Securing the Homeland Through
Information Sharing and Collaboration

Department of Homeland Security Information Sharing Strategy

April 18, 2008

Homeland Security

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 APR 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Department of Homeland Security Information Sharing Strategy	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Homeland Security,20 Massachusetts Ave NW,Washington,DC,20001**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**9**	

Information Sharing Strategy for the Department of Homeland Security

The President and Congress have directed the Department of Homeland Security (DHS)[1] to perform an essential and multi-faceted mission: prevent and protect against terrorist attacks; respond to both man-made and natural disasters; perform the law enforcement and other crucial functions of the Department's component agencies; and play a central role in augmenting the Nation's ability to gather, analyze and disseminate information and intelligence.[2]

To ensure that information and intelligence flow where and when they should, DHS must foster information sharing, consistent with law, regulation and policy, in each of the following ways: i) internally within DHS, ii) horizontally within the U.S. government between both law enforcement agencies and the intelligence community, iii) vertically with State, local, territorial, tribal and private sector partners, and iv) horizontally with the law enforcement and intelligence agencies of foreign allies and appropriate international institutions.

The foundation for DHS's key role with respect to information sharing has been established by statute, regulation, Executive Order and Secretarial directive. The Department has made significant contributions to the Nation's information sharing capability since its inception, but critical work remains to be done. This Information Sharing Strategy for DHS builds on that foundation and sets out DHS's strategy for achieving its information sharing objectives.

This Strategy is comprised of:

- *Background*;
- *Transformation Statement*;
- *Guiding Principles*;
- *Critical Challenges*;
- *Objectives*;
- *Information Sharing Standards*;
- *Information Sharing Security and Privacy*;
- *Performance Measures*; and
- *Communication and Outreach*.

[1]References to the Department of Homeland Security (DHS) include all components, directorates, and offices within the Department, as reflected in the Secretary's *Policy for Internal Information Exchange and Sharing* ("One DHS") memorandum of February 1, 2007.

[2] *See Homeland Security Act of 2002, the Intelligence Reform and Terrorism Prevention Act of 2004, as amended,* and the *Implementing the Recommendations of the 9/11 Commission Act of 2007.*

Background

The attacks of September 11, 2001, along with Hurricane Katrina, highlighted the challenges in our Nation's information sharing and coordination capabilities. The 9/11 Commission cited a number of examples in which the lack of effective information sharing between Federal, State and local agencies resulted in the failure of Federal authorities to intercept the attack.[3] The White House analysis of Hurricane Katrina similarly pointed out the manner in which failures in information sharing at all levels hindered our Nation's disaster response and recovery effort.[4] DHS is addressing these weaknesses and strengthening our Nation's ability to gather, analyze, disseminate, and utilize information to prevent terrorist attacks; to prepare for, protect against, respond to, and recover from catastrophic events of all kinds; and, to coordinate and strengthen the immigration and customs enforcement, border and transportation security, law enforcement and other missions performed by the Department's component agencies.

The Homeland Security Act of 2002 and Presidential Executive Order 13356 provided the impetus for a National effort to improve information sharing and defined the Department's initial role in this effort. This role has been expanded and refined in subsequent statutes, such as the Intelligence Reform and Terrorism Prevention Act of 2004, as amended (IRTPA). IRTPA ensured that DHS would have a central part in the Information Sharing Environment (ISE). Shortly after establishing the ISE, the President established the Office of the Program Manager for the Information Sharing Environment (PM-ISE). DHS works closely with the PM-ISE, currently under the Office of the Director of National Intelligence (ODNI), to coordinate the development of a common National framework for information sharing. DHS also has major responsibilities with respect to the National Response Framework, which outlines how information is to be shared in response to all incidents, including terrorist attacks and natural disasters.[5]

In October of 2007, the President set out the National Strategy for Information Sharing. The National Strategy, and the updated 2007 National Strategy for Homeland Security, envision a coordinated and integrated Information Sharing Environment to effectively fight terrorism and respond to man-made and natural disasters. Both strategies give DHS a central role in ensuring that critical information is shared rapidly to the fullest extent allowed by law.

