and State and local officials in Fusion Centers with appropriate clearances can exchange classified data with each other and other federal agencies. HSDN also enables limited sharing of information with other Federal Secret networks like SIPRNet, DNI-S and FBINet, and supports classified video-conferencing.
- DHS sponsored development of a nationwide self-governing community of federal and non-federal intelligence analysts, and launched the HSIN-Intel portal to support analyst-to-analyst collaboration as well as more secure and efficient dissemination of unclassified finished intelligence products. HSIN-Intel provides enhanced security using Two-factor authentication, among other controls.
- Through the governance structure, a Law Enforcement SMC was established, which represents the first time that DHS law enforcement components have come together to discuss their mutual needs for information sharing. The LE-SMC is in the process of finalizing a DHS Law Enforcement Information Sharing Strategy (LEISS).
- DHS is finalizing a Department-wide Concept of Operations (CONOPS) for how components of the Department will interact with State and local fusion centers to ensure consistency and continuity. The State and Local Fusion Center (SLFC) CONOPs was required by the *Implementing the Recommendations of the 9/11 Commission* Act of 2007.
- DHS created a Department-wide measure for information sharing as part of the Department's Performance Plan that will examine compliance towards the DHS policy on information sharing.
- The Secretary added a goal on information sharing to the Secretarial Priorities. The Department measures its progress towards this goal on a monthly basis.

Actions Required to Complete[3]

- Finalize the DHS Information Sharing Strategy, developed through the information sharing governance structure.
- Sign a Memorandum of Agreement between DHS and FBI on who has the authority to authorize release of information from the State Fusion Centers; this agreement then needs to be promulgated to all State Fusion Centers, Homeland Security Advisors, and USG Departments/Agencies.
- Design and implement a central, Department-wide ISAA repository to ensure that components have the ability to leverage existing agreements.

[3] As listed in the Secretary's Priority Tracker Information Sharing Goal #13.

- Conduct an inventory of data assets and information flows within DHS and with external partners (including state, local, tribal and private sector) to create a Department-wide repository to ensure that components have the ability to leverage existing data assets.
- Lead the state, local, and tribal law enforcement information sharing enterprise by enhancing Regional Sharing System solutions in conjunction with federal partners.
- Distribute the SMC Framework Charter which provides the guidelines for establishing additional SMCs across DHS and with DHS stakeholders.
- Embed intelligence officers at up to 35 State and Local Fusion Center (SLFC) sites by the end of the 2008 Fiscal Year. Assess as many SLFCs as resources will support in high interest locations to understand the mission, information sources/flows, analytic capacity, IT infrastructure, security, and partnerships with state and federal agencies.
- Develop guidelines for private sector handling of Controlled Unclassified Information (CUI) in joint partnership with the private sector through the Private Sector Subcommittee, Information Sharing Environment (ISE).
- Working with other ISE members, develop and document criteria for sharing classified information with appropriate Critical Infrastructure/Key Resource (CI/KR) sectors, and streamline procedures for declassifying critical threat information to enable broader distribution.
- Document awareness of established mechanisms and processes National Infrastructure Protection Plan (NIPP) and National Response Framework (NRF) for information sharing within the targeted private sector community, e.g. CI/KR sectors, through existing DHS outreach programs through the 2008 CI/KR National Annual Report.

Milestones	Original Target End Date	Current End Date	Percent Complete	Comments
A. Utilize info-sharing governance structure to facilitate achieving objectives of "One DHS" memo.				
1. In conjunction with the Office of General Counsel, review all ISAAs to ensure compliance with "One DHS". Where permissible, re-negotiate non-compliant agreements and provide a standard notice to external	12/31/2007	9/30/2008	45%	The ISGB has directed the ISCC to revitalize efforts to collect and review the ISAAs.

Milestones	Original Target End Date	Current End Date	Percent Complete	Comments
partners of "One DHS" policy.				
2. Design and implement a central, Department-wide ISAA repository to ensure that components have the ability to leverage existing agreements.	3/31/2008	9/30/2008	60%	The deliverables (ISAA Data Fields Requirement Document) have been reviewed. The data collection and translation is in process.
B. Develop info-sharing framework to reducing gaps in information flows by establishing organizational awareness of Enterprise Data Assets available within DHS.				
1. Conduct an inventory of data assets and information flows within DHS and with external partners (including state, local, tribal and private sector)	9/30/2008	12/31/2008	50%	As of 7/31/08, at the current rate of acquisition, the data asset baseline will not be complete by the milestone but is on plan to be completed by 12/30/2008.
2. Design and implement a repository to ensure that components have the ability to leverage existing data assets and information flows.	12/31/2008	12/31/2008	50%	Requirements phase is 100% complete. Design phase has begun. Function Requirements Document is complete.

