A Conversation with Kshemendra Paul
Program Manager, Information Sharing Environment

It is critical to the safety and security of this country that federal, state, local, private-sector, and international partners improve their sharing of information about terrorism, homeland security, and weapons of mass destruction. When examining the full scope of information sharing and protection, many widespread and complex challenges must be addressed and solved by multiple agencies and organizations working together. The risk of a future WikiLeaks incident can be reduced, but fixing these government-wide challenges is complex, difficult, and requires a staying commitment. To do this right involves cultivating the horizontal, cross-cutting, data-centric information sharing and protection capability.

What is the Information Sharing Environment? How is information sharing maturing across the ISE? What are the biggest challenges facing the ISE? To what extent does the pursuit of standards limit or defeat innovation? Kshemendra Paul, Program Manager, Information Sharing Environment, joined me on The Business of Government Hour *to explore these questions and more. The following provides an edited excerpt from our interview. – Michael J. Keegan*

On the Information Sharing Environment

The ISE is a complicated topic. The ISE is a collection of normalized mission and technical capabilities distributed and decentralized across all of our mission partners—federal, state, local, tribal, and private sector entities. The ISE is delivered by interconnecting existing networks, systems, and databases working with industry and standards bodies to adopt required standards and other frameworks. The ISE harmonizes and standardizes information processes based on shared mission equities. Finally, the ISE strengthens information safeguards, including protecting the privacy, civil liberties, and civil rights of the American people. A practical way of thinking about the ISE is to think of it as an information analogue to the interstate highway system. The same way the interstate highway system knit together this country post-World War II, the ISE is intended to be the information fabric enabling whole-of-government responses to national security and public safety challenges that face our nation. [The ISE provides analysts, operators, and investigators with integrated and synthesized terrorism, weapons of mass destruction, and homeland security information needed to enhance national security and help keep our people safe.]

On the History and Mission of the Office of the Program Manager for ISE

My office is a core part of the government's response post-9/11. It was called for directly by the 9/11 Commission. In fact, a series of seminal reports issued by the Markle Foundation in the last decade really sketched out in detail the vision for the Information Sharing Environment. The statutory and policy foundation for the office derive from three pillars: the Intelligence Reform and Terrorism Prevention Act of 2004, Executive Order 13388 (further strengthening terrorism-related information sharing), and the 2007 National Strategy for Information Sharing.

From its inception, the PM-ISE has had two key focus areas: first, we have focused on the information sharing

architecture—focusing on the nexus between public safety and national security, or what some in the law enforcement community call the nexus between homeland security and hometown security. Second, our office has had a focus on identifying, integrating, and disseminating best practices around responsible information sharing, management, and integration. [Ultimately, the PM-ISE works with mission partners to improve the management, discovery, fusing, sharing, delivery of, and collaboration around terrorism-related information. It facilitates the development of the ISE by bringing together mission partners and aligning business processes, standards and architecture, security and access controls, privacy protections, and best practices.]

My office has just under 30 government employees, with half agency assignees working on specific projects on behalf of those agencies and also detailees. We have a number of contractors augmenting the skills of our government team. We're organized into four divisions plus two supporting teams. The four divisions are Mission Programs, where we work with state and local law enforcement and other mission programs across the government; the Standards and Architecture division, our primary touchpoint with industry; the Assured Interoperability division, which has a technical CIO program coordination function; and the Management and Oversight division, which focuses on performance budget integration, strategic policy, and governance work. The two supporting teams that work across all four divisions include stakeholder engagement and staff operations. Our budget is between 20 and 25 million dollars a year. Under a third of that budget goes to pay for government employees and administrative expenses. Over a third goes to support contractors; about another third goes to support the implementation fund, which is a unique capability of our office to provide seed funding to accelerate development of the ISE.

On Leading the PM-ISE

As we are not in the chain of command, my specific responsibilities as program manager are to plan for and oversee the agency-based build-out and management of the Information Sharing Environment. The President, via the director of national intelligence, has also delegated his responsibilities as relates to the Information Sharing Environment. In particular, we are tasked with implementing guidelines for five core areas—privacy, common standards, a common framework for sharing between federal, state, local, tribal, and private sectors, controlled unclassified information (which has now moved to the National Archives), and international information sharing. We do this across five communities: law enforcement, homeland security, intelligence, defense, and foreign affairs. Additionally, the White House sets annual priorities through programmatic guidance issued jointly by the National Security Staff and OMB to the agencies.

How do we actually operate? I put it into three buckets. We have a top-down, a bottom-up, and an outside-in approach to how we operate and engage. I explore each approach at length in the ISE annual report to Congress. You can find that on our website, www.ise.gov.

