A Blue Print for Homeland Security Information Sharing

arcAspicio

The need for Federal agencies to share information to prevent future terrorist attacks, a finding of the 9/11 Commission, continues to be a current and pressing concern.

In the simplest terms, Information Sharing is the exchange of data between people and organizations, often enabled by technology. In reality, it is a very complex process involving policy and privacy constraints and technology limitations. Many agencies may lack comprehensive policies, store information in incompatible formats, and have cultural norms, legal restrictions, and tight budgets that inhibit information sharing.

Successful information sharing relies on close cooperation across different levels of government and with private sector partners to promote secure and responsible exchanges. The Government can identify threats more reliably before an event occurs if stakeholders share information in a timely, standardized, and automated way. The consequences of not sharing information can include needless loss of life and detrimental economic impact.

Since 9/11, Federal agencies have done an excellent job gathering and analyzing information within their individual mission areas. These agencies now have an obligation, stemming from legislation and executive orders, to share their national security information with one another. For agencies to feel comfortable, they need to be able to trust that the information remains secure once shared.

While new technologies and innovation have made it easier to share information, it has also made storing information electronically more vulnerable to compromise. To develop trust and safeguard our information, coordinating bodies and policies must focus on recognizing and mitigating internal and external threats, while departments and agencies work to enhance capabilities for data-level controls, automated monitoring, and cross-classification solutions.

Not only does information sharing help prevent future terrorist attacks, but it helps agencies better perform their individual missions with an eye towards the homeland security enterprise.

How Does Information Sharing Affect You?

The Tourist: Hadi and Sarah are returning from a spring break trip in Egypt, flying from Cairo to New York. Saif Bazzi, a known terrorist, also made reservations for the same flight. Saif Bazzi was en route to participate in a terror attack. After 9/11, Bazzi was added to the No Fly List. When Bazzi attempted to board the plane, he was arrested by Egyptian authorities, enabling Hadi and Sarah to fly home safely.

The Veteran: Andy, a service member who was injured while in Afghanistan, is in the process of transferring from DoD medical care to that of Veterans Affairs. It is a stressful time for many veterans and their families. DoD and VA have established a process to share the standards-based electronic health records enabling Andy to transition smoothly as he changes health care providers.

The Policy Maker: Antoinette works for Immigration and Customs Enforcement (ICE) developing the agency's strategy to combat human trafficking. As a result of protocols put into place by DHS and its partner agencies, Antoinette can now access information from across the different departments to determine the best way to distribute scarce resources to address this growing problem.

How Privacy Controls Enable Information Sharing

- The Government highly regulates sharing of information on US citizens and legal permanent residents
- Data tagging and access controls are critical to protecting privacy
- Data tagging facilitates data discovery and improves analysis with privacy in mind

CULTURAL SHIFTS

Not all barriers to information sharing spring from technology or policy; many are cultural. Cultural norms are important when access to data is tightly controlled based upon an individual's clearance and authorized need to know. Prior to 2001, information collection and analysis revolved around individual missions. Sharing was ad hoc and based on individual, personal relationships (e.g., ICE Special Agent Joseph Smith calls Special Agent Sally Rohan at the Federal Bureau of Investigation (FBI) about a potential human trafficking organization). This historical context perpetuated philosophical and cultural barriers within agencies that remain even today.

Culture is the foundation to successful information sharing **(Figure 1)**. There are several ways that agencies can foster cultural shifts to promote regular information exchange between systems and employees. First, nothing creates trust more than personal relationships. Agencies should reward their best employees with detail assignments at major fusion and operation centers. Organizations should invest in joint training sessions, leverage secure Government-only social media tools, and expand the use of Government-wide portals such as the Homeland Security Information Network (HSIN). Additional ideas include:

- Create informal networks and recurring meetings to share knowledge and create more familiarity with the data and the players
- Offer training for mission experts and policymakers in enterprise-wide data sharing topics and solutions
- Engage data owners in enterprise-wide data analysis and solicit their feedback throughout the process
- Align each agency's security models to emerging Intelligence Community Standards

Second, agencies can foster trust among one another by promoting a risk-based mindset when it comes to information sharing. Putting the proper controls in place so that unauthorized individuals do not have access to information is possible with a combination of policy and technology. Not sharing information or sharing information in an inconsistent, fragmented manner increases threats to national security. This risk decreases when sound policies and standards, training and awareness, effective governance, and shared accountability are in place. Adopting a shared approach to risk management and protecting sensitive information increases transparency and promotes trust between data owners and users.