Milestones	Original Target End Date	Current End Date	Percent Complete	Comments
C. Promote a culture of info-sharing by establishing a framework on shared missions and info-sharing standards				
1. Lead SLT law enforcement info sharing enterprise by enhancing Regional Sharing System solutions (RSS) in conjunction with federal partners (DOJ, DOD, ODNI, and PM-ISE). Demonstrate an ability to share DHS law enforcement info with two RSS.	12/31/2007	9/30/2008	99%	The San Diego and Los Angeles deployments are completed and progress continues to be made with DOJ and Arizona communities.
2. Establish the Law Enforcement SMC to foster an environment through which DHS law enforcement components can address their information sharing needs, best practices, and challenges in a unified manner.	10/31/2007	8/22/2008	95%	With the completion of the SMC Framework Charter the LE SMC Charter is complete and ready for consideration by the ISGB.
3. Provide the	12/31/2008	8/22/2008	100%	The SMC

Milestones	Original Target End Date	Current End Date	Percent Complete	Comments
guidelines for and establish additional SMCs across DHS and with DHS stakeholders, with stewardship from I&A.				Framework Charter was unanimously approved by the ISGB on 18 April 2008.
D. Establish partnerships with all State & Local Fusion Centers (SLFCs) and high-interest cities to improve info-flow between DHS and fusion centers; improve fusion center effectiveness				
1. Develop a Concept of Operations (CONOPS) for internal DHS support to State & Local Fusion Centers, which is supportive of the joint CONOPS in development with the Department of Justice	10/31/2007	9/15/2008	95%	The Privacy Office completed the Privacy Impact Assessment and the CONOPS is being re-circulated to ensure currency. Both documents will go out for Departmental review by mid-July.
2. Embed Intelligence Officers at up to 35 sites by the end of the 2008 Fiscal Year.	9/30/2008	12/31/2008	71%	Two Intelligence Officers were deployed to the field in June 2008 after one month of orientation and training.
3. Assess as many SLFCs as resources will support, in high interest locations to understand the mission, information	12/31/2008	12/31/2008	100%	Targeted number of assessments is 35. Four assessments were completed in April – bringing the total to 35.

Milestones	Original Target End Date	Current End Date	Percent Complete	Comments
sources/flows, analytic capacity, IT infrastructure, security and partnerships with state and federal agencies.				
E. Improve info-sharing between DHS Critical Infrastructure/Key Resources protection partners at all levels of government and private sector partners.				
1. Develop guidelines for private sector handling of CUI information in joint partnership with the private sector through the Private Sector Subcommittee, Information Sharing Environment.	9/30/2008	11/30/2008	40%	
2. Working with other ISE members, develop and document criteria for sharing classified information with appropriate CI/KR sectors, and streamline procedures for declassifying critical threat information to	12/31/2008	12/31/2008	70%	

Milestones	Original Target End Date	Current End Date	Percent Complete	Comments
enable broader distribution.				
3. Document awareness of established mechanisms and processes (NIPP and NRF) for information sharing within the targeted private sector community, e.g. CI/KR sectors, through existing DHS outreach programs through the 2008 CI/KR National Annual Report	9/30/2008	9/30/2008	70%	Work has begun on the 2008 CI/KR National Annual Report and progress is steady.

Impediments/Challenges

- Information sharing across geographical, infrastructural, and technical challenges requires a high level of standardization and coordination
- Trust requires opportunity and dedication over long periods of time

Measures

Each Department program and project will develop and document outcome and output performance measures against a baseline of compliance highlighted in the FYHSP database. Gaps and poor performance will be identified and corrective/mission action plans will be required with the goal of reducing and ultimately eliminating the gaps. The Office of Intelligence and Analysis staff will report performance to the Deputy Secretary for the purpose of monitoring progress towards this Plan.