In addition, other Information Sharing strategies have been issued that are consistent with the DHS Information Sharing strategy, such as the just-released United States Intelligence Community Information Sharing Strategy.[6]

---

[3] *See Final Report of the National Commission on Terrorist Attacks Upon the United States* (July 22, 2004) at 221-222.
[4] *See The Federal Response to Hurricane Katrina: Lessons Learned* (February 2006) at 52 (issued by the Assistant to the President for Homeland Security and Counter Terrorism).
[5] *See National Response Framework*, Department of Homeland Security (January 2008).
[6] *See United States Intelligence Community Information Sharing Strategy* (February 22, 2008) at 17.

The Secretary of DHS has made significant strides in creating the environment and infrastructure necessary to foster information sharing by streamlining communication within DHS components, incorporating resources in fusion centers, working with the intelligence community to develop information exchange integrity standards, and developing a senior level governing board that oversees information sharing practices and policy – all in compliance with Constitutional, statutory, regulatory, and other legal requirements, including privacy and civil liberties standards, and internal policies.[7]

- In January of 2007, the Information Sharing Coordinating Council (ISCC) was established. Now a working body of the Information Sharing Governance Board (ISGB), the ISCC is a forum for the offices and components of DHS to collaborate on information sharing initiatives and raise information sharing issues for consideration to the ISGB.

- In February of 2007, the Secretary issued the DHS *Policy for Internal Information Exchange and Sharing*, referred to as the "One DHS" memorandum, to further mandate open information exchange within DHS.

- "One DHS" established the ISGB as the senior-level DHS governing body for information sharing policy and dispute resolution. The ISGB is chaired by the Under Secretary of Intelligence and Analysis.

- On October 2, 2007, the Secretary included an Information Sharing objective as one of his top priorities for management, policy and operational integration. Information Sharing Objective 13 established objectives and milestones to improve information sharing.

- Over the past two years, DHS has launched a number of initiatives and pilots to increase operational information sharing, including but not limited to: the DHS Secure Border Initiative; the Coast Guard-led Inter-agency Operational Centers; and the ICE Agreements of Cooperation in Communities to Enhance Safety and Security (ACCESS) program. DHS has also increased support for, and presence in, State and local Fusion Centers.

Transformation Statement

Transform DHS into an organization whose culture, business processes, and governance structure foster an information sharing environment that ensures the right information gets to the right people at the right time. [8]

[7] These legal authorities include, but are not limited to, 28 C.F.R. Parts 20-23, Executive Order 12333, the Privacy Act of 1974, the E-Government Act of 2002, the Fourth, Fifth, and Fourteenth Amendments, and guidance provided by the PM-ISE.

[8] *See* Secretary's Information Sharing Objective #13.

Guiding Principles

This Strategy is informed by the following guiding principles:

1. *Fostering information sharing is a core DHS mission*. Congress and the President have made it clear that one of the Department's core missions is to create the technological and organizational infrastructure necessary to promote the sharing of information regarding terrorism, homeland security, law enforcement, weapons of mass destruction, and incidents of all types within DHS, across the Federal government, and with State, local, tribal, territorial, private sector and international partners.

2. *DHS must use the established governance structure to make decisions regarding information sharing issues.* The Secretary has established a governance structure dedicated to facilitating information sharing in a manner consistent with the law, including Federal privacy and civil rights laws. The Department must fully utilize this structure to achieve information sharing objectives.

3. *DHS must commit sufficient resources to information sharing.* DHS has taken significant steps, but substantial work remains – including new mandates from the President and Congress – to achieve the desired level of information sharing capability. Further success will require significant organizational resources throughout DHS and continued commitment by all DHS personnel.

