Testimony
Slade Gorton[1]
Subcommittee on Terrorism and Homeland Security of the Senate Judiciary Committee
April 21, 2009

I would like to thank Chairman Cardin and Ranking Member Kyl for holding this hearing and taking the initiative to improve information sharing by dedicating their time and energy to this critical issue. Making information sharing a top priority is essential to safeguard our national and homeland security. Improved information sharing can provide decision makers at all levels of government better information in order to protect the country. Whether the question is Iran's nuclear activities, biosecurity or a potential cyber attack on vital computer networks, federal, state and local government personnel across agencies must collaborate and share information to identify, understand, and respond to evolving security threats.

The 9/11 Commission, of which I was a member, identified ten lost "operational opportunities" to derail the 9/11 attacks—and each involved a failure to share information. If there is another terrorist attack on the United States, the American people will neither understand nor forgive a failure to have connected the dots.

The Congress and the President should reaffirm information sharing as a top priority by providing sustained leadership from the top and ensuring accountability throughout the government. This Subcommittee has a critical oversight role to play in order to ensure that measurable progress is made on information sharing and that urgency does not wane. Otherwise, the United States will not be prepared to confront the threats of the 21st century.

[1] Senator Gorton served in the United States Senate for 18 years representing Washington state and currently practices law at K&L Gates LLP.

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, over seven years after the September 11th attacks, the United States remains at risk. Policy makers, from the President to local police chiefs, still need better information to defend our homeland. Such information should be available in time-critical situations and in ways that are tailored to facilitate decision-making and action at all levels of federal, state, and local government.

Building an information sharing framework that can provide better information to decision-makers requires the new administration and Congress to follow through with the hard work of implementation and to overcome the turf wars that stymie progress. The 111th Congress and President Obama should ensure accountability, sweep away bureaucratic resistance to information sharing, and foster an open debate about how best to achieve the twin goals of national security and protection of civil liberties.

Unfortunately, the sense of urgency on information sharing has diminished in the seven years since the 9/11 attacks. Each new problem our country confronts pushes information sharing further down the priority list.

The good news, to date, is that the required laws have been passed, and the Members of this Subcommittee deserve special recognition for the role they have played in those reforms. Specifically:

- The Congress and President Bush have acted on many of the recommendations of the 9/11 Commission, the WMD Commission, and the Markle Task Force, which informed both Commission reports.

[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/.

- Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 and the 9/11 Commission Recommendations Implementation Act of 2007, which required transformation of the intelligence community to achieve information sharing.
- Pursuant to the 2004 law, President Bush, the Program Manager for the Information Sharing Environment (PM-ISE), the Director of National Intelligence (DNI), and others have issued initial policy guidance reflecting the new "need to share" or "responsibility to provide" principle.

The Information Sharing Environment (ISE) created by Congress was intended to change the way government conducts the business of policy making based on information gathered. The legislation intended 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.

As a former Attorney General of Washington, I understand the important role state and local law enforcement play. A cop on the beat in Seattle 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 and among federal agencies, but among federal, state, and local governments and with key private sector partners.

Yet old habits die hard. The "need to know" principle and stovepiping of information within agencies persist. Cultural, institutional, and perceived technological obstacles have slowed the implementation of laws intended to facilitate the flow of information and create new ways of collaborating.

Much more needs to be done. The Department of Homeland Security and the Federal Bureau of Investigation have engaged state and local law enforcement through fusion centers, but both the role and future of these centers are uncertain and the sharing of information with them has been uneven. While the National Counter Terrorism Center (NCTC) and the

Office of the Director of National Intelligence (ODNI)—and to some extent the wider Intelligence Community (IC)—have made significant progress on information sharing, their work is far from complete. A 2008 review by the Inspector General of the 500 Day ODNI Plan indicated that the IC still has a long way to go on collaboration and information sharing.[3] Information sharing outside the IC—as well as information sharing across the law enforcement, domestic intelligence, and foreign intelligence communities—remains problematic. So, too, is information sharing related to US persons.

