# A Legal and Policy Approach for Responsible Information Sharing:

## The Role of the Information Sharing Environment (ISE)

Responsible information sharing requires policy mechanisms and legal authorities that encourage sharing, with appropriate safeguards, as well as a proven way to resolve legal and policy issues that may impede such sharing. The Information Sharing Environment (ISE) established by the Intelligence Reform and Terrorism Prevention Act (IRTPA) offers a successful legal and policy approach for information sharing and safeguarding. That model could be adopted and used to support the Administration's broader information sharing goals.

Information sharing and safeguarding challenges exist at all levels of government – federal, state, local, tribal – with our international partners, and in the private sector. Under the IRTPA, the role of the Program Manager for the Information Sharing Environment (PM-ISE) is to facilitate progress to resolve these challenges within the scope of the ISE – i.e., to facilitate responsible information sharing to combat the threats of terrorism and Weapons of Mass Destruction (WMD), and to promote homeland security.

PM-ISE has at its disposal a set of foundational legal authorities, contained in section 1016 of IRTPA. Using these authorities, PM-ISE has worked with an array of stakeholders to implement privacy guidelines, to help establish a national network of state-run fusion centers, to design and implement a system for sharing suspicious activity reports (SARs) with protections for privacy and civil liberties, and to use the National Information Exchange Model (NIEM) to facilitate responsible information sharing.

IRTPA also lists a set of attributes that provides a roadmap for effective information sharing. These attributes describe what effective information sharing should look like. This roadmap requires constant adjustment as information sharing initiatives mature within the Departments, agencies, states, local governments, and other stakeholders in order to serve the variety of their mission needs and priorities.

PM-ISE does not work alone. It works with White House and other senior federal officials to formulate policy; it works with stakeholders at the state and local levels to understand their needs and reflect them back to leaders at the federal level; it supports the setting of budget priorities and influences resource allocation to

incentivize responsible information sharing. PM-ISE uses the authorities granted by IRTPA in a way that complements the authorities and responsibilities of its partners.

### THE PROMISE OF INFORMATION SHARING

The information entrusted to the government is a national asset. The challenges we face to our national security - foreign and domestic - cannot be addressed by one agency or by one level of government. Indeed, these challenges cannot be faced by the public sector acting alone, or by the United States acting unilaterally. Terrorism, homeland security, war and peace, securing our global supply chain, securing cyberspace, and other threats cross boundaries and domains of activity.

Information, provided by the American people or developed on their behalf by local, state, territorial, tribal, and federal agencies, is held in trust by those agencies. Effective collaboration is a cornerstone of our national security strategy and is essential to strengthening our national security to counter those who would do us harm. Information must be responsibly shared and safeguarded, not as an end in itself but to inform decisions needed to prevent harm to the American people. In short, we need to share the right data, any time, any place, make the data usable by any authorized consumer; prevent sharing only by law or policy, not technology, and protect information by a comprehensive regime of accountability.

This paper explains how the PM-ISE uses its authorities under IRTPA to address the challenges of responsible information sharing within the ISE and provide best practices for responsible information sharing beyond the ISE. Further use of the ISE approach beyond the categories of terrorism, homeland security, and WMD information could effectively support the Administration's goals for responsible information sharing to protect the American people and strengthen the national security.

## PART I. WHY IT WORKS: A PERFORMANCE-BASED APPROACH TO INFORMATION SHARING AND SAFEGUARDING

Proposals to share data across entities often encounter a familiar refrain: "There's a legal problem – we can't share the information." Part of the frustration with information sharing on an ad hoc basis is that such "legal" issues seem to recur despite having been addressed in the past and sometimes despite having been debunked in the past, and can stymie efforts that are already difficult enough for budgetary, technological, or management reasons.

The last decade, however, has seen substantial progress in information sharing, and the legal and policy approach established in the Information Sharing Environment (ISE), supported by information technology approaches such as the National Information Exchange Model (NIEM), has been a major reason why. Problems that have appeared in the past to be intractable start to appear more manageable.

For example, one reason for the multiplicity of watchlists prior to September 11 was that different agencies had different legal authorities and rules with respect to terrorism information concerning United States persons. It was widely believed that a coordinated list simply was not possible in such circumstances. Similarly, sharing of suspicious activity reports among entities at different levels of government, or across jurisdictions, ran into legal and privacy concerns. State and local agencies are bound by the rules for criminal intelligence systems contained in 28 C.F.R. part 23, while federal agencies (such as the FBI) operate under different investigative guidelines and data retention rules.