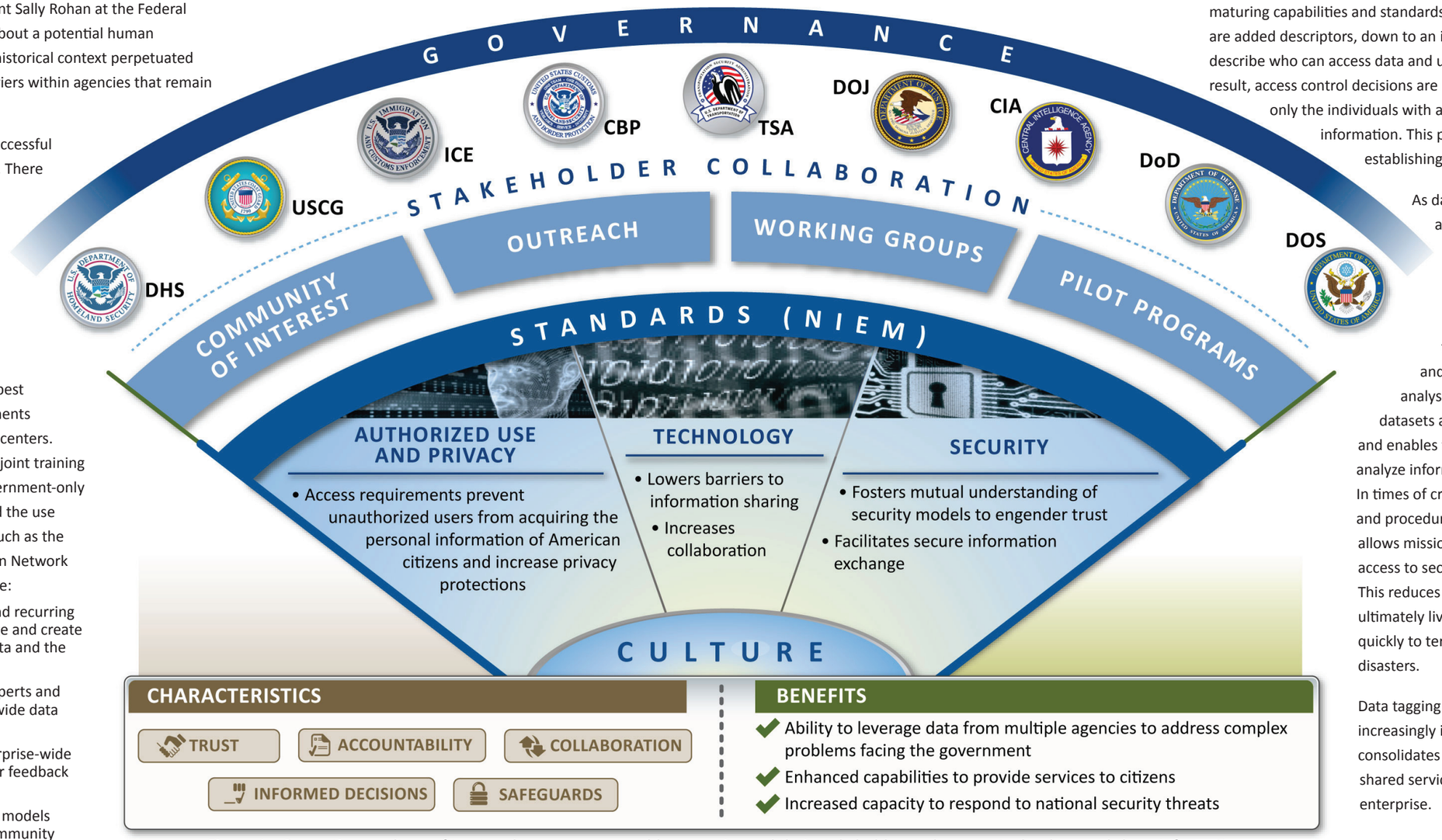


Figure 1 – Promoting a culture of trust and transparency enables agencies and their stakeholders to leverage technology and share information in a secure way, accelerating mission results.

DISCOVERY AND ACCESS CONTROL

The use of Personally Identifiable Information (PII) and classified information is highly regulated by federal laws and policies. Enforcement of these policies and a transparent, auditable system builds trust among stakeholders. As noted in Figure 1, one way to protect personal information is by controlling access to the information so that only those with the proper clearance and need to know can view it. An essential tool in this challenge is the maturing capabilities and standards of data tagging. Data tags are added descriptors, down to an individual data element, that describe who can access data and under what circumstances. As a result, access control decisions are made by a set of rules, allowing only the individuals with an authorized use to view the information. This plays an important part in establishing an agency's security model.

