A BRIEF HISTORY OF THE INFORMATION SHARING ENVIRONMENT (ISE)

As the nation enters the second decade following the terrorist attacks of September 11, 2001, our information sharing challenges are maturing. Sharing cybersecurity information poses new opportunities. Safeguarding information has always been a critical component of responsible information sharing, but has taken on a new urgency in the wake of unauthorized disclosures of classified and sensitive information. In light of these developments, it is useful to review the recent history of information sharing policy, with a focus on the Information Sharing Environment (ISE) created by the Intelligence Reform and Terrorism Prevention Act (IRTPA).

Section 1016 of the IRTPA established an Information Sharing Environment (ISE) for counterterrorism, weapons of mass destruction, and homeland security information. The ISE is a success because it is based on principles of sound information management. The ISE is grounded in initiatives led by the Departments and agencies at all levels of government, and it is informed by their needs and requirements. The ISE is supported by effective governance mechanisms, including integration with the budget process. The ISE also incorporates protections for privacy and civil liberties, which are critical to public confidence. These features provide a model for successful information sharing.

Although the need for greater sharing of terrorism-related information became more evident following the attacks of September 11, sharing and use of data to enhance national security and to improve public safety have been integral to a variety of reform efforts since the dawn of the information age. Conversely, breakdowns in information sharing have contributed to intelligence failures that impeded needed action. Failures in information safeguarding have led to data breaches, leaks, and violations of privacy.

This paper traces the evolution of the Information Sharing Environment (ISE) in the context of information sharing reforms and outlines goals for the future of responsible information sharing.

THE NEED FOR AN INFORMATION SHARING ENVIRONMENT (ISE)

Information sharing to enhance national security and improve public safety did not begin with the post-9/11 era of counterterrorism transformation and intelligence reform. Rather, information sharing has been at the heart of a government reform movement that has sought to make the public sector more efficient and effective through the use of data. For example, in the 1990's, the New York Police Department (NYPD) implemented community policing reforms, based on sophisticated crime mapping, contributing to a substantial drop in crime. Since that time, many other police departments have adapted similar approaches.

At the federal level, the military and intelligence communities also were striving towards closer integration. For example, the Goldwater-Nichols Act of 1986 substantially reorganized the Department of Defense and its chain of command to allow for joint operations and achieve other efficiencies. The Goldwater-Nichols Act did so by eliminating stovepipes between the different military services (while preserving the distinct culture and identity of the Army, Navy, Air Force, and Marines.) During the 1990's, Director of Central Intelligence Robert Gates undertook initial steps toward similar reforms of the intelligence community.

Despite progress, the reforms did not go deep or fast enough. Following the attacks of September 11, a series of reviews uncovered failures of information sharing both within and between agencies. These failures were among the factors that resulted in the government's failure to prevent the attacks. The National Commission on Terrorist Attacks Upon the United States, commonly called the 9/11 Commission, described a number of information sharing failures and recommended a series of reforms to prevent such failures in the future.

2004 – 2006: ESTABLISHING AN INFORMATION SHARING ENVIRONMENT

Prompted by the 9/11 Commission recommendations, President Bush issued several executive orders, including Executive Order 13356, "Strengthening the Sharing of Terrorism Information to Protect Americans," (Aug. 27, 2004). E.O. 13356 required the heads of Departments and agencies to share terrorism information, mandating that "in the design and use of information systems . . . the highest priority" must be given to the "interchange of terrorism information among agencies." The order also established an Information Systems Council chaired by a designee of the Office of Management and Budget (OMB).

Congress also responded to the 9/11 Commission, both by removing legal barriers (real or perceived) and by establishing particular information sharing initiatives. In section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Congress established the Information Sharing Environment

(ISE). IRTPA defined the ISE as "an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section."[1] Section 1016 of IRTPA reinforced and codified many of the requirements of E.O. 13356, including the requirement to share terrorism information. Section 1016 established a Program Manager for the ISE and an "Information Sharing Council" as the successor to the Information Systems Council. Section 1016 also mandated the issuance of guidelines to protect privacy and civil liberties. Executive Order 13388, "Further Strengthening the Sharing of Terrorism Information to Protect Americans," (2005) replaced the earlier Executive Order and reinforced the IRTPA approach. This order again restated the imperative for agencies to share terrorism information with each other, subject to the requirement to protect privacy and civil liberties.