The ISE does not answer these questions directly, but it does provide an approach for addressing information sharing legal challenges. First, it begins with the mission and authorities that already exist within Departments and agencies at all levels of government to facilitate responsible information sharing. Second, it provides a mechanism for addressing the principal legal challenges to information sharing.

## "THERE'S A LEGAL PROBLEM": UNDERSTANDING THE ISSUE.

Federal, state, local and tribal governments obtain, manage, and use information in the course of a wide variety of missions. They collect, manage, safeguard, share, disseminate and dispose of information under their own distinct legal authorities. The data they maintain is subject to a variety of real as well as perceived legal restrictions. The term "legal problem" can cover a wide variety of issues, ranging from genuine legal problems, to more or less legitimate concerns about agency authorities or "turf," to policy constraints or simple misunderstandings.

### GENUINE LEGAL PROBLEMS.

The "legal problem" may reflect a specific legal restriction that limits the sharing of certain data (or allows the sharing of information only under certain circumstances which are not satisfied by the proposed sharing arrangement). These restrictions are often for valid or even highly compelling reasons, such as to protect privacy and civil liberties, or to abide by court orders regarding the handling of information, or to fulfill important statutory responsibilities such as the protection of sources and methods. Or the restrictions may reflect outdated legal rules or overly restrictive legal interpretations that need to be revised or updated, but that must be adhered to as long as the existing legal restriction or interpretation is operative. In either case, the legal problem is real and the information cannot be shared – or, at least, can only be shared subject to conditions that satisfy the law – at least, until the law or overly restrictive interpretation is changed, if a change in the law is in fact desirable.

### AGENCY AUTHORITIES OR "TURF."

The "legal problem" may reflect a concern that data, collected by a particular entity under its legal authorities, simply should not be made available to a different entity with a different mission and different legal authorities. For example, agency X does not feel its data holdings are relevant to Agency Y's mission, and believes Agency Y's request for its data intrudes upon Agency X's responsibilities as provided by law. Note that this is dissimilar to the legal problem described above because it is not a

limitation on sharing per se. The risk in this instance is that Agency X's position may reflect culture or turf issues masquerading as issues of agency legal authorities.

### POLICY CHOICES AND MISCOMMUNICATION.

And finally, the "legal problem" may also simply reflect miscommunication or policy choices. For example, a sharing arrangement may be under review to identify *whether* there are any legal barriers, and this may create a perception that there is a "legal problem" with the arrangement and that it should therefore be abandoned. Or the "legal problem" may in fact reflect policy decisions about the *risks* of sharing that are incorrectly characterized as legal restrictions. In other words, it may be that the law does permit Agency X to share its data with Agency Y, and that Agency Y has a valid need for that data to execute its mission under its legal authorities, but that Agency X does not trust Agency Y to comply with valid legal requirements (or policy requirements intended to implement legal rules). Since Agency X controls its own compliance mechanisms and can manage its own compliance risks, but does not control Agency Y's compliance mechanisms, it rejects the sharing arrangement.
The ISE does not provide a magic bullet for resolving any of these issues, but it does represent a unique approach to encouraging resolution of them.

### IRTPA'S PERFORMANCE BASED ADVANTAGE.

Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA), as amended, provides a performance based approach that promotes appropriate sharing and safeguarding of terrorism, homeland security, and WMD-related information. It provides a detailed roadmap for information sharing that includes – uniquely – a series of attributes describing what effective information sharing should look like, a performance management approach to help the government get there, and set of a duties and responsibilities both for the Program Manager and for participating agencies at all levels of government.

IRTPA lays out a detailed list of attributes -- including requirements related to security -- for the sharing of terrorism, homeland security and WMD information. Of the fifteen attributes that must be provided or supported by PM-ISE policies and plans, all are designed to facilitate greater information sharing, and to some extent, information safeguarding. Some of the more notable attributes of this approach are requirements to connect "existing systems," build upon "existing systems capabilities," and incorporate "legacy technologies." These requirements help ensure against creating new stovepipes for counterterrorism sharing.

Information sharing systems should have "no single points of failure," and allow for "direct and continuous online electronic access to information." Critically, the information should be made available "in a form and manner that facilitates its use in analysis, investigations and operations." In other words, information sharing is not an end in itself. Rather, the purpose of sharing information is to enable action to prevent harm.

To ensure that information is safeguarded as well as shared, the IRTPA mandates "an information access management approach that controls access to data rather than just systems and networks, without

sacrificing security." Information should be shared "at and across all levels of security." Sharing must include "protections for individuals' privacy and civil liberties" as well as "strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls." These mechanisms are useful for ensuring compliance, including compliance with privacy policies, and policies to protect classified or otherwise sensitive information from unauthorized disclosure.

