STATEMENT OF ZOË BAIRD
PRESIDENT, MARKLE FOUNDATION

House Permanent Select Committee on Intelligence
U.S. House of Representatives
October 19, 2005

Mr. Chairman, Ranking Member, Honorable Members of the Committee, thank you for the invitation to appear today. I appreciate the opportunity to speak on the progress of the Office of the Director of National Intelligence (DNI).

Overview of Recommendations

More than a year ago, the President issued Executive Orders to create an Information Sharing Environment (ISE) and in December 2004, Congress enacted the Intelligence Reform and Terrorism Prevention Act of 2004 specifying the attributes of such an Information Sharing Environment and the Program Manager, privacy institutions and protections it anticipated as part of the environment. While there has been some progress, we still have a long way to go to implement this law. The government-wide direction and accountability anticipated in both the Executive Orders and the Act should today be a major priority for the DNI. Without effective information sharing, information collection remains stovepiped and the importance of information held by different agencies or at different levels of government cannot be understood. **My statement centers on the following four recommendations:**

- **Re-establish a greater sense of urgency to share information and a clear expectation that the DNI will report on progress regularly to the President;**
- **Empower the ISE Program Manager;**
- **Translate law and executive orders into government-wide consistent guidelines;**
- **Focus on establishing trusted information sharing relationships, including with state, local, tribal organizations and the private sector, rather than structural reorganization.**

Immediate actions that can be taken by the DNI are to: staff and fund the Program Manager's office adequately; assume clear authority for the immediate decisions that have to be made over government-wide guidelines; determine with the Department of Homeland Security and the Federal Bureau of Investigation a consistent process to

appropriately include state and local government officials so they do not continue to feel disenfranchised; establish priorities for modernizing the information sharing guidelines that empower government employees to share information while protecting civil liberties and privacy, and priorities for modernizing the technology infrastructure of key agencies to facilitate sharing; develop an Information Sharing Institute that draws on private sector talent; and reestablish the sense of urgency. In addition to briefing the President daily on collected intelligence that has come to the DNI, the DNI should take the initiative to brief the President regularly on steps taken to implement the information sharing environment because without information sharing the DNI cannot be providing the President with the best available intelligence.

Perspective

As President of the Markle Foundation, I have had the privilege to convene a Task Force on National Security in the Information Age. The Task Force I have been honored to co-chair with Jim Barksdale, is comprised of leading national security experts from the administrations of Presidents Carter, Reagan, Bush, Clinton and Bush, as well as widely recognized experts on technology and civil liberties, and was created to focus on how best to mobilize information and intelligence to improve security while protecting privacy and civil liberties. We issued two reports that are relevant to the mission of the Office of the Director of National Intelligence (DNI).

In addition, from 1993 to 2001, I was a member of the President's Foreign Intelligence Advisory Board and I also served as a member of the Congressional Commission on the Roles and Responsibilities of the United States Intelligence Community. I no longer have access to classified information, but I continue to be an informed observer of the intelligence community. My remarks today are based on an outside look at the organization of the DNI.

Both the Markle Task Force reports, "Protecting America's Freedom in the Information Age" (October 2002) and "Creating a Trusted Information Network for Homeland Security" (December 2003) have stressed the importance of creating a decentralized network of information sharing and analysis that achieves security while at the same time protects our civil liberties. We need to create an Information Sharing Environment that fundamentally changes the way we think about the business of national and homeland security. It requires clear and understandable rules and business practices on collection and sharing of data that is permissible and that which is prohibited. The Executive Branch and the Congress must assume leadership for this task and must both seek out, not avoid, responsibility.

Creating an Information Sharing Environment

On September 6th of this year, Co-Chairman Jim Barksdale and I sent a letter to the President on behalf of the Task Force with our thoughts on the progress of the Information Sharing Environment (ISE). The letter is attached and is available on Markle's website (www.markle.org) and my remarks today largely parallel it.

Timeline – Greater Sense of Urgency Needed

Many first steps have been taken in the right direction, but much more needs to be done and the pace needs to be accelerated. We recognize the competing demands of an ongoing military engagement abroad and back-to-back catastrophic natural disasters, but getting information sharing right will pay dividends not only in preventing terrorist attacks, but natural disasters as well. The line between national and homeland security continues to blur. It is time to stop applauding first steps and to raise our expectations for progress.

The nation must move to implement an effective ISE with much greater urgency. There are many initiatives that can be taken immediately, and many policies that must be adopted to empower government officials and provide assurance of privacy protections. The same sense of urgency and focused attention exercised by our military and intelligence men and women in the battlefield must be applied to reforming how government agencies work together to understand and prevent the threats to our nation.

Well-motivated people throughout the government are having a hard time adjusting to the new realities. In our letter to the President, we urged him to reiterate to Cabinet officers and all U.S. Government officers that they should interpret applicable laws and regulations to enable information sharing and not use old interpretations as an excuse to protect prior approaches. Any ambiguities as to authorities and lines of responsibility should be construed in favor of sharing and against turf battles. We still hear too many stories, despite explicit Presidential and Congressional direction, of departments and agencies using arguments from interpretations of their authority prior to the change in the law to protect their turf. Constructive Congressional oversight is needed here and the White House staff should itself take a more active role. The Intelligence Community should embrace rather than resist change and realize that change is not a rejection of the past, but a path to the future.