Information-sharing practices are still a hodge-podge because too much discretion has been left to each agency. While Congress and the Executive Branch have generally set out the basic policy structure for an effective information sharing framework, the Executive Branch should give agencies government-wide policy guidance on hard issues such as privacy, identity management, discoverability, and authorization. Congress should also engage in vigorous oversight to measure progress and create accountability.

Now is the moment for breakthrough progress on information sharing. Action at the start of the new administration is required. It is much better to remodel the house right the first time rather than remodeling it later.

The Markle Task Force takes heart from recent actions:

- First, the previous DNI, Admiral McConnell, signed a new Intelligence Community Directive (ICD 501) on January 21, 2009 mandating wide-ranging actions to promote information sharing, including the ability to discover and request information from all IC elements, who now have a "responsibility to provide" such information.
- Second, the Secretary of the Department of Homeland Security issued an Action Directive on State and local information sharing on her first day in office, calling for "an evaluation

[3] See *Follow-up Report of the 500 Day Plan, Part 2*, available at http://www.dni.gov/500-day-plan/500%20Day%20Plan%20Follow%20Up%20Report%20part%202.pdf.

of which activities hold the most promise for achieving the smooth flow of information on a real-time basis."

- Third, the President has affirmed the need to establish an integrated, effective and efficient approach to address 21st century threats. In *Presidential Study Directive 1*, he has called upon the Homeland Security and Counter-Terrorism Assistant to the President to review how to strengthen interagency coordination of the full range of homeland security and counterterrorism policies, including information sharing.
- Fourth, the administration has embraced information technology—and technology is now widely available both to help solve the hard issues mentioned above and to protect civil liberties.

The President has called for a new way of doing business. 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 will make the government more effective in areas like energy security, bio-defense, and healthcare as well.

It is time to reaffirm our nation's commitment to improving information sharing by accelerating implementation of the laws and policies Congress put in place to shift government from a "need to know" to a "need to share" paradigm. One example of an important step toward reaffirming information sharing as a top priority is moving the PM-ISE into the Executive Office of the President (EOP), as discussed in detail below.

Overcoming persistent barriers to information sharing requires strong, sustained leadership from the top and accountability throughout the government. Therefore, I would like to take this opportunity to discuss two key elements of the Markle Task Force's latest report: (1) reaffirming information sharing as a top priority, and (2) transforming the information sharing culture with metrics and incentives.

Reaffirming Information Sharing as a Top Priority

While initial steps by the new administration are promising, the 111th Congress, President Obama, Secretary Napolitano, Director of National Intelligence Dennis Blair, and Attorney

General Eric Holder should provide strong, sustained leadership to reaffirm information sharing as a top priority. A waning sense of urgency in the seven years since the 9/11 attacks means that old habits of withholding information are returning. Top down leadership, to reaffirm the importance of information sharing, is necessary. Congress should conduct robust oversight and the President should convene a Cabinet meeting to affirm information sharing as a top priority and to help overcome the bureaucratic resistance and turf wars that stymie progress.

Moving the PM-ISE into the EOP. One important way to reaffirm this issue as a top priority would be for President Obama to move the Program Manager for the Information Sharing Environment into the Executive Office of the President. The reason for such a move is clear. It will enable the PM-ISE to carry out its statutorily required government-wide authority[4] to coordinate the policies and procedures necessary for an effective information sharing framework, and give the PM-ISE White House backing to carry out its mission. Currently, the PM-ISE lacks policy clout and is seen (incorrectly) as an adjunct to the intelligence community. Elevating the PM-ISE into the EOP will ensure that the PM-ISE is able to coordinate across federal, state and local agencies effectively in order to improve the way our government shares information.

I am also sensitive to Congress' concern that the PM-ISE be responsive to congressional oversight. Congressional oversight is essential to the success of information sharing, as emphasized later in my testimony.