The ISE attributes require a distributed, horizontal approach, allowing "the full range of analytic and operational activities without the need to centralize information." The environment should permit "analysts to collaborate both independently and in a group" and across multiple levels of classified and otherwise sensitive information.

These and other detailed attributes provide a roadmap not only for sharing, but for *assured* information sharing. If implemented poorly, greater sharing of information (including classified information) introduces new vulnerabilities. If implemented properly, there should be no conflict between sharing and safeguarding, and indeed the right policies, guidelines, procedures, and standards to bring about these attributes may even strengthen security. For example, sharing "at and across all levels of security" could introduce new risks if done improperly, but if done correctly should incorporate technical, policy and other controls to protect that information, commensurate with its security requirements.

## PERFORMANCE MANAGEMENT APPROACH.

To achieve the desired environment described by the attributes, the law lays out a performance management approach. Under section 1016(b) of IRTPA, the President is instructed to issue guidelines for the ISE and to "*determine* and *enforce* the policies, directives, and rules that will govern the content and usage of the ISE." These authorities have been delegated to the PM-ISE, through the Director of National Intelligence. The PM also has his own authorities pursuant to IRTPA, including government-wide authority to issue "policies, procedures, guidelines, rules and standards." IRTPA section 1016(f). As explained below, under IRTPA section 1016(i), agency compliance with these requirements is mandated whether such requirements are established under the PM's own authority (under section 1016(f)) or under the authorities delegated by the President (under section 1016(b)). The annual report is the mechanism for measuring the success of these policies and directives.

Policies are established after consultation with the Information Sharing Council (ISC), which has now been integrated into the Information Sharing and Access Interagency Policy Committee (ISA IPC). Under section 1016(g), agencies must contribute to this governance process, and provide detailees to support the PM-ISE. Subsidiary groups of the ISA IPC also include representatives of state, local and tribal organizations. Industry representatives participate by membership in the Standards Coordinating Council, another subsidiary group of the ISA IPC. These mechanisms allow the ISE to reflect a much broader constituency, providing a perspective that reaches outside the federal government.

Implicit in the law is the obligation for agencies to organize their own information sharing and information management (including safeguarding) approaches so that they contribute to the delivery of the ISE. The policies are, by law, not optional but mandatory for the heads of federal departments and

agencies, at least within the scope of information governed by the ISE. IRTPA specifically lays out "agency responsibilities" along with the authorities given to the President and the Program Manager. Section 1016(i) provides that the "head of each department or agency that possesses or uses intelligence or terrorism information" or is otherwise involved in the ISE "shall:"

- ensure full department or agency compliance with information sharing policies, procedures, guidelines, rules, and standards established under subsections (b) and (f) of this section;
- ensure the provision of adequate resources for systems and activities supporting operation of and participation in the ISE;
- ensure full department or agency cooperation in the development of the ISE to implement government-wide information sharing; and
- submit, at the request of the President or the program manager, any reports on the implementation of the requirements of the ISE within such department or agency.

Properly implemented, the guidelines, directives, and standards that constitute the ISE provide a mechanism for resolving the "legal issues" that often seem to stymie information sharing efforts. The ISE gives participating entities a governance process by which they can raise issues for discussion and, if necessary, elevate any unresolved issues for decision. The ISE Privacy Guidelines and other governing rules provide an approach for safeguarding information and measuring compliance with valid legal or policy restrictions.

The requirement to comply with ISE directives provides the enforcement mechanism to flush out bureaucratic inertia, inattention, or turf-related resistance to responsible information sharing.[1]

## PART II. WHAT IT CAN DO. APPLYING THIS MODEL TO SUPPORT THE ADMINISTRATION'S BROADER INFORMATION SHARING GOALS.

While the scope of the ISE is terrorism, WMD, and homeland security information, the challenges to national security and the safety of the American people are much broader. They include serious transnational crime, pandemics, cyber attacks, and a host of traditional and emerging threats that require timely, relevant information to prevent harm or inform actions.

Information sharing and safeguarding initiatives, whether or not formally part of the ISE, will necessarily resemble the IRTPA approach. The legal issues (real and perceived) that frustrate information sharing in the terrorism context also exist in other contexts. In those other contexts, these issues also generally

[1] PM-ISE has used these authorities to resolve a variety of difficult information sharing challenges, in coordination with its mission partners. Examples are further described in "A Brief History of the Information Sharing Environment," and in much more detail in the ISE annual reports from 2007 to 2012.

represent a range of concerns including genuine legal barriers, competing agency authorities, policy choices, and miscommunication. The ISE model has proven effective in addressing these problems in information sharing to support decisions necessary to combat terrorism. It also can be used to facilitate responsible information sharing to support other classes of decisions.

