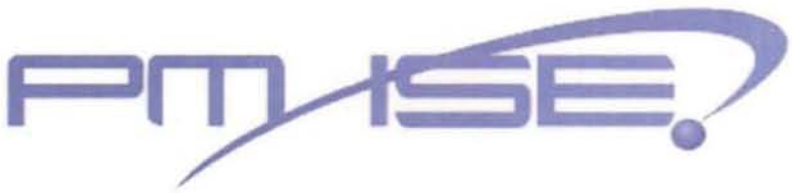
Statement for the Record

before the
Senate Homeland Security and
Governmental Affairs Committee

"Information Sharing in the Era of WikiLeaks:
Balancing Security and Collaboration"



Statement of Kshemendra Paul
Program Manager for the Information Sharing Environment

10 March 2011

Statement of Kshemendra Paul

Program Manager for the Information Sharing Environment

before the Senate Homeland Security and Governmental Affairs Committee

10 March 2011

"Information Sharing in the Era of WikiLeaks: Balancing Security and Collaboration"

Introduction

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee, thank you for the opportunity to speak about our efforts to effectively share and protect information at every level of government. I want to thank the Chairman and Ranking Member for their attention to information sharing reform efforts and support of my office's mission. I also recognize my fellow panelists who are key partners in our government-wide efforts to further strengthen information sharing and protection.

As the WikiLeaks story emerged, concerns were voiced that information sharing efforts would suffer a setback. This Administration is committed to improving information sharing and information protection. While complex and challenging, we do not see a conflict between these goals. Guidance throughout the Executive Branch has been consistent: we need to continue to accelerate our information sharing in a responsible and secure way. As has been echoed by Chairman Lieberman and Ranking Member Collins,[1] Secretary of Defense Gates, Office of Management and Budget Director Lew, and Director of National Intelligence Clapper have each championed efforts to further strengthen information sharing and protection; what Director Clapper has termed the "sweet spot" between the two.

The WikiLeaks disclosures primarily involved classified information, but the fundamental challenges associated with sharing and protecting sensitive information span across all security domains, including classified and sensitive but unclassified domains. Moreover, missions do not stop at the security domain or at organizational boundaries. Fundamental policies and solutions

[1] Wall Street Journal, Op-Ed, Dated: January 26, 2011.

should be framed to address all types of protected information, classified and unclassified, held by the federal government and by our state, local, tribal, private sector, and international mission partners. Across all mission partners, no matter the level of government, we need to establish structural elements such as strong governance, strategy, and policy to move incentives towards common, comprehensive solutions and away from agency-based, bilateral, fragmented approaches.

Information Sharing Environment[2]

My role, as outlined in the Intelligence Reform and Terrorism Protection Act of 2004, is to improve the sharing of terrorism-, homeland security-, and weapons of mass destruction-related information sharing across the federal, state, local, and tribal governments, as well as with the private sector and international partners.[3] I co-chair the Information Sharing and Access Interagency Policy Committee, which integrates the Information Sharing Council with the National Security Staff Senior Director for Information Sharing Policy.

The Information Sharing Environment facilitates sharing at all security domains among federal agencies, and across all levels of government. Our mission partners own the Information Sharing Environment. As you know, the Information Sharing Environment is defined through both a vertical mission – terrorism, homeland security, and weapons of mass destruction information sharing – and through a number of desired attributes,[4] a horizontal, cross-cutting, data-centric information sharing and protection capability. The law granted the Program Manager government-wide authority – a unique capability allowing us to work with existing programs to facilitate assured information sharing.

---

[2] For more information, see www.ise.gov.

[3] IRTPA, as amended, Section 1016

[4] IRTPA, Section 1016(b) (2) (I), for example, requires "strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls".

The Program Manager's role is to plan for, oversee the agency-based delivery of, and manage the Information Sharing Environment. Our office is not operational; agencies conduct mission operations, agencies develop and implement policy and procedures, and agencies make investments to interconnect systems, networks, databases, and business processes. Collectively, these contributions by mission partners form the Information Sharing Environment.

A practical way to think of the Information Sharing Environment is as an infrastructure and capability – analogous to the interstate highway system. The Information Sharing Environment represents the structure and "rules of the road" – including commonly understood road signs, traffic lights, and speed limits – that allow information traffic to move securely, smoothly, and predictably. We are charged with ensuring that the Information Sharing Environment is built to improve sharing and protection of terrorism, homeland security, and weapons of mass destruction information. If built properly, everyone can use the roads within appropriate mission and policy context. Indeed, like other infrastructures, the Information Sharing Environment is a public good and has the potential to pay dividends by supporting information sharing and protection beyond its initial mission space. Terrorism-related information can flow between partners, as can other classes of information such as those related to non-terrorism intelligence and law enforcement.

