STATEMENT OF WILLIAM P. CROWELL

MARKLE TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE

The House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment
November 8, 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 progress made towards building an Information Sharing Environment.

Key Task Force 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 (IRTPA) of 2004 specifying the attributes of such an Information Sharing Environment. In particular, Section 1016 on Information Sharing tasks the President with creating an "information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties". The IRTPA also designates the new position of Program Manager to plan and oversee the implementation of the ISE. Responsible for terrorism information sharing across the Federal government, the Program Manager is tasked to develop policies, rules, and procedures to govern the operation of the ISE in consultation with the Information Sharing Council. On October 25th, 2005 the President signed Executive order 13388 creating the anticipated Information Sharing Council as required by the Act.

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 five recommendations suggested by the Markle Task Force on National Security in the Information Age:

- **Re-establish a greater sense of urgency to share information;**
- **Empower the ISE Program Manager;**
- **Translate law and executive orders into government-wide consistent guidelines;**
- **Adopt a Risk Management Approach to Information Sharing**
- **Focus on establishing trusted information sharing relationships, including those with state, local, tribal organizations and the private sector, rather than structural reorganization.**

Perspective
I have had the privilege to participate as member in the Task Force on National Security in the Information Age since its creation in March 2001. The Task Force which is co-chaired by Zoë Baird and 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.

My own background includes having been a former Deputy Director of Operations and then Deputy Director of the National Security Agency (NSA) during the intelligence draw-downs of the early 1990's. After retiring from NSA I became CEO of a public company in Silicon Valley that was focused on securing cyberspace for industry and government customers. After my company was acquired in early 2003 I became an independent consultant in security and intelligence systems and serve on a variety of boards of technology companies. My remarks today are based on an outside look at progress made by government.

The Markle Task Force has issued two reports: "Protecting America's Freedom in the Information Age" (October 2002) and "Creating a Trusted Information Network for Homeland Security" (December 2003). Both 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. We believe that the Executive Branch and the Congress must both assume leadership for this task to succeed.

Creating an Information Sharing Environment
On September 6th of this year, Co-Chairmen Jim Barksdale and Zoë Baird 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), as is the response from the White House. In addition Zoë Baird testified to the House Intelligence Subcommittee on Oversight at an Open Hearing on the Office of the Director of National Intelligence on October 19, 2005. My remarks today largely parallel and mirror the letter and subsequent testimony.

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 in dealing with natural disasters as well. National and homeland security are based on many of the same concepts. 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 of departments and agencies using rigid interpretations of their authority prior to the change in the law in order 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 these changes 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 foreignintelligence/domestic information 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, we believe 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 into the DHS, Federal law enforcement, and State and Local public safety arenas. Further, 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. Obviously the priority response to Hurricane Katrina may have delayed the formation of the office, yet 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 other responsible parties 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 exercise 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 lawfully 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 specified that originator control (ORCON) be used very judiciously. Information sharing should not be impeded because of excessive classification rules that classify information according to sensitive intelligence collection sources and methods even when it could have been acquired by less sensitive means. 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 timely dispute resolution are needed to minimize and adjudicate failures to share information. There should also be a mechanism to turn disputes into policy. 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 to successfully perform their assigned missions 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 risk of release and sharing should be balanced with the risk of not sharing. 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. You cannot connect dots that you cannot access.

Privacy and Civil Liberties

As change in the intelligence community is being furthered, privacy and civil liberty interests must be considered consistently. 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

Our 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. We know this is one of the toughest challenges facing the federal government, but it must be done.

Recommendations

The 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.

- Government-wide guidelines to promote information sharing as called for in the Act and Executive Order should be established as soon as possible;

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

- Working with the Congress, the Executive branch 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);

- 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);

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.