In fact, the policies, guidelines, standards and rules adopted for counterterrorism sharing are already being used by agencies at the federal and state level for broader purposes. Fusion centers do not merely analyze counterterrorism information; they analyze all crimes and threats relevant to their areas of responsibility. The National Information Sharing Exchange Model (NIEM) is used not only for counterterrorism purposes, but for other lawful purposes where information needs to be standardized to be shared effectively.

The IRTPA approach is well suited to being expanded beyond its initial purpose. IRTPA did not mandate a centralized database for counterterrorism information, but rather a horizontal, flexible environment that facilitates information sharing between and among entities across the federal government and with state, local, tribal, private sector and international partners. These partners have no desire to fragment their missions artificially, using one information management approach for data labeled "counterterrorism" and a different approach for other public safety and national security missions. IRTPA does not permit such fragmentation in any event, as the law requires a sharing environment that "connects existing systems" rather than creating new ones, and the "existing systems" are – with very few exceptions – not limited to counterterrorism information.

Indeed, the IRTPA model reflects an important insight about information sharing to protect the American people and enhance national security, which is that discrete arenas such as terrorism, serious transnational crime, homeland security, and cybersecurity do not really describe classes of information. Rather, they describe classes of <u>decisions</u> to address serious problems. The responsible sharing of information is required to support these classes of decisions. The Markle Foundation and the WMD Commission recognized this reality when they recommended the adoption of an "authorized use" standard for accessing lawfully collected information – a standard that would ask whether the person seeking the information had authority to do so in order to make use of it for a particular, important purpose such as counterterrorism.

Congress directed the PM-ISE to consider replacing existing standards for collection, sharing and access to information with an "authorized use" standard. <u>See</u> IRTPA § 1016(j)(1)(C). The PM-ISE determined that adopting the "authorized use" standard described in IRTPA as a wholesale replacement for existing law was not feasible, but that such an approach could be useful if it worked within existing law. The basic insight – that the purpose of information sharing is to support classes of <u>decisions</u> – is basic to the successful achievement of the Administration's responsible information sharing goals.

For all these reasons, the IRTPA approach can and should be adapted beyond terrorism, WMD and homeland security information by leveraging the successes of the ISE with the other legal authorities and requirements for sound information management that are already reflected in law and in the existing legal authorities and responsibilities of the participating agencies. Put another way, the approach outlined

above could aid in facilitating information sharing to better inform other decisions necessary to protect public safety. These would include, in addition to terrorism, other priority or serious crimes, such as transnational organized crime and drug trafficking, human trafficking, cyber crimes, and similar areas that suffer, as a result of real or perceived legal complexity, from the same problems.

This approach would use many of the mechanisms of the ISE to achieve the Administration's broader responsible information sharing goals. In many cases, these goals can and are being met in the context of the ISE itself, using the authorities embodied in section 1016 of the IRTPA. Departments and agencies that are involved in counterterrorism also have a variety of other missions. Their information systems, and information sharing activities, are not fragmented into counterterrorism and everything else. As discussed above, IRTPA itself recognizes this and requires the ISE to adopt an approach that "connects existing systems."

In areas in which information sharing activities are required that are generally outside the core scope of terrorism, WMD and homeland security information (or the newer mission for classified information sharing and safeguarding under EO 13587), the objectives of building a horizontal information sharing environment could be accomplished through a variety of other legal authorities and mechanisms, as discussed below, as well as through the use of the legal authorities of the participating agencies themselves. These authorities stem not only from legislation but also from the President's authority to supervise and organize the Executive Branch. Of course, Congress could always confirm this approach by taking action formally to expand the scope of the ISE, as envisioned in IRTPA. See IRTPA § 1016(g)(2)(I).

Presidential Policy Directive 1 (PPD-1) empowers interagency policy committees, such as the ISA IPC, to coordinate national policy. The ISA IPC thus already has the authority (at least where it can achieve agreement among its participants) to direct information sharing and access initiatives quite apart from section 1016 of IRTPA. This governance approach, anchored in the President's authority, has at its disposal a host of additional, more specific authorities and legal tools to strengthen information sharing and safeguarding.

