Testimony of Jeffrey H. Smith[1]
Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment of the House Committee on Homeland Security

July 30, 2009

Chairwoman Harman, Ranking Member McCaul, I appear today as a member of the Markle Foundation Task Force on National Security in the Information Age and would like to thank you for holding this hearing and taking the initiative to improve information sharing by dedicating your time and energy to this critical issue. Making information sharing a top priority is essential to safeguard our national and homeland security.

The Markle Task Force's most recent report found that, although we have made much progress, we are still vulnerable to attack because—as on 9/11—we are not able to connect the dots. At the same time, our civil liberties are at risk because we don't have the government-wide policies in place to protect them as more powerful tools for intelligence collection and sharing information emerge.

Our government cannot identify, understand, and respond to 21st century threats, such as cyber attacks, terrorism, and energy security, without the collaboration and sharing of information across the federal, state, and local levels and with the private sector so fragments of information can be brought together to create knowledge. The Information Sharing Environment (ISE) was created by Congress to improve our ability to know what we know about terrorist threats. The ISE was intended to effect a "virtual reorganization of government," allowing communities of interest to work on common problems across agency boundaries and between federal, state, and local governments, and the private sector—wherever important information could be found.

[1] Member of the Markle Foundation Task Force on National Security in the Information Age and Senior Partner at Arnold & Porter LLP. I am grateful for the assistance of Nicholas Townsend, an associate at Arnold & Porter, and Daniel Friedman, a summer associate from Harvard Law School.

Ambassador McNamara recently released the Third Annual Report to Congress on the ISE. I am pleased to testify with him this morning and believe the nation owes him our thanks for a job well done. But much work remains. Under his leadership as the Program Manager for the Information Sharing Environment (PM-ISE), progress has been made toward reducing the barriers to information sharing that persist throughout government. The ISE has made substantial strides in developing the ISE framework and policies, training, and guidelines for sharing information. However, as the PM-ISE's report acknowledges, there is still a great deal of work to be done.

The Markle Foundation Task Force on National Security in the Information Age, on which I have had the privilege of serving since its inception, recently released a report[2] that found that our nation remains at risk. Unfortunately, the sense of urgency on information sharing has diminished in the nearly eight years since the 9/11 attacks. Old habits die hard. The "need to know" principle and stovepiping of information within agencies persist. The Markle Task Force's 2009 report makes concrete recommendations to address the cultural, institutional, and perceived technological obstacles that are slowing the implementation of laws intended to facilitate the flow of information and create new ways of collaborating.

I would like to take the remainder of my time to briefly outline the Task Force's core recommendations and to discuss three specific areas in detail where future work is needed −

(1) Strong sustained leadership from within the Executive Office of the President (EOP) and congressional oversight are needed to drive information sharing;

(2) All government information relevant to national security should be discoverable and accessible to authorized users while audited to ensure accountability; and

[2] *Nation at Risk: Policy Makers Need Better Information to Protect the Country* (2009). All of the Markle Task Force's reports are available at http://www.markle.org/.

(3) Enhanced government-wide privacy and civil liberties policies must be developed.

I hope my comments will give this Subcommittee a better sense of how far the government has come toward a trusted information sharing environment and what steps we believe still need to be taken to provide policy makers at all levels of federal, state, and local government better information so they can make the best decisions to protect our country.

I. The Markle Task Force's Core Recommendations

Before turning to a detailed discussion of the three areas where we believe more work is needed, let me provide a brief overview of the Markle Task Force and the four core recommendations in our most recent report. The Markle Foundation Task Force on National Security in the Information Age is a diverse and bipartisan group of experienced former policy makers and national security experts from the Carter, Reagan, Bush, Clinton, and Bush administrations, senior executives from the information technology industry, and privacy advocates. Under the leadership of Zoë Baird and former Netscape CEO Jim Barksdale, the Markle Task Force has released four reports[3] recommending ways to improve national and homeland security decision making by transforming business processes and the way information is shared while at the same time protecting civil liberties.

The Task Force has worked closely with government officials, and I am pleased to report that the government has taken many of our recommendations to heart in both legislation and executive orders. Chairwoman Harman and this Subcommittee deserve special recognition for their hard work on improving information sharing.

[3] *See* MARKLE FOUND. TASK FORCE, NATION AT RISK: POLICY MAKERS NEED BETTER INFORMATION TO PROTECT THE COUNTRY (2009); MOBILIZING INFORMATION TO PREVENT TERRORISM (2006); CREATING A TRUSTED INFORMATION NETWORK FOR HOMELAND SECURITY (2003); and PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE (2002), *available at* http://www.markle.org/markle_programs/policy_for_a_networked_society/national_security/projects/taskforce_national_security.php.