4. *DHS must measure progress toward information sharing goals.* The Secretary has identified clear objectives in this arena. DHS must now institute performance measures that provide a realistic and actionable assessment of the Department's progress toward meeting these objectives.

5. *DHS must maintain information and data security and protect privacy and civil liberties*. Achieving the Department's information sharing goals requires maximizing operational effectiveness while protecting privacy and civil liberties. The Office of General Counsel, the Privacy Office, the Office for Civil Rights and Civil Liberties, the ISGB and the ISCC will continue to work closely with DHS components on their information management processes to ensure that privacy, civil rights and civil liberties, and other legal protections are fully respected and implemented.

Critical Challenges

DHS continues to face barriers to information sharing. As the 9/11 Commission emphasized, although technological issues exist, the primary challenge both within DHS

and with external information sharing partners is creating a widely accepted process for sharing mission-relevant information while adequately protecting the information.[9]

Creating a broad foundation for information sharing requires trust between all information sharing partners. Lack of trust stems from fears that shared information will not be protected adequately or used appropriately; and, that sharing will not always occur in both directions. For example, law enforcement and the intelligence community are concerned that competing information uses will compromise ongoing investigations, sources and methods. State, local, territorial, tribal and private sector partners are willing to share information with the Federal government, but want assurances that information held at the Federal level will be shared adequately with them. The Department must emphasize mission-based information sharing that ensures the right information gets to the right people at the right time.

The many different missions of the Department and its information sharing partners add complexity to defining mission related information sharing needs. Clearly defined and institutionalized rules, roles and responsibilities are necessary to ensure effective information sharing. The need for an information sharing environment to encompass and address these complexities has slowed the process of developing information sharing protocols at the policy level even more than at the technological level. These complexities also have created challenges in identifying and appropriately distributing useable information to those who need it.

Objectives

To address critical challenges and to implement DHS Secretarial Objectives and Priorities for information sharing, DHS will strive to achieve the following:

1. Secure and maintain active participation in the ISCC by each DHS component, directorate and office.

2. Fully coordinate DHS information policies, programs and projects with the ISE to promote sharing with Federal partners, while at the same time strongly advocating that the PM-ISE recognize and accommodate DHS mission needs, enterprise requirements and solutions.

3. Build a robust set of Shared Mission Communities to identify mission-specific information sharing opportunities and build trust, using the experience gained in establishing the Law Enforcement Shared Mission Community and in other endeavors.

4. Make the fusion centers an integral part of DHS and Federal information exchange with State, local, territorial, tribal and private sector partners.

[9] *See Final Report of the National Commission on Terrorist Attacks Upon the United States*, at 146 ("The biggest impediment to all-source analysis – to a greater likelihood of connecting the dots – is the human or systemic resistance to sharing information.")

5. Fully recognize and integrate Federal, State, local, territorial, tribal, private sector and foreign government information needs as part of the DHS information sharing environment, consistent with applicable laws, regulations and international agreements.

6. Ensure that DHS technology platforms evolve to facilitate appropriate mission-based information sharing with Federal, State, local, territorial, tribal, private sector and foreign partners.

7. Ensure that mission-relevant information sharing agreements are in effect with Federal, State, local, territorial, tribal, private sector and foreign partners to promote information sharing consistent with the "One DHS" mandate.

Information Sharing Standards[10]

As DHS further develops its information sharing standards, these standards principally will comply with the requirements of the ISE as promulgated by the PM-ISE, and with any other applicable standards as may be required by law. Development of DHS standards will be guided by the following precepts:

- The information needs and missions of all stakeholders, not technology, will drive the design of the DHS information sharing environment. Technology will be used to enhance and simplify information sharing.

- Information sharing technology and protocols will be cross-functional with various domains, information technology systems, and infrastructures with the goal of creating a degree of interoperability with the systems utilized by the Department's Federal, State, local, territorial, tribal, private sector and foreign partners.

- DHS standards and protocols will utilize or leverage published commercial standards and protocols when available and where appropriate.