Regardless of where the PM-ISE is situated, the President should ensure that it is fully integrated into, and has a lead role in coordinating, all information sharing policy development

[4] *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. No. 108-458, 118 Stat. 3638 (2004), states that the PM-ISE is "responsible for information sharing across the Federal Government" and that he "shall have and exercise government wide authority."

and implementation across the government, including the intelligence, law enforcement, and homeland security communities. Otherwise, wasteful duplicate efforts are inevitable as individual agencies try to address information sharing independently. This approach is a more efficient and effective way of governing, consistent with President Obama's efforts to change the way government does business.

Ordering a High-Level Review. The President should also order an initial 60-day high-level review of the current policy and privacy guidelines and processes for the ISE. The Markle Task Force's discussions with senior officials revealed that departments and agencies have widely differing priorities and perspectives with respect to information sharing. President Obama should also demand an assessment of the state of the ISE on an annual basis thereafter, in order to ensure government-wide focus and coordination. The administration should release public reports on the results of its 60-day review, the status of implementation, and each annual review. Congress should hold hearings on the 60-day review and on each annual report to assure that information sharing remains a high national priority.

As part of this 60-day review, the new administration should apply ISE best practices to areas of national and homeland security concern in addition to terrorism, such as cybersecurity, nuclear proliferation, energy security, and climate change. To date, the ISE has been used primarily to facilitate the flow of terrorism-related information.

Congress and the new administration should also focus directly on the overlapping worlds of law enforcement and domestic intelligence, because the sharing of information between the law enforcement community and the intelligence community—a major lapse on 9/11—remains a critical challenge. Tension persists between the intelligence and law enforcement communities and concern exists on both sides that "the wall" may be creeping up

again. The Markle Task Force encourages continued work on robust pilots that test concepts that could improve the way the two communities work together. Such pilots have reportedly been very successful in resolving information sharing disputes, and some are still underway. The Obama administration should establish a review process to transfer best practices from successful pilots to the broader intelligence and law enforcement communities.

Congress has a vital leadership role to play that can help ensure that improving information sharing remains a top priority. This Subcommittee should keep the pressure on the administration to implement the information sharing reforms in recent legislation. The oversight process can help ensure that the individuals charged with making information sharing a reality are held accountable for producing measurable progress toward a safer country.

Transforming the Information Sharing Culture with Metrics and Incentives

Sustained leadership from the top is essential, but the President and Congress cannot implement an effective information sharing framework alone. The Congress and President Obama should ensure accountability throughout the government in order to follow through with the hard work of implementation and overcoming bureaucratic resistance to information sharing.

The Markle Task Force's recent report recommends specific metrics that help Congress measure progress so it can perform its oversight function and the report puts forth a series of practical incentives that will help the Obama administration transform the culture and reduce resistance to information sharing.

Improved Metrics. Mission-oriented metrics are necessary to change the "need to know" culture that persists in many agencies. Past Markle Task Force reports discussed the need to establish performance metrics and self-enforcing milestones for the information sharing

framework. In our second report,[5] for instance, we provided a detailed set of questions Congress and others could use to evaluate progress made on information sharing and analysis. These 24 questions focused on whether:

- Roles, responsibilities and authorities were clarified.
- Progress was made to remove roadblocks to sharing information within the federal government.
- Intelligence was produced for a set of new customers.
- Communications and sharing was being promoted with state and local governments and the private sector.
- Overall analysis was improved.
- The capabilities of state, local and private sector entities were being improved.

Congress should develop key questions in order to evaluate and measure agencies' performance in meeting essential information sharing and analysis objectives. Once established, these metrics should be incorporated as part of the regular annual review of information sharing.

One of the first metrics should focus on discoverability (the ability of users to discover data that exists elsewhere) because data indices are necessary to enable an effective information access framework. This metric should measure what percentage of an agency's data holdings have been registered in the data indices directory. If you 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, this metric would measure how many of the library books have a card in the card catalog. This could be accompanied by ongoing tests across organizations on how the ISE scores according to certain critical system requirements (akin to the Quality Assurance scenarios used in the private sector).