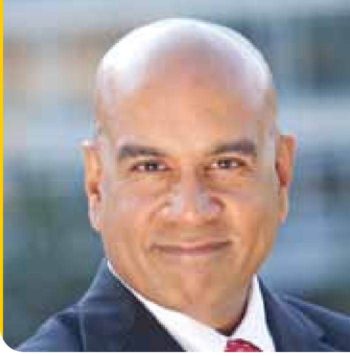
Top-down approach. Regarding the top-down approach, I co-chair a White House policy committee around information sharing and access. We work closely with OMB on implementation guidance to the agencies. In this instance, our most powerful tool is our ability to identify best practices and share them among the various communities that compose the ISE.

Bottom-up approach. Our second approach is bottom-up. Since our inception, we've been focused on the domestic architecture, information sharing, and intelligence. Our strongest advocates are state and local agencies and the law enforcement community. They have become fully integrated partners in the national information sharing architecture, the national network of fusion centers, and suspicious activity reporting. In doing all this, we are viewed as an honest broker. We're able to convene and bring these stakeholders into the national policy conversations around responsible information sharing.

Outside-in approach, We also have an outside-in approach, which involves working with industry and standards organizations to mature interoperability standards, looking for

"The whole point of information sharing is not simply to share information, but to get information to the proper decision-maker, so they can make better, more proactive decisions that protect the American people and enhance national security."

— *Kshemendra Paul*



opportunities to leverage procurement policy so agencies can buy interoperable solutions, and creating capabilities to deliver the Information Sharing Environment.

We're not in the chain of command, but we've crafted an innovative approach that combines traditional top-down with bottom-up and outside-in approaches. We have momentum in all those dimensions, which enables us to be a platform for agencies to drive informational transformation.

On Challenges Facing the PM-ISE

Accelerating responsible information sharing. Eleven years after 9/11, the number one [challenge] is retaining that urgency for accelerating responsible information sharing. We've made progress, but there's more work to do and it requires focus and prioritization.

Budget constraints. The number two challenge may be a somewhat new development, but it is just as big an issue. It's the structural financial challenge facing all government agencies. It's bad at the federal level. It's much worse at the state and local level.

Evolving threats. The number three challenge is the evolving and increasingly integrated threats that span national security and public safety missions. Terrorism is a great example, but things like cyber, human trafficking, transnational organized crime, prescription drug diversion—there's a whole variety of missions and threats … that are increasingly integrated and intertwined and evolving.

These two challenges go together. As a result, we need to keep front and center the top priorities of our stakeholders. We also provide economies of scale—an efficiency imperative that we need to realize with our work. The tools we provide the ISE will reduce duplication and redundancy, leading to increases in productivity. Regarding continuously evolving threats, our mission partners seek to leverage the assets we put in place as a community. These include the national network of fusion centers, for example, to address additional threat areas.

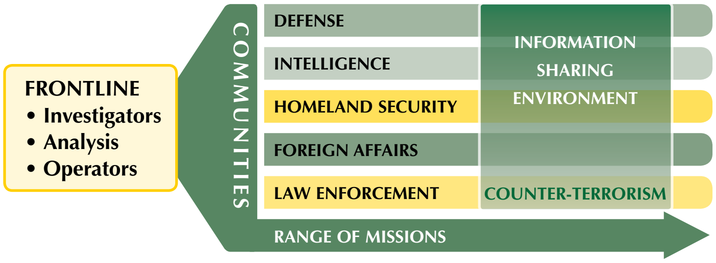
Information tsunami. The fourth challenge involves the information tsunami—simply, the quantity of information and available data, and the imperative to correlate disparate bits of information across the distributed ISE.

Given the volume of data, our best-practices approach to responsible information sharing plays a key role in shifting through the data and assisting the ISE owners. For example, we're working with several agencies, such as DHS, to improve how terrorism-related data move across the government. We're able to implement enterprise data management ideas; we've developed repeatable processes and leveraged shared services. These activities will result in gaining efficiencies over time while also improving data quality.

On Issues Facing the ISE Community

From the view of the agencies and our mission partners, there are two specific issues. First, these agencies are all under varying degrees of financial pressure. It's either bad or really bad, and [involves] the degree to which working with a government-wide initiative such as the ISE can be viewed as a tax versus an enabler; as a result folks are wary. Second, The figure below depicts a notional view of the ISE, portraying some of the major mission processes, core capabilities, and enablers.