- DHS standards, procedures and applicable laws for privacy and civil liberties will guide and support the DHS information sharing environment.

Information Sharing Security and Privacy

DHS must ensure the security of the information collected and shared by the Department. At the Federal level, statutory and other policy mandates such as the Privacy Act of 1974, the E-Government Act of 2002, the Homeland Security Act of 2002, the Federal Information Security Management Act of 2002 (FISMA), and Executive Order 12333

[10] *See Information Sharing Environment Implementation Plan* (November 26, 2006), prepared by the PM-ISE, and the *President's Guideline 5* as stated in the *Memorandum for the Heads of Executive Departments and Agencies, Subject: Guidelines in Support of the Information Sharing Environment* (December 16, 2005).

require careful safeguarding of any information that personally identifies U.S. persons. Executive Order 12958, as amended, defines the safeguarding requirements for classified national security information. Other Federal regulations and individual department and agency policies set requirements for the various categories of sensitive but unclassified information. In addition, States and local jurisdictions have enacted privacy and data security laws. Also, the private sector will always be concerned about protecting proprietary information and trade secrets, despite recently created safeguards.[11] Finally, as the Department shares information with foreign partners, foreign laws and international agreements may also impose data security and privacy requirements.

The Department's approach to information security will be threefold. The Department will:

- Develop robust information protection and data security protocols that comply with applicable laws, regulations and agreements as a matter of policy;

- Devote sufficient resources to train DHS personnel and the Department's information sharing partners in appropriate security requirements, protocols, practices, and privacy and civil liberties standards[12]; and

- Adopt technology solutions that support the appropriate level of information and data security and commit sufficient resources to the electronic and physical protection of information media.

The threats to secure and reliable information sharing are numerous, potent and persistent. DHS will pursue data security and privacy as primary elements of information sharing, such that these protections enhance and do not prevent or delay appropriate information exchange.

Performance Measures

Spearheaded by the Information Sharing and Collaboration Branch (IS&C) within the Office of Intelligence & Analysis, and the ISCC, DHS is implementing a comprehensive approach to measuring the effectiveness of Departmental information sharing. The IS&C has developed and continuously tracks milestones for each of the priorities under Secretarial Objective 13. The current milestones focus on building the institutional infrastructure that will enable DHS to create the secure and trusted environment necessary for information sharing. As these milestones are achieved, the IS&C will create new benchmarks, coordinated through the ISCC, to move toward outcome-oriented measures that track the effectiveness of DHS information sharing.

In fiscal year 2007 DHS included the first Departmental measure of information sharing in the Performance Budget Overview process. The ISCC will develop additional

[11] *See* Section 214 of *The Homeland Security Act of 2002*.
[12] *See* Section 501 of the *Implementing the Recommendations of the 9/11 Commission Act of 2007*.

measures, tied to the Departmental budget and planning process, to ensure progress toward information sharing that meaningfully contributes to DHS mission outcomes.

As a member of the ISE, DHS will continue to assist the PM-ISE to design, baseline, validate and refine information sharing performance metrics with an emphasis on the results of information sharing. Through the ISCC, the IS&C will collect, compile and submit data to the PM-ISE. DHS also will continue to monitor progress toward successful achievement of the goals set out in the National Intelligence Strategy and as articulated by the Director of National Intelligence in the "500 Day Plan."

Communication and Outreach

Formulating and promoting the DHS information sharing environment and the elements of this Strategy will be an ongoing departmental effort. A principle conduit for this effort will be the ISCC. The ISCC is developing a communications plan to disseminate information regarding this effort and to encourage participation within DHS and among external partners. In crafting the communications plan, the ISCC will:

- Identify key audiences among internal and external stakeholders and partners;
- Develop messages that inform and educate;
- Solicit feedback and participation;
- Identify the most effective vehicles to deliver coordinated and useful messages and develop standardized procedures for communications; and
- Assess the status of our communications vehicles and identify improvement opportunities.