In March, the Task Force published its most recent report in the hope that it would help the Obama administration, which now includes several former Task Force members, develop information sharing priorities.[4] The report's four core recommendations, which are summarized below, emerged from common themes that arose during the Task Force's interviews with officials in the Executive Branch and Congress on the current state of information sharing.

First, Congress and the administration must provide strong, sustained leadership to reaffirm information sharing as a top priority. There is unfinished business in implementing an information sharing environment across all government agencies that have information important to national security, including state and local organizations. We are at a critical moment where top down leadership and immediate action at the start of the new administration are required. If there is another terrorist attack on the United States, the American people will neither understand nor forgive a failure to have taken this opportunity to get the right policies and structures in place.

Second, authorized users must have the capacity to discover and locate relevant information quickly and efficiently—a capability called "discoverability." Data should be tagged with standardized information that can be indexed and searched. Using a decentralized system of discoverability, rather than large centralized databases, simultaneously improves our security and minimizes privacy risks by avoiding bulk transfers of data. When combined with an authorized use standard, discoverability ensures that users obtain what they need, but only what they need. This authorized use standard would permit an agency or its employees to obtain information based on their role, mission, and a predicated purpose. We also recommend strong auditing throughout the system, which would allow for improved enforcement of the authorized use standard and would contribute to enhanced information security.

[4] I have attached a copy of the Markle Task Force's March, 2009 report, which I would like to submit for the record.

Third, the Obama administration should develop government-wide privacy and civil liberties policies for information sharing to match increased technological capabilities to collect, store, and analyze information. These policies should be clear, detailed, transparent, and consistent, and must provide direction on hard issues while allowing agencies the flexibility that their different missions and authorities may require. Such policies are necessary both for the American people to have confidence in their government and for the users of the information sharing framework to have confidence that their work is lawful and appropriate.

Fourth, the President and Congress need to overcome bureaucratic resistance to change by transforming the culture with metrics and incentives. Mission-oriented metrics are necessary to move away from the "need to know" culture and stovepiping of information that persists in many agencies and towards adoption of a "need to share" principle. Accountability and transparency should be joined with performance incentives and training to expose failure and reward success. Additionally, users should be empowered to drive information sharing by forming communities of interest. When individual users insist on better information, more effective practices are likely to be put in place to align information flows with user needs.

Although the Task Force's recent work has largely focused on the federal government, our recommendations are applicable at the state and local level as well. State and local law enforcement have an essential role to play in protecting our homeland security. A cop on the beat may have information that can stop the next attack, but he needs to know what to look for and how to report it. To keep our country safe, information must be shared effectively, not only within the intelligence community (IC) and among federal agencies, but also among federal, state, and local governments and with key private sector partners. As outlined in the PM-ISE's annual report, the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) has been a major focus of the ISE over the last year. The program has enjoyed enthusiastic support from the LAPD and other state and local participants. But more work needs to be done, including a careful examination of the role of fusion centers.

II. Strong Sustained Leadership from within the EOP and Congressional Oversight are Needed to Drive Information Sharing

The PM-ISE has made great contributions to enhancing information sharing. Ambassador McNamara's recent report says that a comprehensive information sharing policy requires coordination between five communities—Intelligence, Foreign Affairs, Homeland Security, Law Enforcement, and Defense—that cut across all levels of government. However, the PM-ISE's report does not discuss the significant challenges the PM-ISE faces coordinating those five communities from within the Office of the Director of National Intelligence (ODNI). Today, the PM-ISE is widely, but incorrectly, seen by those in the other four communities as part of the intelligence community; as the Subcommittee knows, his mandate is much broader.

The White House is currently taking steps to improve the existing structure by carrying out key information sharing work under the auspices of the EOP. In a July 2, 2009 memorandum, Assistant to the President for Homeland Security and Counterterrorism John Brennan took important steps in three key areas. First, Mr. Brennan's memo identifies effective information sharing and access as a "top priority" of the Obama administration and says "senior-level attention" to this issue is crucial. To advance this priority, the Information Sharing Council (ISC) is being integrated into the Information Sharing and Access Policy Interagency Policy Committee (IPC), so that the "important work of the ISC will move forward under the auspices of the Executive Office of the President." The position of Senior Director for Information Sharing Policy has been established within the EOP. The Senior Director will be the Chair of the

IPC and will lead the interagency policy process and identify information sharing and access priorities going forward.