This process will take continuous commitment and persistence from the leadership and all stakeholders. The issues are tough. We are aware of several individual agency initiatives that show good promise. Some examples include:

-The FBI has developed the FBI Intelligence Information Report Dissemination System (FIDS); FBI officers are being trained and issuing more intelligence reports that are shared with the intelligence community;

-The National Counterterrorism Center (NCTC) is enhancing collaboration across the foreign/domestic divide that was so detrimental to our efforts before 9/11.

Program Manager for Information Sharing

Now that the DNI has the administrative responsibility for the Program Manager, he must assume the responsibility for the success of that office. The DNI must also recognize that the Information Sharing Environment extends beyond the Intelligence Community. As a

clear indicator of this, we recommended to the President that the Program Manager chair the Information Sharing Policy Coordinating Committee.

The Program Manager's office should immediately be staffed with the appropriate talent and given the resources needed to get the job done. More full-time government employees (FTE) positions must be provided. The Deputy Director of National Intelligence testified in July that they were striving to have the Program Manager's key leadership positions filled by mid-August. It is now mid-October and not much has changed.

New Guidelines and Policies

High-level direction and sweeping change is needed to remove any pre 9/11 confusion about information sharing. We have emphasized the immediate need for clear, new government-wide policies and guidelines for dramatically increasing information sharing, while protecting our civil liberties and protecting sensitive information. Regrettably, any confusion created about how to reconcile new legislation and executive orders with prior laws governing agencies and departments have not been resolved by the Department of Justice, the DNI or another responsible party designated by the President. A single set of policies across the government, with some additional rules depending on agency-specific missions, should end confusion and interagency battles about whose rules apply in particular situations.

We believe the DNI's office must take responsibility for ensuring that the changes mandated in legislation and executive orders result in changes in practice. We assume that the President is looking to the DNI to assume such responsibility.

These new guidelines should at a minimum include:

- Clear and enforceable rules and procedures that ensure information is accessed, shared, handled and retained in a manner that meets operational efficiency and security, while protecting our nation's privacy and civil liberties.

- Updated policies on the U.S. Persons rule: Since at least 1981, access to and sharing of intelligence information collected by U.S. Government agencies has been controlled by two factors: (1) whether information was collected within the territory of the United States or overseas; and (2) whether information involved a U.S. Person (U.S. Citizen or Permanent Resident Alien). These distinctions remain relevant for the collection of intelligence, but we believe they should no longer be the basis for controlling access to and sharing of intelligence information collected by the government. While there is broad recognition that these rules must change in the post 9/11 world, there also is justifiable concern that they be replaced with easily understandable rules that serve the same goal of protecting our civil liberties. In the next several months, our Task Force will propose a new approach to these issues that we believe can initiate a necessary dialogue about how to move beyond these outmoded rules while enhancing both civil liberties and operational success.

- New classification procedures: Executive Order 13356 recommended that originator control (ORCON) be used very judiciously. Information sharing should not be impeded because of outdated classification rules that classify information according to sensitive intelligence collection sources and methods. Furthermore, we must work to extinguish the belief that those who collect information own it. The President clearly stated that standards be developed "requiring terrorism information be shared free of originator controls, including, for example, controls requiring the consent of the originating agency prior to the dissemination of the information outside any agency to which it has been made available, to the maximum extent permitted…."

- Technical and organization mechanisms for policy compliance, oversight, and dispute resolution are needed to minimize and adjudicate failures to share information. This will reduce risk aversion by government officials who might be concerned about the personal impact of wrong decisions in a new environment.

- A comprehensive and independent assessment of the value being created by the Information Sharing Environment.

A Risk Management Approach to Information Sharing

We realize that many in the Intelligence Community have concerns that the increased focus on information sharing creates a greater risk of damaging security breaches. What the Task Force has recommended – and I believe is critical – is that a distributed information sharing system like the ISE contain policy, procedural, and technical protections including robust access controls that reduce the risk of unwanted disclosure and promote trust. We are not advocating that all information be shared with everyone; we suggest that information must be accessible to those users who need it and are authorized to see it. This will require leadership by the DNI to determine legitimate user needs and innovative cross-agency teams of people working problems together.

Sophisticated technology exists to secure and protect information and we must take full advantage of it. However, the government must recognize that perfect information security is not possible and that the costs of seeking it are too high. There are security risks not only from information falling into the wrong hands, but also from information failing to find its way into the right hands. The government's current approach to protecting classified information does not recognize this risk from failing to share. As wrenching as it is, the government must move to a risk management approach to protecting classified information that balances the risks of failing to connect critical information and adopts flexible and creative mechanisms for mitigating risks on both sides.