The law does not ask my office to do this alone – we are not pouring the concrete – rather, we are providing leadership and coordination of a complex set of factors that make the highway safe and navigable: governance and engagement, strategy and policy alignment, business process harmonization, guidelines, standards, and architecture. This leadership and coordination enables our mission partners – the general contractors building and managing the day-to-day operation of the highways – to build to common specifications.

In the five years since Congress directed the creation of the Information Sharing Environment, significant steps have been taken toward establishing a strong foundation. Important mission initiatives, such as the Nationwide Suspicious Activity Reporting Initiative, and core capabilities

and enablers, such as the National Network of Fusion Centers and the National Information Exchange Model, have produced results and show ongoing promise. Yet, as the persistent and evolving threat demonstrates, including vulnerabilities underscored by the WikiLeaks breach, much more remains to be done.

Information Sharing and Protection Opportunities

The WikiLeaks breach is not principally an information sharing problem; at its root a bad actor allegedly violated the trust placed in him. While we cannot always stop bad actors, we can take this opportunity to reassess our posture, our progress, and our focus regarding information sharing and protection to take a more holistic approach. When examining the full scope of information sharing and protection, there are many widespread and complex challenges that must be addressed and solved by multiple agencies and organizations together. The insider threat, the security concerns, and related challenges are being tackled by our mission partners – as described by my fellow panelists. Many of the best practices and work being done by our mission partners can, and should, be scaled more broadly.

From the lens of the Information Sharing Environment, we have observed three opportunities from the WikiLeaks incident that we believe require attention. First, a **whole-of-government** approach is necessary to effectively address these issues in a robust way. Second, fundamental policies and solutions should be framed to address all types of protected information, **classified and unclassified**, held by the federal government and by our state, local, and tribal partners, as our critical national and homeland security issues cut across security domains. Finally, a strong and broadly applied **governance, strategy, and policy framework** is foundational to improving information sharing and protection. A strong, comprehensive governance framework will help streamline policy and standards across the federal government.

We are being deliberate and collaborative in our approach. My office is currently leading an effort to update the 2007 National Strategy for Information Sharing. As part of this effort, we are reviewing the post WikiLeaks-related developments to determine how best to incorporate

improvements to both sharing and protection, and are engaged with our mission partners and other stakeholders to understand their needs, requirements, missions, and opportunities. As we further refine the principles of the strategy, the end goal is to accelerate the development and implementation of the Information Sharing Environment and contribute to our government's ability to securely and effectively share terrorism, homeland security, and weapons of mass destruction information among our mission partners.

Today, the mission spans organizational boundaries. It is only possible to further strengthen information sharing and protection by supporting these cross-cutting missions through shared policies, guidelines, and common standards; accompanied by governance, training, logging and auditing, performance management, and oversight mechanisms that provide confidence and accountability spanning all mission partners. No one size fits all, but an ecosystem that allows for effective risk-based decisions ensures progress.

Activities

We, in coordination with our mission partners, are actively working on a number of initiatives which will reduce the risk of another WikiLeaks–like incident. We want to build on current momentum to accelerate delivery of the Information Sharing Environment to provide a trusted, assured information sharing and protection ecosystem. The following demonstrate our work with both mission partners and with industry to develop and provision the standards-based Information Sharing Environment:

- **Harmonizing protection policy**. Robust privacy and security protections are critical to an effective Information Sharing Environment. The capabilities that permit policy-driven, predictable, mission-effective, and efficient information sharing are similar to the capabilities that increase privacy and security.
- **Driving Assured Interoperability across our Sensitive but Unclassified and Secret Networks.** The Program Manager for the Information Sharing Environment is supporting mission partners to deliver assured sensitive but unclassified network interoperability and assured secret network interoperability. Efforts regarding the

sensitive but unclassified networks are focused on the Federal Bureau of Investigation's Law Enforcement Online; the Department of Justice's grant-funded, state-owned Regional Information Sharing System Network; the Department of Homeland Security's Homeland Security Information Network; and the Intelligence Community's Intelink. The assured secret network interoperability effort brings together eight agencies[5] that operate at least 10 distinct secret networks with three main goals: (1) to streamline and ensure effective mission and policy framework for sharing classified information with our state and major urban area fusion centers; (2) to enhance governance and multi-lateral decision making to replace the current patchwork of bilateral agreements, and (3) to enhance operational coordination.

