Testimony
Jeffrey H. Smith[1]
Senate Committee on Homeland Security & Governmental Affairs
July 23, 2008

Mr. Chairman, Senator Collins, it is a privilege for me to appear before this Committee today to discuss an issue of significant importance to our national security: ensuring that the right people have the right information at the right time.

The terrorist attacks of September 11th and the dynamic threat of global terrorism prompted an introspective review of the failures of American intelligence and, especially, how information is shared and how government agencies collaborate. I hope my comments today will give this Committee a better sense of how far the government has come toward a trusted information sharing environment and how far it still has to go.

Under the leadership of Zoe Baird and former Netscape CEO, Jim Barksdale, the Markle Foundation convened a bipartisan Task Force, of which I am a member, to examine national security in the information age.[2] This diverse group has consulted with government officials, private industry, experts on technology and civil liberties, and foreign partners in order to find solutions for this critical information sharing problem. Through a series of reports, the Markle

[1] Senior Partner, Arnold & Porter LLP; former General Counsel, Central Intelligence Agency; and former General Counsel, Senate Armed Services Committee.

I am grateful for the assistance of Nicholas Townsend, an associate at Arnold & Porter, and Manav Bhatnagar and Daniel Bernstein, summer associates from Yale Law School and Stanford Law School.

[2] I am appearing today at the request of the Committee on my own behalf. Although I have consulted with members of the Markle Task Force in the preparation of my testimony, I am here in a personal capacity and not as an official representative. I do not speak for the Markle Task Force. A listing of all the Task Force members is attached to my testimony.

Task Force has advocated for the creation of a trusted information sharing environment that achieves the twin goals of national security and civil liberties.[3] 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. The country has adopted important reforms through legislation, executive orders, and national strategies to facilitate the flow of information among the federal government, state and local agencies, the private sector, and foreign partners. This Committee deserves special recognition for the role it has played in these reforms.

As the GAO found in the report it released today on the information sharing environment, although the Congress, President, and intelligence community have made progress, much still needs to be done. Significant cultural, institutional, and technological obstacles remain. Our nation cannot allow recent reforms or the absence of a new attack on our homeland to lull us into complacency. There is reason to be concerned that the initial focus and momentum have dissipated, while confidence in the process and deliverables have decreased. To meet modern national security challenges, we must renew our commitment to greater information sharing consistent with respect for privacy.

As the Task Force articulated in its three reports, an effective information sharing environment must be built on trust. The agencies of government must trust each other with sensitive information, and the American people must trust their government to protect their civil

[3] *See* MARKLE FOUND. TASK FORCE, 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.

liberties and privacy. Realization of this trusted environment urgently requires: (1) sustained leadership and strong oversight from all branches of government; (2) clear policies, processes, and guidelines that facilitate collaboration and sharing of information while protecting civil liberties; and (3) technologies that facilitate sharing while protecting security and privacy.

Information sharing must not be a partisan issue; it goes to the core of good governance. To this end, the Markle Task Force continues to assess the government's progress and is currently preparing a report card that will make constructive recommendations to give to the next president and to Congress that will help the nation move its information sharing system forward.

I. Leadership on Intelligence Reform and Information Sharing

Creating a trusted information sharing environment requires leadership throughout the government.

Congressional leadership is needed to pro-actively exercise oversight responsibilities and provide adequate funding for the implementation of information sharing provisions. In response to various study group reports, Congress has passed landmark legislation such as the USA PATRIOT Act, the Intelligence Reform and Terrorism Prevention Act of 2004, and the Implementing Recommendations of the 9/11 Commission Act of 2007. These acts have removed obstacles to information sharing and established procedures for implementing further reforms. Importantly, Congress has also held regular oversight hearings, such as this one, to keep the government on the right track. To make additional progress, Congress should

streamline the jurisdiction of its oversight and appropriations committees, and expedite the confirmation of political appointments to the intelligence community and its oversight bodies.