Second, the White House has initiated a comprehensive review of information sharing and the ISE, which the Markle Task Force recommended as a key step to ensure government-wide focus and coordination. Third, Mr. Brennan notes that the importance of effective information sharing extends beyond exclusively terrorism-related issues.

The Markle Task Force takes heart from these early actions by the White House, which are largely in line with the Task Force's recommendations. Although the Task Force supports these efforts, we believe that it is imperative that the IPC and its Chair have adequate horsepower to drive interagency coordination at a senior level. As a general principle, the White House must assert strong sustained leadership across all agencies with a national or homeland security mission to assure that there is effective information sharing. Senior leadership from within the EOP will ensure government-wide authority to coordinate the policies and procedures necessary for effective information sharing, and provide the policy clout necessary to overcome the bureaucratic resistance and turf wars that stymie progress. Otherwise, wasteful duplicate efforts are inevitable as individual agencies try to address information sharing independently. Congressional oversight will be critical to ensure that government-wide efforts are being coordinated effectively.

It is our understanding that the administration is considering several possible structures for information sharing to leverage the accomplishments of the PM-ISE and recognize the role of the Chief Information Officer in the ODNI and other agencies. There are a variety of possible models, including (1) an approach similar to the Director of the Office of National Drug Control

Policy, (2) expanding the PM-ISE's mandate and making him the Co-Chair of the IPC, or (3) giving the Chair of the IPC greater authority.

It is critical that the official charged with leading government-wide coordination of information sharing policy (1) have the President's clout behind him, and (2) be responsive to Congress. Many believe this official should be appointed by the President and confirmed by the Senate. This will ensure accountability to Congress, like other Senate confirmed officials in the EOP, such as the Director of the Office of Management and Budget or the Associate Director and Chief Technology Officer in the Office of Science and Technology Policy. Congressional oversight is essential to the success of information sharing because the oversight process can help ensure that the individual charged with making information sharing a reality is held accountable for producing measurable progress toward a safer country. In addition to improving oversight, a presidentially appointed and Senate confirmed position will have increased policy clout, providing the necessary horsepower to drive interagency coordination.

Moreover, serious consideration should be given to providing some budget authority to the official charged with leading the government-wide coordination of information sharing. Budgetary certification authority would greatly increase the official's ability to ensure that agencies are adhering to the administration's information sharing policies. Similar authority has been granted in other contexts to officials such as the Director of the Office of National Drug Control Policy.

Broadening the Scope of Information Sharing: In light of the current financial crisis and growing budget pressures, we need to do more with less. An effective information sharing framework is not only important to protect against terrorism; it can make the government more effective in areas like energy security and preventing a full blown H1N1 pandemic this fall. Mr.

Brennan's memorandum acknowledges the need to expand the scope of information sharing beyond just terrorism information. The lessons learned from national and homeland security information sharing should be applied – under White House leadership – to other federal responsibilities, such as air traffic control and healthcare. Congress should carefully examine the potential for broader implementation of ISE best practices in order to improve information sharing in other areas beyond terrorism. Broader implementation will create an ongoing need for a senior official at the White House to drive effective information sharing from the top by continuing to maintain pressure on agencies to effectively share information.

III. All Government Information Relevant to National Security Should be Discoverable and Accessible to Authorized Users while Audited to Ensure Accountability

The PM-ISE's annual report focuses on developing infrastructure and technology that can help make accessing and sharing information easier. However, we believe greater attention should have been given in the report to data users and how they can find and access information. Intelligence Community Directive 501 (ICD 501), which was signed on January 21, 2009, mandates wide-ranging actions to promote information sharing throughout the IC. ICD 501 is not discussed in the PM-ISE's report. Connecting the PM's work with ODNI's efforts on ICD 501 more effectively could yield best practices with broad applications throughout the government. Specifically, the Obama administration needs to take two steps − (1) greater emphasis must be placed on discoverability, and (2) the PM-ISE's determination regarding the feasibility of an authorized use standard should be reassessed in light of ICD 501.

Greater Emphasis on Discoverability: As discussed in detail below, the Obama administration and Congress should consider adopting a policy that requires all agencies with a national or homeland security mission to make their data discoverable. Discoverability is a critical precursor to effective information sharing; making information more accessible will help only if users are able to discover what information is out there and who has that information.

The traditional information sharing model requires either the sender to know what information to send to whom ("push") or requires the end-user to know who to ask for what ("pull"). Whether push or pull, there are too many doors on which to knock. The chances of the right data holder and the right end-user locating each other and sharing the right information are slim at best.