[5] Markle Task Force report *Creating a Trusted Network for Homeland Security* (2003), page 26, Exhibit F.

Accountability and Transparency. Once improved metrics are in place, agencies should be held accountable for reaching certain benchmarks or milestones. Congress and the administration should couple program funding with how well that program increases discoverability. Programs that do not make their information discoverable by putting their data in the index should get less funding. This type of financial accountability is logical because data held by a system that is not discoverable to other federal, state, and local agencies is less useful and less valuable. This system of discovery metrics and accountability would significantly reduce the voluntary aspect of exposing select data with data indices, and can help Congress carryout effective oversight by providing clear information about who is contributing the most to the shared library and whose data is most useful.

Agency level accountability should also be accompanied by individual accountability. Penalties should be widely known, proportionate to the misuse or failure to share, and applied consistently. Field officers, mid-level analysts, and state and local actors should have a special confidential channel to call senior leadership's attention to their belief that critical information is not being shared. This channel would send a clear message of individual accountability—that information sharing is not someone else's responsibility, but critical to the mission and part of everyone's job.

Driving Cultural Change with Performance Incentives and Training. Individual performance incentives and training are two important tools that can change agency culture in favor of information sharing. The government has put in place some training and policies to institutionalize sharing incentives, but implementation at the agency level is lacking. For example, the PM-ISE issued a plan in 2006 requiring that agencies develop the following:

- Tailored training programs based on their unique business processes, missions, program, and policy needs.

- A core training module that will serve as the common educational baseline for the ISE.

- Incentives to adopt the ISE culture that hold personnel accountable for the improved and increased sharing of information.

Based on agency self-reporting, the PM-ISE found in June 2008 that fewer than 50 percent of agencies had adopted such training programs and personnel incentives. Moreover, there has been little assessment of the quality of any of the programs the agencies have adopted. PM-ISE guidance released on September 24, 2008 aims to make information sharing a factor in annual performance appraisals for employees of agencies that are members of the Information Sharing Council and others who handle terrorism-related information. The ODNI is still working on uniform training across the IC elements and on adding information sharing as a factor in performance evaluations throughout the IC.

Congress and the Obama administration should focus on improving incentives to share information because such incentives can accelerate cultural change where the "need to share" or "responsibility to provide" culture has not fully taken root. Many individuals still perceive risk and penalties for sharing information that might later be claimed to have been unauthorized or ill advised. They believe they are more likely to get in trouble for sharing too much information than too little.

Three specific examples of incentives and training that could drive cultural change are:

- Integrating information sharing into performance reviews and budget and personnel resource allocations for all agencies that have a national security mission.

- Creating an information sharing award. This award should be given to the federal, state or local agency or unit within an agency that has been most successful at making its data discoverable. This award would highlight the overall value of information sharing to national and homeland security, and help facilitate the necessary culture shift.

- Increasing joint duty in the IC, in order to build a sense of trust and community. As in the military, the IC is instituting the practice that promotion to senior levels requires a tour of duty at another agency. A broader concept of joint duty, especially among mid-level employees, will foster a sense of community that is not narrowly focused on each agency's separate mission.

The heart of the matter is for employees at every level to understand why information sharing is valuable to *them*. Information sharing works well in Iraq and Afghanistan because the sense of shared mission is great. The Obama administration should take these lessons learned in the field and make them work back home.

***

In conclusion, Mr. Chairman, Senator Kyl, thank you for the opportunity to appear before this Subcommittee today. I hope my comments have helped give you a clearer idea of steps that can be taken to reaffirm information sharing as a top priority and to ensure accountability throughout the government. Congress' oversight role in this area is crucial.

I commend this Subcommittee for its leadership on these issues. Sustained leadership is vital because a waning sense of urgency in the seven 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. Your leadership on this issue can ensure accountability, sweep away bureaucratic resistance, and foster an open debate.

I applaud the Subcommittee for having this hearing today. I am happy to answer any questions you may have.