The structure and design of the ISE reflected, in large part, the vision of the Markle Foundation Task Force on National Security in the Information Age. In a report issued in 2002, the Markle Foundation had outlined its vision of a decentralized model for information sharing in which authorized users could access the information they needed to analyze threats, "connect the dots", and provide useful information to prevent harm to national security. The ISE addressed the major shortcomings that contributed to 9/11 – not a failure to collect too little information, but a failure to share, analyze and act upon information the government had already collected under its lawful authorities.

The ISE adopted a distributed, decentralized model. Instead of creating a central database of terrorism information, the ISE approach was to maintain control of information with the agency that collected or maintained it, with distributed sharing. IRTPA requires an ISE that "connects existing systems." The model enables operations across federal agencies as well as among the different levels of government and with private sector and international partners. This model also lessens the risks of privacy abuses, compromise, or data breaches.

The distributed model also had significance for information sharing well beyond the boundaries of the ISE itself, which is limited by statute to terrorism information. Because of the law's mandate to connect existing systems, and the reality that the systems being connected were and are, almost exclusively, not limited to terrorism information, the improvements to information sharing that the ISE realized were not – and generally could not be – limited to terrorism information alone. Rather, the ISE approach would inevitably lead – and did lead – to the establishment of best practices for information sharing and management generally in a number of areas (such as in the Controlled Unclassified Information (CUI) initiative discussed below).

[1] The Government Accountability Office (GAO) in its 2008 report described the ISE as "…a set of cross-cutting communication links—encompassing policies, processes, technologies—among and between the various entities that gather, analyze, and share terrorism-related information."

Through IRTPA, Congress also established a new office, with government-wide authority – the Office of the Program Manager for the Information Sharing Environment (PM-ISE). PM-ISE was charged with spearheading efforts to realize the vision of the ISE. The PM-ISE opened its doors on April 14, 2005.[2]

IRTPA did not specify in which agency the PM-ISE should reside, leaving that decision to the President. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, commonly called the WMD Commission, recommended that the PM-ISE should be placed within the newly created Office of the Director of National Intelligence (ODNI) in order to better coordinate the Program Manager's government-wide terrorism information sharing mission with the DNI's responsibility to improve intelligence information sharing. The White House accepted this recommendation. It directed the DNI to incorporate the PM-ISE and to administer "all of its personnel, funds and other resources, as part of the ODNI." It was understood that the PM-ISE would maintain a very close relationship with OMB and the White House generally.

Over the next several years, the ISE was made real through the adoption of a series of foundational documents and key programs. For example:

- The ISE initial implementation plan, as required by section 1016 of IRTPA, was issued in November 2006. It lays out a series of tasks required to achieve particular requirements of the statute, such as the requirement to provide directory services.
- The President issued a series of guidelines and requirements for the ISE in December 2006. These guidelines and requirements continue to embody the ISE's basic structure. They include the privacy and civil liberties guidelines required by the IRTPA (guideline 5), developed with input from privacy and civil liberties advocates and with the participation of the major counterterrorism, law enforcement, and other ISE mission partners.
- Guidelines were also issued for sharing with state, local and tribal sector entities and the private sector (guideline 2) and for sharing with international partners (guideline 4).
- A process to issue common terrorism information sharing standards. Several standards were issued pursuant to that process.

Signature initiatives enabled the information sharing that makes the ISE a reality. For example:

- Strengthening of a national network of state fusion centers (guidelines were issued in 2006);
- Major improvement and maturation of the terrorist watch list;
- The development of a nationwide system for documenting, vetting, and sharing suspicious activity reports (SARs). The SARs effort involved all aspects of the ISE approach – including building a program with the input of stakeholders from all levels of government and non-government organizations, using functional standards to guide decentralized sharing (i.e., no central database), and including privacy and civil liberties protections in the development of the standards and process for sharing SARs.

[2] Coincidentally, the PM-ISE moved into, and still occupies, the office space that the 9/11 Commission formerly occupied.

The Government Accountability Office (GAO) ensured continued focus on counterterrorism information sharing with a series of reports, and particularly with its decision in 2005 to place sharing of terrorism information among agencies and with state, local, private and foreign partners on the list of programs identified as "high risk." At the time, the Program Manager welcomed this designation because of the many challenges information sharing poses, and continues to engage with GAO on its approach and GAO's recommendations.

2007-2010: EXPANDING THE INFORMATION SHARING PRIORITY

In 2007, Congress enacted the Implementing Recommendations of the 9/11 Commission Act ("9/11 Act"), a major update to IRTPA. In so doing, Congress indefinitely extended the term of the Program Manager for the ISE (which had previously been limited to two years), added homeland security and weapons of mass destruction information to the ISE's scope, and included several new ISE attributes for information sharing. These amendments demonstrated that Congress valued the ISE approach to information sharing and had confidence in the efforts of the Executive Branch to bring it about.

