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

Chairman Cardin, Senator Kyl, it is a privilege for me to appear before the Subcommittee today to discuss the risk our homeland faces because of insufficient progress on information sharing. Today, we are still vulnerable to attack because—as on 9/11—we are still 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.

The United States confronts a stark set of national security challenges including terrorism, the global economic crisis, energy security, climate change, cybersecurity, and weapons of mass destruction. Our government cannot identify, understand, and respond to these threats without the collaboration and sharing of information among officials across the federal, state and local levels in a manner that protects civil liberties so fragments of information can be brought together to create knowledge. To improve decision making, Congress and the President need to take immediate steps to enhance information sharing. Otherwise, despite all the United States has invested in national and homeland security, we will remain vulnerable because we have not adequately improved our ability to know what we know about these threats.

I hope my comments today will give this Subcommittee a clearer idea of the steps that should 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 the country.

[1] President of the Markle Foundation, a private philanthropy that focuses on using information and communications technologies to address critical public needs, particularly in the areas of health care and national security.

The Markle Foundation Task Force on National Security in the Information Age

Since 2002, I have served as the Co-Chair of the Markle Foundation Task Force on National Security in the Information Age, 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. The Markle Task Force has released four reports[2] 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.

On March 10, 2009, the Markle Task Force released its most recent report entitled 'Nation At Risk: Policy Makers Need Better Information to Protect the Country.' Over the last seven months, the Task Force has interviewed numerous officials in the Executive Branch and the Congress on the state of information sharing in order to identify priorities for the new administration, which now includes several former Task Force members. Common themes and findings emerged from these interviews, forming the basis of our recent report's four core recommendations, which are outlined below.

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. Much work on the state and local level still needs to be done, such as a careful examination of the role of fusion centers.

[2] The four Markle Task Force reports are *Nation at Risk: Policy Makers Need Better Information to Protect the Country* (2009), *Mobilizing Information to Prevent Terrorism* (2006), *Creating a Trusted Network for Homeland Security* (2003), and *Protecting America's Freedom in the Information Age* (2002). All reports are available at http://www.markle.org/.

I commend the Subcommittee for its oversight efforts in this area because, where there have been improvements, they have been aided a great deal by Congressional attention.

Four Core Recommendations from the Markle Task Force's 2009 Report

First, the Congress and President Obama should reaffirm information sharing as a top priority, ensuring that policy makers at all levels of federal, state and local government have the best information to inform their decisions. Information sharing must not get ahead of strong protections for privacy and civil liberties. We are at a critical moment, where immediate action at the start of the new administration is required. There is unfinished business in implementing an information sharing framework across all government agencies that have information important to national security, including state and local organizations. The 111th Congress and the Obama administration should take this opportunity to get the right policies and structures in place. An information sharing framework will allow government to collaborate effectively across diverse areas to better inform policy makers without undermining civil liberties.

Second, the Obama administration and Congress should ensure that all government information relevant to national and homeland security is discoverable and accessible to authorized users while audited to ensure accountability. Otherwise we will remain vulnerable. When federal, state and local government officials have the capacity to locate relevant information and to make sense of it, they can find the right information in time to make better-informed decisions. Such a decentralized system of discoverability, rather than the creation of large centralized databases, simultaneously improves our security and minimizes privacy risks because it avoids 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 data users, such as fusion centers or CIA analysts, to

obtain information based on their role, mission, and a predicated purpose. We also recommend strong auditing throughout the system, which allows for improved enforcement of the authorized use standard as well as contributing to enhanced information security.

Third, the new administration should develop government-wide privacy and security policies for information sharing to match increased technological capabilities to collect, store, and analyze information. These policies should be detailed and address the hard questions not answered by current law—who gets what information for what purpose under what standard of justification and where should information be maintained to provide for security and accuracy. Without such policies, the American people won't have confidence in their government, while the users of the information sharing framework won't have confidence that they have what they are expected and allowed to know, and that their work is lawful and appropriate.

Finally, the President and Congress should overcome bureaucratic resistance to change. Old habits die hard. The "need to know" principle and stovepiping of information within agencies persist. The adoption of the "need to share" principle and the responsibility to provide information, and actions to transform the culture through metrics and incentives, are necessary to the success of the information sharing framework. In addition, those federal, state and local officials who depend on information to make decisions and accomplish their mission should be empowered to drive information sharing, to ensure they get the best possible data.

These are broad recommendations but our recent report, which I would like to submit for the record, sets out very detailed measures to achieve these objectives. The Markle Task Force's recommendations are not complicated. We believe that technology currently exists to achieve them. But they do require strong, sustained leadership and attention to implementation.

I would like to take the remainder of my time to focus on two of our four recommendations: (1) making government information discoverable and accessible to authorized users, and (2) enhancing security and privacy protections to match the increased power of shared information.