Presidential leadership is also necessary to steer implementation across agencies, facilitate the kind of cultural transformation that is required, and encourage public confidence in the government's information sharing policies. Through executive orders and memoranda, the President has made the creation of a trusted information sharing environment a priority within the executive branch. The White House has recently issued a comprehensive information sharing strategy, standardized the classification system, and streamlined the security clearance process. The President also established the National Counter Terrorism Center (NCTC) in 2004, which serves as a centralized clearinghouse for all intelligence related to terrorism and counterterrorism. While these are steps in the right direction, the President should renew his commitment to trusted information sharing and exercise greater leadership in implementing specific recommendations from recent intelligence reform legislation so that this momentum is not lost.

Earlier this year, the Director of National Intelligence released his first-ever Community Information Sharing Strategy, and Ambassador McNamara, the Program Manager for the Information Sharing Environment, has now presented his second annual report to Congress. These executive branch efforts have initiated a paradigm shift from a "need to know" to a "need to share" culture. I greatly appreciate Ambassador McNamara's efforts and the leadership of Charlie Allen in the effort. I also welcome the GAO's recent report to Congress on the information sharing environment and recognize the importance of defining the ISE's scope and

measuring its performance. However, the Administration must ensure that transforming government in order to improve information sharing and collaboration is an urgent priority that does not wane or fall victim to turf battles and ambiguity about responsibility and authority.

Finally, leadership is needed at the state and local level to improve coordination, standardize information sharing procedures, and evaluate progress. There has been some progress on this front, as many state and urban areas have established "fusion centers" to coordinate information sharing and turn intelligence into actionable knowledge. However, it is unclear whether the fusion center model is the best approach; certainly, further work needs to be done to ensure information sharing among all levels of government and with the private sector.

II. Implementation Status of the Markle Policy Recommendations on Intelligence Reform and Information Sharing

Mr. Chairman, while there is now broad agreement on the need for greater information sharing, I believe that many of the relevant government actors have not yet internalized this priority.

I would like to turn to some of the most important policy recommendations of the Markle Task Force and discuss both the progress and shortcomings of the government in the pursuit of these goals.

First, a core recommendation of the Markle Task Force is the adoption of an *authorized use* standard. Under such a standard, agencies or employees could obtain mission-based or threat-based permission to access or share information, as opposed to the current system which relies on place-of-collection rules, U.S Persons status, and originator control (ORCON) limitations. Congress took a step in the right direction by asking the President to consider adoption of an "authorized use" standard in the Implementing Recommendations of the 9/11 Commission Act. However, one year later, the ISE Program Manager issued a "Feasibility Report" which argued against adopting such a standard because of perceived conflicts with existing privacy protections, as well as overlap with existing ISE privacy guidelines. I believe that the adoption of an authorized use standard is still a desirable and necessary goal. Although weight should certainly be given to the Program Manager's concerns, I am confident that an authorized use standard that is consistent with and respectful of security and privacy interests can be developed.

Second, the Markle Task Force has also called for the creation of a government-wide *dispute resolution mechanism* to replace the current cumbersome ad-hoc process. The 2007 Implementing Recommendations of the 9/11 Commission Act established the parameters, and affirmed the need, for a government-wide mechanism. Congress has also provided the Program Manager with the necessary authority, ability to hire, and funding to implement such a program. Such a system should be developed, as disputes between agencies during information sharing are inevitable, and should not be allowed to interrupt the functioning of the intelligence community.

Third, the Markle Task Force has emphasized the importance of protecting the *privacy and civil liberties* of our citizens through detailed guidelines. To earn the trust of government employees and the public, greater protections for privacy and civil liberties must accompany greater information sharing. The ISE has issued guidelines that require that information sharing complies with the Constitution and applicable laws, occurs only for a proper purpose, identifies protected information, is accurate and secure, and remains subject to audit. Accordingly, each agency must now develop a written privacy protection policy consistent with these guidelines. In the past year, the ISE has released helpful implementation instructions for the agencies. The next step is for the ISE Program Manager and the DNI to work with agencies to develop the kind of detailed and specific guidelines that are needed to support trusted information sharing. New policies may be needed that go beyond the Privacy Act and existing laws to address situations specific to information sharing. Even if the government can legally do something, prudence may require forbearance. For example, as the NCTC's Terrorist Watch List grows ever longer, more Americans' privacy and freedom of travel may be put at risk. It is therefore essential to have robust procedural controls in place.