The 9/11 Act also directed the Program Manager to report on the feasibility of replacing existing policies for information collection, sharing, and access with a standard allowing information to be accessed using a threat or mission based approach (commonly described as an "authorized use" standard.) Such a standard would require "mission-based or threat-based permission to access or share information" in order to accomplish "a particular purpose" that the government (in consultation with the Privacy and Civil Liberties Oversight Board) determines was lawful for "a particular agency, component, or employee." In response, the Program Manager determined that such an approach would not be a feasible replacement for existing rules and laws, but that such a standard would be consistent with the ISE approach if it worked within existing rules and laws.

The National Strategy for Information Sharing, issued by the White House in 2007, essentially replaced the earlier, more limited implementation plan under IRTPA with a comprehensive approach and an overall framework for counterterrorism information sharing that included many of the signature initiatives discussed above. The PM-ISE began to issue comprehensive annual reports on information sharing. Along with the annual reports, PM-ISE collaborated with the Office of Management and Budget and the White House staffs of the National and Homeland Security Councils to plan and execute information-sharing priorities across the government. The White House began to issue information sharing programmatic guidance, supplemented by more detailed implementation guidance issued by the PM-ISE.

This process essentially replaced the approach contained in the initial implementation plan issued in 2006 with an approach that was fully integrated with the government's annual budget and program priorities. One example of this approach in action was the comprehensive reform to handling what is now described as controlled unclassified information (CUI). An interagency policy review process identified over one hundred markings for sensitive, but unclassified information. There was no standard approach for such

markings, making exchange of such information for counterterrorism purposes, as for other valid purposes, difficult. The PM-ISE, using its government-wide authority and pursuant to Guideline 3 of the Presidential ISE guidelines, formulated and negotiated a process for standardizing "Controlled Unclassified Information" (CUI), first codified in a 2008 Presidential memorandum (later memorialized in Executive Order 13556). The CUI initiative is an example of how addressing a problem that impeded information sharing for counterterrorism purposes has made sharing for other valid purposes easier as well.

In 2009, the incoming Obama Administration made further adjustments to information sharing governance. Under Presidential Policy Directive 1, the Administration combined the White House staffs of the National Security Council (NSC) and the Homeland Security Council (HSC) and directed that day-to-day work would be supported by a combined National Security Staff (NSS). NSS leads "interagency policy committees" (IPCs), senior bodies on geographic or topical areas that do the bulk of the policy coordination work, raising issues to the deputies' or principals' committees of the NSC or HSC as appropriate.

In keeping with this new structure, the Information Sharing Council, an interagency body chaired by the PM-ISE and established by IRTPA section 1016, was integrated into the Information Sharing and Access Interagency Policy Committee (ISA IPC). The Program Manager became co-chair of the ISA IPC along with an NSS co-chair. The ISA IPC serves as both an IPC under PPD-1 and as the Information Sharing Council under IRTPA section 1016.

In addition, the ISA IPC was given a remit that is broader than the scope of the ISE. The White House memorandum establishing the ISA IPC provides:

> Achieving effective information sharing and access throughout the government is a top priority of the Obama Administration. This priority extends beyond terrorism-related issues, to the sharing of information more broadly to enhance the national security of the United States and the safety of the American people.

The ISA IPC, co-chaired by PM-ISE and the NSS Senior Director for Information Sharing and Access, has served as the principal interagency forum for information sharing issues, both those that concern the ISE itself and the broader issues related to sharing beyond the ISE's formal scope.

Pursuant to this new approach, the ISA IPC has launched new initiatives, particularly in the areas of standards development with industry, with a goal of influencing government-wide procurement of information technology systems. It has focused its attention on critical infrastructure and key resources, and the need to partner with the private sector to further strengthen information sharing. Another major effort has been in the area of data aggregation, i.e., ensuring the right policy approach for aggregation of high-value terrorism-related data sets.

2010 – PRESENT: INCREASING INFORMATION SHARING AND SAFEGUARDING

The next major development in this brief history of the ISE concerns safeguarding information that is shared. In 2010, the website WikiLeaks published, in cooperation with leading newspapers including the New York Times, a trove of secret diplomatic cables allegedly downloaded and provided to WikiLeaks by a 23-year-old Army private, Bradley Manning. This development led some to question whether sharing had gone too far, endangering sources and methods. However, the reaction of national security leaders was not to jettison or slow the pace of sharing, but to refocus on the need for sharing to go hand-in-hand with safeguarding of sensitive information.