Making Government Information Discoverable and Accessible to Authorized Users

In an effective information sharing framework, information is not simply shared without restraint. The Markle Task Force recommends two critical features that regulate access in the information sharing framework: (1) discoverability and (2) authorized use. When combined, increased discoverability and an authorized use standard ensure that federal, state and local users can obtain what they need, but only what they need. This system of selective revelation ensures that, in time-critical situations, authorized users can locate, get access to, and make sense of, relevant information, while protecting privacy and enhancing information security.

Increased Discovery. Perhaps the single most important step to foster an effective information sharing framework is to give users the ability to discover data that exists elsewhere—a capability that can simply be called "discoverability." 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 use of data indices is therefore the first step in any effective system for sharing information. Such indices serve as a locator service, returning pointers to data holders and documents based on the search criteria used. If information is not registered in data indices, then it is essentially undiscoverable. Think of data indices as a card catalog at a

library. In this analogy, every aisle of the library is the equivalent of an isolated information silo. It would be unimaginable to roam the aisles expecting to find a relevant book. Rather, the card catalog provides a user with pointers to the location of books.

Both privacy and security protections are enhanced through this approach to discoverability. Locator and topic information are transferred to the index, but the underlying information isn't transferred until the user requesting it is authorized and authenticated. This decentralized system avoids bulk data transfers minimizing both privacy and security risks. Further, with commercially available technology that allows for removal of personally identifiable information (PII)—so called anonymization—the index can be created without any information that identifies an individual by name or other specific identifier. Therefore, the risk of unintended disclosure of PII contained in the data indices is reduced. Congress should revisit the determination of the Program Manager for the Information Sharing Environment (PM-ISE) that adequate removal of PII via data anonymization is technologically infeasible.

In order to build a system that enables users to discover data elsewhere, each agency's data needs to be tagged at the point of collection with standardized information that can be indexed and searched. Many agencies, however, 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 Director of National Intelligence (DNI) has recognized the need for data to be tagged and indexed at the point of collection. The DNI recently signed an Intelligence Community Directive (ICD 501), which establishes policies for discovery that require Intelligence Community (IC) agencies to make all information collected and all analysis produced available for discovery by automated means. ICD 501 is an important step toward increased discovery

because it creates a "responsibility to provide" information. Although ICD 501 tackles a number of hard questions, its implementation presents challenges and many important details need to be resolved. Moreover, ICD 501 only applies to the IC. An effective information sharing framework will require increased discoverability across many federal, state and local agencies.

The Congress and President Obama should place a high priority on discoverability as the first step toward effective information access. The technology is readily available. What is needed now is clear government-wide policy guidance, accountability, and the painstaking work of implementation. The Obama administration should establish a policy obligating all agencies with a national or homeland security mission to make their data discoverable. This policy should require departments and agencies 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.

Authorized Use and Identity Management. Improved discoverability must go hand in hand with a trusted system that will facilitate access to the data indices and the information these indices point to (in the library analogy, access both to the card catalog and the book itself). An authorized use standard provides a model for building such a trusted system that can overcome some of the systemic challenges of classification, data categorization, and compartmentalization. Under such a standard, data users would be required to provide a predicate in order to access data. To establish a predicate, a federal, state or local user seeking information would need to state a mission- or threat-based need to access the information for a particular purpose. Thus, a fusion center or its employees could obtain mission-based or threat-based permission to discover, access, or share information, as opposed to the current system that relies on place-of-collection rules, US persons status, and originator control limitations.

Congress asked President Bush to consider adoption of an authorized use standard in the 2007 9/11 Commission Recommendations Implementation Act. The PM-ISE's 2008 Feasibility Report discussed what he viewed as potential obstacles to implementation of an authorized use standard. All of the technical objections, however, can be addressed through commercial off-the-shelf technology, which continues to become more widely available, enabling the use of such a standard even in today's environment of multiple and differing authorities and standards.

The Markle Task Force believes that a combination of high-level policy attention from the President and Congress and appropriately deployed technology can allow phased implementation of an authorized use standard. ICD 501 has started the IC down the path toward phased implementation of an authorized use standard. 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.

The main hurdle that is often asserted as preventing implementation of an authorized use standard is the lack of an effective identity management system—a system that verifies the identity of individuals in a network and controls their access to information by associating user rights and restrictions with each individual and his or her role. The DNI is currently trying to complete the plan for an "Enterprise Architecture" to put technology in place that will enable identity management across all of the IC agencies, which, in turn, will make possible discoverability, disclosure control, and information access.

Overcoming identity management obstacles must be a priority. Technology to implement such a standard is commercially available today and phased implementation should begin now. Using existing technology to create an effective system for identity management will not only help improve information sharing—it will also be an important tool to enhance cybersecurity

because it will identify all data users and, with appropriate protections, flag attempts to go beyond authorized access and use, or to cause damage to systems or information.