Discoverability through the use of "data indices" is thus a critical precursor to an effective system of information sharing. These indices serve as a locator service, returning pointers to data holders and documents based on the search criteria used. Information not registered in data indices is essentially undiscoverable. Think of data indices as a card catalog at a library, where every aisle of the library is the equivalent of an isolated information silo. Without a card catalog to provide users with pointers to the location of books, users would be left to roam the isles in the hopes of finding a relevant book.

The technology to give users the ability to discover data that exists elsewhere is readily available. However, in order to make data discoverable, each agency needs to tag its data at the point of collection with standardized information that can be indexed and searched. Many agencies do not adequately tag and index their data, so it is not readily discoverable, which undermines not only an agency's ability to share the data with others, but also the agency's ability to share within its organization. The DNI recently took an important step towards implementing such a system by signing ICD 501, which requires all IC agencies to make all information collected and all analysis produced available for discovery by automated means.

ICD 501 only applies to the IC. An effective information sharing framework will require increased discoverability across the government, so that data users will be able to find and have access to information across agency lines. Therefore, the Obama administration and Congress should place a high priority on broader discoverability as the first step toward effective information access. The technology is readily available − all that is needed is government-wide policy guidance and implementation. The administration should establish a policy that requires all departments and agencies with a national or homeland security mission to: (1) tag their data at the point of collection; (2) contribute key categories of data (*e.g.*, names, addresses, passport numbers, etc.) to data indices; and (3) follow through on implementing widely available means to search data indices.

We are pleased that the PM-ISE's annual report discusses creation of output-related goals and metrics, such as the ISE Maturity Score Card. The administration should build on these metrics by adopting more concrete outcome oriented metrics. One of the first metrics should focus on discoverability because data indices are an essential precursor for effective information sharing. This metric should measure what percentage of an agency's data holdings have been registered in the data indices directory. Additionally, just as the private sector uses Quality Assurance scenarios to test the performance of critical system requirements, the administration should conduct ongoing tests across federal, state, and local organizations to determine how the ISE scores according to certain critical system requirements.

The Feasibility of an Authorized Use Standard Should be Reassessed: Improved discoverability must go hand in hand with a trusted system that will facilitate access to the data indices and the information to which these indices point (in the library analogy, access both to the card catalog and the book itself). An authorized use standard provides a model for such a system. Under such a standard, a federal, state, or local agency or its employees obtain mission-based or threat-based permission to discover, access, or share information, as opposed to the current system which relies on originator control limitations, U.S. persons status, and place-of-collection rules.

Congress asked President Bush to consider adoption of an authorized use standard in the 2007 9/11 Commission Recommendations Implementation Act. The PM-ISE discussed what he viewed as potential obstacles to implementation of an authorized use standard in his 2008 Feasibility Report. The report concluded that an authorized use standard was not feasible. Yet none of the objections in the report were technical in nature; commercial off-the-shelf technology enables the use of such a standard and can address perceived obstacles such as identity management. Moreover, an authorized use standard would not require amendment of statutes, such as the Privacy Act, and it would be in full compliance with the vital principles underpinning the constitutional, statutory, and regulatory requirements currently in place.

We believe the PM-ISE's determination that an authorized use standard is not feasible should be revisited in light of ICD 501 and pilot projects that are testing these concepts in the field. The IC has started down the path toward phased implementation of an authorized use standard with ICD 501. ICD 501 incorporates many principles from the Markle Task Force's previous work on authorized use. For example, ICD 501 requires that information collected or analysis produced must be available to authorized IC personnel who have a mission need for information and an appropriate security clearance. As part of ICD 501, the National Security Agency has designed a new collaborative system that will link disparate intelligence databases to support field operations in Iraq and Afghanistan. This system, which is currently in testing, is designed to address the challenge of providing data gathered from multiple agencies to authorized users based on different privileges. It represents a good first step that indicates that implementation of an authorized use standard is feasible.

Other organizations are also undertaking pilot projects that will test the Markle Task Force's recommendations. As the Subcommittee knows, the Project on National Security Reform (PNSR), led by Jim Locher, is working on the issue of improving national security decision making. I am privileged to serve on the "Guiding Coalition" for PNSR and am pleased to advise the Subcommittee that PNSR has adopted not only the spirit of the Markle Task Force's approach to information sharing, but also many of our specific recommendations. PNSR has been exploring with several government agencies the possibility of a pilot project that would incorporate the basic elements of a fully integrated information sharing system. I hope that the administration will conduct such a pilot project, and I encourage this Subcommittee to support this pilot project and to monitor its progress. Such real world tests can help reassess the feasibility of an authorized use standard.