As data become more integrated and the associated data analysis becomes increasingly important, mission-focused, standardized data tagging also helps analysts to identify relevant information and improve the quality of data analysis. Standard data tagging across datasets also makes analysts more agile and enables them to easily discover and analyze information from different owners. In times of crisis, pre-established policies and procedures based on tagging capabilities allows mission operators to get authorized access to secure information in real-time. This reduces costs, and saves time and ultimately lives, by preventing or responding quickly to terrorist attacks and natural disasters.

Data tagging will continue to become increasingly important as the Government consolidates data networks and develops shared services across the homeland security enterprise.

SMALL PROJECTS, BIG IMPACT

Budgets continue to shrink across the Federal Government. Undertaking cross-agency projects (where one agency leads and the others help fund) is a proven, successful model in homeland security.

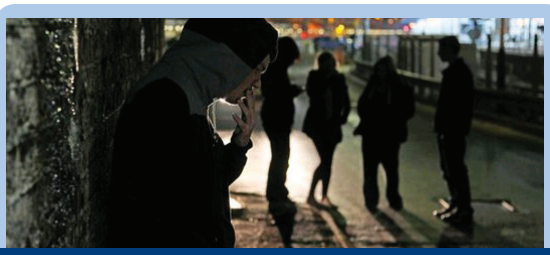
Agencies can harness the power of information sharing by adopting small, agile projects, such as pilots, or by using proven models, such as the National Information Exchange Model (NIEM). These options require a low initial investment, yet produce repeatable solutions that have an exponential return on the initial project.

Proven models, processes, and reusable toolkits are available. Sponsoring organizations such as the Program Manager – Information Sharing Environment (PM-ISE) and the Department of Homeland Security (DHS) promote these through training, webinars, and other outreach efforts. For example, in addition to providing agencies with a foundation for creating an information sharing program, the NIEM Program Management Office also provides technical support. NIEM has enabled a wide range of agencies throughout the Federal government to share information by creating communities of interest (COI) or agencies with overlapping mission areas.

To lower costs and promote interoperability, agencies can adopt enterprise big data platforms and, when possible, build on collective demand to acquire new technology. Hosting shared information systems on a common infrastructure distributes workloads, reduces computing capacity requirements, and lowers costs.

No matter the methods for implementing an information sharing program, agencies must define clear plans and adopt an information sharing strategy in line with the National Strategy for Information Sharing and Safeguarding. Progress against defined milestones and performance measures builds momentum, completes projects within budget, and achieves the desired outcomes. Identifying roles, responsibilities, milestones, and governance at the onset enables planning and helps to prevent risks due to miscommunication. Creating appropriate performance measures to monitor the project's impact help meet the objectives or help provide early warning if a project is at risk of falling short of expectations.

A small project is a big step to mission results.

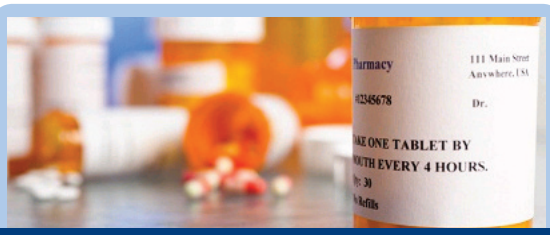


CASE STUDY 1: Mass Gangs

Problem: Information on gang members in Massachusetts was stored in disparate federal, state, and local databases, complicating investigations and prosecutions of gang members.

Solution: With funding from the Department of Justice, federal, state, and local law enforcement organizations used NIEM to create a web-based database.

Impact: The creation of a streamlined gang data management process provided agencies with a unified way to share gang-related information in Massachusetts.



CASE STUDY 2: California-Nevada Prescription Monitoring Information Exchange Pilot Program

Problem: Prescription drug abusers realized the short coming of interstate reporting systems and began traveling across state lines to acquire drugs.

Solution: California and Nevada created an online information exchange system to combine reporting systems.

Impact: The states both increased their capacity to identify prescription drug addicts by integrating criminal justice and public health reporting systems.

Contact Us: To learn more about information sharing, email Rob O'Keefe, Chief Technology Officer, at info@arcaspicio.com or call our Information Sharing team at 703.465.2060.

arcAspicio