Congress has a critical role to play in ensuring effective implementation of authorized use and discoverability. Congress should hold regular hearings to oversee the development of the information sharing framework, including how much data is discoverable and progress toward an authorized use standard. Congress must also adequately fund these efforts.

Enhancing Security and Privacy Protections to Match the Increased Power of Shared Information

Building the information sharing framework should entail the development of new and more powerful privacy protections. As the 9/11 Commission stated, the change in governmental need for information "calls for an enhanced system of checks and balances." No information sharing framework will succeed unless the American people are confident that it will respect their privacy, and the analysts and operatives using the framework have confidence that it protects against inappropriate disclosure. The Markle Task Force believes that the President and Congress should develop clear, detailed, government-wide policies that address the hard questions associated with information sharing and increased use of technological capabilities to collect store, share, and analyze information.

Privacy and security are not a zero-sum game. In developing these government-wide policies, the administration needs to recognize that an effective information sharing framework can enhance both privacy and security simultaneously. From its inception, the Markle Task Force has focused on the "twin objectives" of preventing terrorism through improved information sharing while at the same time preserving and protecting the civil liberties that are a bedrock of our national values. The importance of privacy should not be dismissed as an impediment to security. Indeed, the Markle Task Force's latest report found that many of the

measures that should be taken to improve privacy protections will actually enhance the effectiveness of the information sharing framework by improving the reliability of information.

Enhanced Information Security. In a "need to share" culture, greater sharing of sensitive information increases the risk of damaging security breaches. Therefore, increased sharing must be accompanied by protections to assure that information is used appropriately.

Technology already exists that can help create an environment where sharing can increase because users trust the security measures that are in place. Immutable audit logs should be used to protect privacy and security of information. Additionally, regular, automated compliance and behavior audits are an indispensable element of an information sharing framework. Such audit capabilities enable oversight and accountability and are a critical protection against misuse and abuse. Real-time audits of user compliance and behavior and immutable audit logs should be implemented immediately. Such audits and network monitoring will play a key role in efforts on information security and protecting against cyber threats.

Greater Privacy Protection. Much more needs 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. The DNI and several other agencies now have Civil Liberties and/or Privacy Officers, but many agencies do not have clear policies to implement. To date, PM-ISE guidelines and associated documents are more advisory than directive—they tell the agencies that they must address various privacy and security principles, but do not tell them how to do so. The guidelines state, for example, that all agencies must comply with the Privacy Act, but the Privacy Act does not address many of the hard questions surrounding who gets what information for what purpose under what standard of justification. So far, the privacy guidelines issued for the ISE do not require agencies to provide any more protections than they offered before the ISE.

Government-wide, there should be measurable changes. The new administration should promulgate government-wide policies on privacy and civil liberties that provide direction on hard issues and provide consistency, even as they allow agencies the flexibility that their different missions and authorities require. These government-wide policies 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, (5) redress systems that offer a meaningful opportunity to challenge adverse action and that ensure that corrections or qualifications catch up with disseminated data. In addition, agency heads should ensure that Civil Liberties and/or Privacy Officers are engaged at all stages of the policy development and implementation process.

Congress and the President should also act within the next 60 days to nominate and confirm members to the Privacy and Civil Liberties Oversight Board. Over 19 months ago, 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.

Commercially available technologies, such as anonymization, strong encryption, and digital rights management, are also critical tools for protecting privacy.

Congress should engage in vigorous oversight with respect to privacy and civil liberties. The Obama administration should fully inform the relevant Committees and appropriately cleared staff of the challenges the government faces as a result of rapidly developing communications technology and of tools the administration is currently employing to collect information, including any new technology that may be needed to adequately collect and analyze information.

***

In conclusion, Mr. Chairman, I appreciate your invitation to appear before this Subcommittee today. This Subcommittee deserves special recognition for the role it has played on these critical issues.

Yet more needs to be done. We are still vulnerable to attack because, despite the information sharing reforms that have taken place, federal, state and local decision makers still need better information to protect the United States. At the same time, privacy and civil liberties are not adequately protected because we don't have detailed government-wide policies in place.

Our nation cannot allow recent reforms or the absence of a new attack on our homeland to lull us into complacency. What America urgently needs is renewed leadership on this issue from Congress, the President, and state and local governments.

The Markle Task Force will continue to work with Congress and the Obama administration to find practical solutions to this critical national security challenge. 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.

The threat of terrorism is the impetus for the information sharing framework, yet its value is enhanced knowledge creation to improve decision-making and policy implementation across all levels of government. Improved information sharing can make the government more effective in areas like energy security, bio-defense, and healthcare. There is also a clear connection between cybersecurity and information sharing. The same technology that will help improve information sharing is a critical part of protecting against cyber threats.

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