Mission Processes	LE	SAR	Watchlisting	Screening	
Core Capabilities	Fusion Centers	SLT Information Needs	CUI Framework	SBU Interoperability	
ISE Enablers	Standards & Architecture	Privacy & CL	Protection & Access	Governance	



Source: http://ise.gov/scope-ise

as a government, we're still fragmented with our programmatic management processes and how we make decisions across agencies and programs. These two themes are not new and go beyond the ISE, reflecting the characteristics of most government-wide initiatives. The PM-ISE, through our implementation fund and dispute resolution capability, seeks to assist our mission partners. We fund high value projects that lead to the development of core capabilities of the ISE; for example, our work on the NSI as well as a project with the Domestic Nuclear Detection office, integrating real-time rad-nuke sensor data across federal, state, local stakeholders.

We're also able to facilitate the resolution of disputes. Though we're not in the chain of command, we're seen as an honest broker. We bring the variety of tools to help identify creative solutions. We're staying invested in a tool we call Building Blocks of the ISE. You can find it on our website, www.ise.gov. Building Blocks is a knowledge management tool [incorporating] work that we've done over the last number of years, the work in the interagency partners, federal, state, local; and packaged it in different functional areas, answering questions. It almost becomes a how-to for folks that want to do responsible information sharing, want to leverage the best practices that we've packaged but … aren't students of the ISE, don't live in … the work that we do every day. So we've got a lot of good feedback on that, and we see it as a first step towards, again, packaging our work and making it more accessible to folks to be able to leverage at arm's length.

We've taken the work we've done and packaged among our different functional areas. We've received good feedback on this effort; we see it as a first step towards making our work more accessible for those most in need of it.

On the Success of the Nationwide Suspicious Activity Reporting Initiative (NSI)

[The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) builds on what law enforcement and other agencies have been doing for years—gathering information regarding behaviors and incidents associated with criminal activity—and establishes a standardized process whereby SAR information can be shared among agencies to help detect and prevent terrorism-related criminal activity.]

ISE
INFORMATION SHARING ENVIRONMENT
ANNUAL REPORT TO THE CONGRESS
NATIONAL SECURITY THROUGH RESPONSIBLE INFORMATION SHARING
Prepared by the
Program Manager, Information Sharing Environment
30 June 2011

The NSI allowed us to develop many aspects of the ISE in a contained, albeit national scope environment. The scope of the ISE is huge; the scope of NSI is still huge, but it's much more contained; we're able to actually make progress on key aspects of the ISE. For example, let's take the ISE SAR functional standard that defines the 16 behaviors that are reasonably indicative of pre-operational criminal planning or terrorism-related activity. This standard was developed across our stakeholders. We tested it in an evaluation environment with 12 fusion centers. We engaged with all the privacy advocacy groups. Through the process, we were able to evolve the standard, get buy-in, be able to roll it out more broadly to where now, about 250,000 to 300,000 front-line officers have been trained; we're actually expanding it beyond law enforcement to the public safety community more generally. In partnership with DHS, DOJ, and the FBI, we've used our implementation fund to support the development of training programs with the professional societies, targeting 2.3 million private security guards and 1.3 million firefighters. It is a great example of our efforts. We've invested about $15 million in the NSI with agency partners like the FBI, DOJ, and DHS. This is a flagship success.

On Changing Cultures from Need to Know to Need to Share

This need for transforming cultures goes to the heart of the PM-ISE mission. Several years ago, the Markle Foundation championed the idea of authorized use, which focuses on decisions that needed to be made to protect the American people and enhance national security. The whole point of information sharing is not simply to share information, but to get information to the proper decision-maker, so they can make better, more proactive decisions. Authorized use is about placing information sharing in a mission context and defining policy that way. It's about moving from an information ownership model to a stewardship model; the key challenge given a decade's focus on classes of information is how do you make this transition. We need to get folks comfortable with the idea. It all boils down to the producers of information and consumers of information operating off the same rulebook, in a way that's transparent and auditable across the ISE.

In the end, we also believe that standards enable innovation. Let's innovate where we can add value and let's standardize where we have defined requirements and common mission equities; we really need to share information, so our standards framework is focused on exchange standards. You innovate on top of this foundation.

To learn more about the Information Sharing Environment, go to www.ise.gov.

To hear *The Business of Government Hour's* interview with Kshemendra Paul, go to the Center's website at www.businessofgovernment.org.

To download the show as a podcast on your computer or MP3 player, from the Center's website at www.businessofgovernment.org, right click on an audio segment, select Save Target As, and save the file.

To read the full transcript of *The Business of Government Hour's* interview with Kshemendra Paul, visit the Center's website at www.businessofgovernment.org.