IV. Increase Privacy Protections

As detailed in the PM-ISE's annual report, the PM-ISE has issued ISE privacy guidelines and the ISE Privacy Guidelines Committee has published a "Privacy and Civil Liberties Implementation Workbook" and several associated documents, such as Policy Development Tools and Privacy Policy Outlines, to help agencies implement their own privacy policies. These are a good first step, but much more remains to be done to develop policies to assure both the public and government officials that privacy and civil liberties are protected while information is shared. Clear, detailed, and consistent policies are necessary to protect privacy and civil liberties.

Few agencies have produced privacy policies to date because there is little incentive for them to do so. Of the 17 agencies that were supposed to develop their own privacy policies, only three have produced such policies, a paltry 18 percent. By way of comparison, state fusion centers are required to submit privacy policies by a certain deadline in order to receive federal grant money. Of 70 fusion centers, 80 percent have submitted policies. ISE agencies should be given a 30-day deadline to submit privacy policies to the PM-ISE for approval, and failure to meet deadlines should result in concrete penalties—including loss of funding.

Moreover, merely having a privacy policy is not enough. To date, the PM-ISE guidelines and associated documents are more advisory than directive—they tell the agencies to address various privacy and security principles, but do not tell them how to do so. A comprehensive privacy policy must provide direction and consistency on hard issues. Yet the PM-ISE guidelines do not address many of the most challenging issues. For example, the guidelines state that all agencies must comply with the Privacy Act, but they do not address many of the difficult questions about who gets what information for what purpose under what standard of justification.

The Obama administration should promulgate government-wide policies on privacy and civil liberties that provide consistency and direction on hard issues while allowing agencies the flexibility that their different missions and authorities require. Such a policy should address (1) auditing of both data quality and data flows; (2) enhanced fidelity of watchlists; (3) deployment of access and permissioning systems based on carefully defined missions and authorities; (4) clear predication for collection and retention of data; and (5) redress systems that offer a meaningful opportunity to challenge adverse action and that ensure that corrections or qualifications catch up with disseminated data.

The President and Congress should also act within the next 60 days to nominate and confirm members to the Privacy and Civil Liberties Oversight Board. Congress re-chartered the Board to strengthen its independence and authority, but the new Board has never come into existence. The statutory charter for the new Board gives it a role both in providing advice on policy development and implementation and in reviewing specific programs.

Finally, the ISE should take advantage of technological tools to minimize the risk of unintended disclosure of personally identifiable information. In his March 2008 Feasibility Report, the PM-ISE found that although data anonymization has the capacity to improve privacy protections, it was technologically infeasible. This determination should be revisited in light of technological advances. There are now a number of commercially available technologies, including anonymization, strong encryption, and digital rights management, that can help protect privacy and civil liberties as well as information security. Moreover, both privacy and security protections can be enhanced through the decentralized approach to discoverability outlined above because this approach avoids bulk data transfers minimizing both privacy and security risks. When locator and topic information are transferred to the index, the underlying information isn’t transferred until the user requesting it is authorized and authenticated, reducing the risk of unintended disclosure.

Building the information sharing environment should entail the development of new and more powerful privacy protections. But existing guidelines do not require agencies to provide any more protection than they already offered. Much work is needed in this area.

***

In conclusion, Madam Chairwoman, it has been a privilege for me to appear before the Subcommittee today. I commend this Subcommittee for its leadership on these issues. Sustained leadership is vital because a waning sense of urgency in the nearly eight years since the 9/11 attacks means that old habits of withholding information are returning. The United States must not become complacent about improving information sharing in the face of the current financial crisis and in the absence of a new attack. This Subcommittee has a critical oversight role to play in order to ensure that measurable progress is made on information sharing.

Much more needs to be done. Now, at the start of the Obama administration, is the moment for breakthrough progress on information sharing. The Markle Task Force will continue to work with Congress and the Obama administration to find practical solutions to the critical homeland security issue of information sharing. The Task Force has concrete recommendations for steps that can be taken today to ensure that decision makers at all levels get better information so they can protect the nation. Our recommendations are neither complicated nor technically difficult. They require attention to implementation and strong, sustained leadership.

It is important to have a public dialogue about this vital issue. I would like to thank the Subcommittee for having this hearing to facilitate that essential dialogue. I look forward to working with you and am happy to answer any questions you may have.