To provide institutional oversight, the privacy guidelines also created a governance structure comprised of the ISE Privacy Officials from each relevant agency, the ISE Privacy Guidelines Committee, and the Privacy and Civil Liberties Oversight Board.
However, the Privacy and Civil Liberties Oversight Board that Congress created to review the effects of information sharing and to advise the president is currently inactive. Following the Board's first report in 2007, one of its members resigned because he believed that the Board interpreted its responsibilities too narrowly and lacked sufficient independence from the White

House. In response, Congress wisely reconstituted the Board as an independent agency within the executive branch. By statute, this new Board should have been up and running by January 30, 2008. It is regrettable that a full slate of new Board members has not yet been nominated or confirmed. Congress and the President should breathe new life into this important institution.

Fourth, the Administration and Congress have made significant progress on the Markle Task Force's recommendation to improve information sharing through *greater training and development of human capital*. The Information Sharing Environment Implementation Plan calls for departments and agencies to develop tailored training programs, a baseline training module, and incentives to encourage the adoption of an information sharing culture by holding personnel accountable. Similarly, the implementing recommendations of the 9/11 Commission Act of 2007 require the development of a curriculum and of training for employees of federal intelligence agencies, as well as state, local, and tribal officials with regard to information sharing processes. The third Markle Report also calls for the establishment of an entry-level evaluation administered to all employees of the intelligence community in order to promote information sharing skills, familiarity with technology, and a culture of trusted information sharing. This recommendation, however, has not yet been implemented.

Fifth, the Markle Task Force's recommendation for *improving the decision making* of officials by providing them with more diverse intelligence has seen progress. The intelligence community has acknowledged the shortcomings of existing analysis and placed a greater emphasis on considering divergent perspectives. For example, agencies have adopted "alternative analysis cells" to ensure more rigorous intelligence estimates. Some agencies have

also internalized the practice of including confidence assessments within reports to better assess the reliability of evidence. Further, the DNI created an Open Source Center to encourage the use of non-classified information. As a result, the President's briefing now relies on a more diverse intelligence base. To better inform decision-making, efforts should continue to create a unified open-source system.

Sixth, information sharing reforms have reflected the Markle Task Force's emphasis on *vertical integration of state, local, and private actors*. The Interagency Threat Assessment and Coordination Group (ITACG) has begun to support the NCTC by sharing "federally coordinated" information with other levels of government, and the Homeland Security Information Sharing Fellows Program now brings non-federal government analysts into the department. As noted earlier, state and urban areas around the country have also established "Fusion Centers." However, the legal and financial foundation for these efforts remains shaky. Unfortunately, state, local, and private actors are not fully integrated into the ISE. For instance, they do not currently sit on the Information Sharing Council as full members.

III. Adoption Status of Technology to Support Information Sharing

Finally, we must continue to develop and deploy technologies that support policies and processes to connect people and information. Congress reaffirmed the importance of the Markle Task Force's recommendations regarding immutable audit logs and anonymized information use technology in the Implementing Recommendations of the 9/11 Commission Act of 2007. These

technologies are designed to improve data sharing, enhance security, and facilitate privacy and accountability.

The Program Manager's "Feasibility Report" concluded that implementation of anonymization technology was not feasible because of shortcomings in existing technology, difficulty with integration into existing systems and processes, and complications related to re-identification. It is vital that resources be directed into overcoming the obstacles to a more technologically robust information sharing system that incorporates anonymization and audit technology. These technologies are essential to connect people who fight terrorism and to do so in ways that enhance trust in information sharing.

***

In conclusion, Mr. Chairman, it has been a great honor for me to appear before this Committee today. As you can see, the country has made significant progress toward the creation of a trusted information sharing environment that achieves the twin goals of ensuring national security and protecting civil liberties. Yet more needs to be done.

The Markle Task Force will continue to engage with the government on the critical national security issue of information sharing. In the coming months, the Markle Task Force will reach out to both presidential campaigns with specific recommendations for what steps need to be taken to ensure a trusted information sharing environment. The Markle Task Force will also continue to work with Congress as it develops further information sharing legislation. As I

described earlier, we need to implement additional policies that make information sharing a reality and we need to capitalize on the best technology available. America urgently needs renewed leadership on this issue from Congress, the President, and the agencies, as well as state and local governments.

It is important to have a public dialogue about this vital issue. I would like to thank the Committee 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.