OMB's mission is both to develop the budget and to manage the execution of those funds in accordance with Administration priorities. The IRTPA authorities and the PM-ISE's efforts already assist OMB's execution of this mission as it relates to information sharing and safeguarding. The ISE Annual Report is integrated fully with this OMB process and serves to measure progress. For example, IRTPA requires that the annual report include "an accounting of how much was spent on the ISE in the preceding year." OMB and the National Security Staff also issue programmatic guidance to agencies on information sharing priorities, and PM-ISE supports this process and the delivery of the ISE by issuing more detailed implementation guidance for the ISE and by working with OMB to develop resource allocation criteria.

Through OMB integration and in other ways, the PM-ISE's policies, guidelines, standards, rules and procedures can be adopted across the variety of missions for which agencies are responsible. The President, through OMB and through the National Security Council and Homeland Security Council (supported by the National Security Staff and the ISA IPC), has authority for supervising the Executive Branch and for the sharing and safeguarding of all information within the Executive Branch (consistent

with law), as well as the intersection of such policies with other entities, including state, local and tribal governments, international partners, and the private sector.

Because ISE guidelines and policies inevitably impact the manner in which mission partners share and safeguard all their information, information sharing and safeguarding must be carried out in close coordination with mission partners and the exercise of ISE authorities should be leveraged with the exercise of other legal authorities to share and protect information. If properly coordinated through White House leadership, these additional authorities will augment, rather than compete with, ISE authorities.

For example, OMB has broad authority over information security under the Federal Information Security Management Act (FISMA). This includes the authority for "developing and overseeing the implementation of policies, principles, standards, and guidelines on information security . . . ." 44 U.S.C. § 3543(a)(1). OMB's authorities extend to all information systems except national security systems, which are reserved to the Secretary of Defense and the Director of National Intelligence. OMB is instructed to ensure that NIST guidelines and standards are coordinated with the National Security Agency (NSA) and others operating national security systems to ensure such guidelines and standards are "complementary."

The OMB Director's authority to implement "policies, principles, standards and guidelines" for information security for all non-national security systems is similar to the PM's authority with respect to the ISE. The key differences are that 1) FISMA lacks the detailed attributes that make IRTPA a performance-based law, and 2) the OMB Director's authorities extend to all non-national security systems rather than only terrorism, homeland security and WMD information. The bifurcation of information security authorities between national security systems and non-national security systems is a critical difference between FISMA's approach and the IRTPA approach which governs both.
Pursuant to the Clinger-Cohen Act (which includes the Information Technology Management Reform Act), OMB is also given the responsibility of improving the acquisition, use, and disposal of information technology to improve federal programs. These responsibilities are handled through the federal Chief Information Officer (CIO) Council, chaired by OMB and composed of Department and agency CIOs. Both security and interoperability are key components of a sound information technology management approach, and so Clinger-Cohen offers additional support for OMB's ability to contribute to the information sharing and safeguarding mission.

Finally, OMB's roles under both the E-Gov Act and the Privacy Act have a very significant impact on information sharing and safeguarding. Under the E-Gov Act, OMB issues guidance to Departments and agencies on the preparation of Privacy Impact Assessments (PIAs), which are required for new information systems (other than national security systems) but have also become a widespread tool for examining the privacy impact of new programs and policies. OMB has required that federal Departments and agencies designate "senior agency officials for privacy," and Congress has also designated, by statute, a number of Department and agency privacy and civil liberties officers. OMB also issues guidance for implementing the Privacy Act, which contains requirements for notice, transparency, record access and correction, for federal systems of records containing personally identifiable information of United States citizens and residents.

# CONCLUSION

The federal government has available a host of Departments, agencies and offices with significant legal authorities to ensure the appropriate sharing and safeguarding of information needed to protect the American people. OMB and the Information Sharing and Access Interagency Policy Committee (ISA IPC) provide policy coordination and direction from the White House. Participating agencies themselves possess organic legal authorities that can be used in furtherance of responsible information sharing.

PM-ISE's authorities over the Information Sharing Environment are subject-matter based, cover both sharing and safeguarding, and provide a roadmap of attributes that lays out a vision for what effective information sharing looks like. The use of these authorities has already driven successful instances of appropriate, assured information sharing that includes significant information safeguarding components.

Responsible information sharing involves much more than technology challenges. Success will require an approach that addresses legal and policy challenges effectively. The ISE authorities provide a way to achieve that goal. If implemented to support broader information sharing objectives, they will achieve broader information sharing successes, while safeguarding important values such as the protection of privacy and civil liberties. Addressing the legal and policy requirements, no less than the technology challenges, is essential to ensure that information gets to the right people, at the right time -- and with the right legal protections.