- **Harmonizing the Various Identity, Credential, and Access Management Frameworks.** There are at least five identity, credential, and access management frameworks in use by federal agencies.[6] These frameworks are critical to establishing trusted, assured identity, which in turn is foundational to information sharing and protection. It is essential that these frameworks are interoperable. While there is a large degree of bilateral alignment, the risk of fragmentation remains. The Program Manager for the Information Sharing Environment is focused on this challenge and is stepping up efforts to characterize necessary distinctions while focusing on shared minimum capabilities and whole-of-government optimization.

- **Reinventing the Public Safety Business Model.** The Information Sharing Environment's flagship initiatives, in conjunction with mission partners, have had a counterterrorism and homeland security focus, such as the network of state and major urban area Fusion Centers and the Nationwide Suspicious Activity Reporting Initiative. The Department of Homeland Security's Law Enforcement Information Sharing Service, the Federal Bureau of Investigations' National Data Exchange and the state-owned

---

[5] Office of the Director of National Intelligence, Department of Defense, Department of Homeland Security, Department of State, Department of Treasury, Department of Energy, Department of Justice, and the Federal Bureau of Investigation.

[6] These include: the Federal CIO Council's Federal Identity, Credential, and Access Management (FICAM) Roadmap and Interoperable Personal Identity Verification (PIV-I) guidance for unclassified networks; the Department of Justice's Global Federated Identity and Privilege Management (GFIPM) standards for unclassified networks and non-federal partners; DOD's Committee on National Security Systems PKI for secret networks; State Department, FBI, and Justice PKI solutions on their individual secret networks; the Intelligence Community's Identity and Access Management (IDAM) effort across all IC networks at all security domains.

National Law Enforcement Telecommunications System, or Nlets, highlight related and aligned national-scope law enforcement solutions. For our state, local, and tribal partners, counterterrorism is an important mission, but it is only one facet of the overall mission of protecting the American people. By advocating for, and embracing, an integrated, all-crimes, all-threats, all-hazards approach, all of our mission partners are positioning themselves to apply the broad benefits of the Information Sharing Environment to their entire mission. Our domestic mission partners are also looking at how to respond to a constrained budget environment by enhancing coordination and shared services across jurisdictions and levels of government through leveraging core Information Sharing Environment frameworks, policies, guidance, standards, and architecture.

- **Adopting Information Exchanges.** Two of the most important initiatives that must be implemented to enable effective information sharing are: (1) standardizing and translating terminology, code lists, and data definitions; and (2) harmonizing business processes so that all mission partners have a context for standardized information exchanges. To solve this issue, the National Information Exchange Model allows disparate systems to share, exchange, accept, and translate information. The National Information Exchange Model has been adopted by 13 cabinet agencies, is used internationally, and has been endorsed by the National Association of State Chief Information Officers. The required use of the National Information Exchange Model has also been incorporated into federal grant guidance issued by the Department of Homeland Security and the Department of Justice. The use of this framework enables greater information sharing through the use of existing exchanges and policy automation and enforcement through enterprise standards for security, access, and data protection.

Another key activity for solving these challenges rests in aligning and strengthening a comprehensive governance and outreach framework – a core focus of our office. There are three components to the current governance and outreach structure:

- Intergovernmental policy development, the first tier, represents the top-down authoritative source of direction for driving innovation by developing information requirements and defining mission processes through harmonizing common mission

equities. This is accomplished primarily through the Information Sharing and Access Interagency Policy Committee, its five subcommittees, and related working groups, where interagency policy decisions are discussed and made.

- The second tier is bottom-up, bringing the voice of the practitioner and subject matter experts to a collective table. To promote information sharing, existing representative organizations or intra-agency bodies are leveraged to promote collaboration for functional requirements and standards, to engage the key information integrators and best practices, and to promote seamless information sharing and protection.
- The third tier is outside-in, providing a means for mission partners to effectively communicate and collaborate with industry. The architecture, methodologies, and technologies used to build the Information Sharing Environment will rely upon standards that must be developed based on shared mission partner requirements.

Additionally, we are actively working with our interagency partners to develop further recommendations for how to enhance protections and improve information sharing. We are following agency reactions to WikiLeaks to ensure information protection efforts do not set back recent information sharing improvements or impede future information sharing improvements. As we work through these efforts, we will keep you informed.

Conclusion

In closing, pursuant to our charter in law, our efforts have been and, continue to be, focused on information sharing in a responsible and assured manner. We are committed to advancing the sharing of information with the protection of information. Effective information sharing and collaboration are absolutely essential to keeping America safe. The risk of future WikiLeaks-like incidents can be reduced; but, fixing these government-wide challenges is complex, difficult, and requires sustained commitment. We are committed to further strengthening information sharing and protection together. Thank you for your continued support and guidance as we work together on solutions to implement this critical national security priority.