Following a comprehensive interagency review, President Obama issued Executive Order 13587, "Structural Reforms to Improve Sharing and Safeguarding of Classified Information on Computer Networks." EO 13587 established several new interagency bodies to coordinate efforts to improve security on classified networks, including a Senior Information Sharing and Safeguarding Steering Committee, an Insider Threat Task Force, and an Executive Agent for Safeguarding comprised of the National Security Agency and the Department of Defense.

To ensure that information sharing efforts are complemented with appropriate safeguarding efforts, EO 13587 also established a Classified Information Sharing and Safeguarding Office (CISSO) within the PM-ISE. Like other bodies established in EO 13587, CISSO's work is focused on classified information on computer networks, a category that is both broader than the ISE (because it includes all such information, not just terrorism, homeland security, and WMD information) and narrower (because it covers only classified information on computer networks).

As discussed above, the PM-ISE already had considerable expertise and experience in sharing and safeguarding of Controlled Unclassified Information (CUI) and classified terrorism information. Indeed, the CUI initiative originated within PM-ISE before being handed off to the National Records and Archives Administration (NARA). Many of the issues concerning sharing and safeguarding were similar whether the information was classified or unclassified, but sensitive. The establishment of CISSO and the integration of its work with the larger information sharing and safeguarding mission was a significant broadening of the PM-ISE's role in responsible information sharing.

Finally, the efforts to improve information sharing internationally continue. Canada and Mexico have deepened their information sharing initiatives and have established sharing of best practices with the PM-ISE. Of note, Canada has actually established its own PM-ISE, modeled on the United States PM-ISE.

THE FUTURE OF RESPONSIBLE INFORMATION SHARING

The success of information sharing efforts in the decade since September 11 does not mean that the issues have been resolved, or that information sharing should be given a lower priority in the present decade. Instead, for a host of reasons, such efforts need to be accelerated and broadened to other classes of information – for example, to include other priority crimes, such as transnational organized crime and drug trafficking, human trafficking, and cyber crime and other cyber threats. These efforts reflect the government's basic responsibility to provide information to enable action to protect the American people, as well as the more prosaic need to enhance efficiency in an era of budget cuts and resource constraints.

The Administration continues to advance responsible information sharing to protect the American people and enhance the national security. The vision is to ensure that the right data is available to the right people at the right time in order to enable action to enhance national security and protect the American people. The existing performance, management, and governance structures of the ISE are to be leveraged to support this overall strategy. Meanwhile the Program Manager is committed using this approach to work with GAO to remove government-wide terrorism related information sharing from the high risk list.

Sharing of additional categories of information, and use of such information to support decisions needed to protect the public, will benefit from the best practices and tools developed by the ISE. For example, the ISE is increasing its focus on assured sharing for cybersecurity-related information. Cyber threat information can benefit from the same standards, policies, and processes that have been successful in sharing counterterrorism information. Such policies include extending ISE privacy and civil liberties protections to the sharing of cyber threat information among federal and non-federal partners. Cybersecurity sharing represents both a future challenge and a future opportunity for success.

As the head of the national office for responsible information sharing, the Program Manager and the White House are working together to:

- **Advance responsible information sharing to further the counterterrorism and homeland security missions.** The goal is to enable all levels of government to make decisions to prevent harm to the American people, empowering them with more effective and efficient capabilities. The domestic information sharing architecture should be configured to allow assured discovery and sharing of information across data holdings through interoperability, standards-based acquisition, and advanced analytic capabilities. All this must be accompanied by enforcement of information sharing and safeguarding policies that data originators will trust, and that ensure protection of privacy, civil rights, and civil liberties.
- **Lead a transformation from information ownership to information stewardship**, grounded in the view that information is a national asset that must be used and safeguarded to benefit the American people. Increasingly tight public safety budgets demand a standards-based approach

that will allow shared services, greater interoperability, and more efficient use of existing systems by facilitating secure interconnection of those systems. Likewise, information sharing policy can benefit from greater standardization, by developing reusable, standardized information sharing agreements that respect the equities of disparate organizations and provide strong protections for privacy and civil liberties.

- **Promote partnerships across federal, state, local and tribal governments, the private sector, and internationally.** Engagement, training and management support are key to building the organizational capacity of our partners at all levels. Successful engagement will help create a culture shift that will instill partners with an enduring commitment to responsible information sharing.

The federal government and its state, local and tribal counterparts have achieved significant information sharing success and continue to face substantial challenges. The lessons from these success and challenges will be invaluable as the nation enters a new chapter in what is still quite a new era – the era of responsible information sharing.