Privacy and Civil Liberties

As the Director of National Intelligence continues to coordinate and implement change in the intelligence community, he must consistently and seriously consider privacy and civil

liberty interests. Both the Congress and the Executive Branch must demonstrate that privacy is a priority. The Chairman and Vice Chairman of the Privacy and Civil Liberties Oversight Board in the Executive Office of the President have not been confirmed and the Board has never met. We hope the members have begun to be briefed so that, if confirmed, they are ready to assume their responsibilities immediately. It is critical that these oversight mechanisms established by law and executive order become operational immediately and get engaged as policies and guidelines are developed.

Furthermore, the position of the Chief Privacy Officer at the Department of Homeland Security must be filled again quickly.

Acquisition Procedures for New Information Technology

We cannot afford to lose the innovation race to the terrorists who are aggressively using technology like the Internet to connect and train recruits as well as plan and execute operations. Our government must be much more flexible and adaptive, taking full advantage of new technologies as they become available.

A Request for Information (RFI) was issued recently by the Program Manager seeking vendors to provide Electronic Directory Services (EDS) to "enable authorized participants to locate and access information, organizations, services and personnel in support of their respective mission requirements for terrorism information." We have recommended that a directory service is a critical element of an effective Information Sharing Environment, but it is not clear the Program Manager has the resources or authority to implement such a system. The technology is available to get this done, but it must be introduced quickly using an incremental approach. Attempting to seek a perfect solution will paralyze the effort – just as we have seen in other programs.

State, local, tribal and private sector

My last concern has to do with an aspect of information sharing where very little progress has been made. Yes, it is true that more intelligence information is being shared with state and local officials and even with the private sector. However, the nature of the terrorist threat requires that we harness all resources available and, within guidelines that protect privacy and civil liberties, we develop two-way engagement with key organizations outside the federal government. Because terrorists are presumably living and working among us, some of the best intelligence may come from non-traditional and unclassified sources.

Meetings with state and local officials and the private sector have led us to believe that the federal government has not yet realized the value of information identified by state and local entities. A system to integrate this information has not been developed. Much more attention must be paid to this gap, because we as a government are ignoring a critical component of national security. This must be done jointly with the Department

of Homeland Security because it is partly the reason why that department was created. I know this is one of the toughest challenges facing the federal government, but it must be done.

An Information Sharing Institute

The Markle Task Force has had initial discussions with and submitted a concept paper to the Director of National Intelligence and the Program Manager to create an **Information Sharing Institute** – a brand new federally funded research and development center (FFRDC) that would marshal available expertise and resources, both inside and outside the federal government, to advise on implementation of the policy and technology decisions necessary to creating a robust information sharing environment that protects civil liberties. The Institute would be a new potent collection of resources dedicated to supporting the success of this central mission, but not encumbered by the institutional agendas and cultural biases that often exist within departments and agencies.

Should Congress and the DNI see the benefit of such an Institute, or something like it, the Markle Foundation and members of its Task Force are prepared to work with the DNI to help stand up this new organization.

Recommendations

Our Task Force will be announcing some proposals over the next months, but we offer a few specific recommendations to the Committee as you consider priority actions. These recommendations are in addition to the underlying point that the administration must get on with fully establishing and empowering the Program Manager.

- The DNI must establish and publish government-wide guidelines to promote information sharing as called for in the Act and Executive Order;

- The Program Manager should act quickly on the RFI issued to establish electronic directory services; this is a critical step toward better information sharing;

- The DNI should convene a group immediately to explore the options for creating the Information Sharing Institute; short term measures should be identified if creating a new organization is a longer term goal;

- Working with the Congress, the DNI should support the Program Manager in sponsoring some pilots which demonstrate information sharing between federal agencies, state, local, tribal and the private sector;

- Establish a panel of experts, primarily from industry, to review and advise the program manager, DNI, DoD, DHS, and Justice on architecture and system design (particularly important given the number of failed IT and information sharing programs between those four organizations);

- Consider establishing a small staff at each of the major units of the intelligence community that would be aware of the operations and issues within that agency and could report to the DNI staff and provide a way for the DNI to communicate to these agencies his goals and priorities;

- Congress should move quickly to act on key positions that are pending confirmation, and if they are not confirmed the President must quickly nominate others (the Privacy and Civil Liberties Oversight Board Chairman and Vice-Chairman have not been confirmed, and neither has a General Counsel to the DNI, a particularly important position given the legal barriers and confusion cited by many as preventing implementation of the ISE);

- The DNI should develop cross-community training and provide incentives and awards for information sharing.

Conclusion

Our nation has now reorganized the intelligence community as called for in many earlier reports. For this to address the significant challenges of the future, we must train government employees to work in new ways, develop our civil liberties guidance, sponsor research on new technologies and methods, and create systems that manage information in smarter and more cost-effective ways, while providing real security improvements and accountability. Any future intelligence failures will not rightly be blamed on legal constraints that prevent sensible information collection and sharing. The authorities to collect and share information exist; we must thoughtfully exercise them.

Finally, we must work toward improving our national security without eroding privacy and civil liberties. Our task force has expressed concern that if another major attack were to take place on our homeland, the immediate reaction could cause the pendulum to swing toward measures that impinge on our privacy and civil liberties in ways in which none of us would support given time for thoughtful consideration and debate. We have the opportunity now and we should seize it.

Thank you again for the invitation to appear before you, and I welcome any questions you may have.