TESTIMONY OF ZOË BAIRD, PRESIDENT, MARKLE FOUNDATION
CHAIRMAN, TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE

Select Committee on Homeland Security
U.S. House of Representatives
"Information Sharing After September 11: Perspectives on the Future."
June 24, 2004

TESTIMONY OF ZOË BAIRD, PRESIDENT, MARKLE FOUNDATION
CHAIRMAN, TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE

Select Committee on Homeland Security
U.S. House of Representatives
"Information Sharing After September 11: Perspectives on the Future."
June 24, 2004

Good Morning, Chairman Cox, Congressman Turner and members of the Committee. I appreciate the opportunity to testify today.

Reports due out this summer from the Senate Intelligence Committee and the 9/11 Commission are expected to be highly critical of our nation's information collection and sharing capability. As we await the release of these reports, we can predict one of their findings with near certainty: That systemic barriers to information sharing, which seriously hampered the efforts of our nation's intelligence agencies prior to the September 2001 terrorist attacks, still exist today.

A number of recommendations have already been made about what further reforms are needed to better equip our government in the fight against terrorism. Some have recommended an American domestic intelligence agency, similar to Britain's MI-5, to improve collection and analysis of intelligence at home. Others have advocated the creation of a Director of National Intelligence (DNI) with greater authority than the current Director of Central Intelligence, to direct and coordinate the entire intelligence community.

Once the debate begins in earnest, we will find ourselves grappling with a number of very complex questions. For example, does the "line at the border" – the different rules for collecting and handling of intelligence depending on whether it is foreign or domestic – a line already eroded, need to be substantially reconsidered? Must we find new ways to protect critical interests like sources of information or the privacy of our people because the line at the border or classification systems prevent us from fully understanding terrorists' intentions and capabilities?

It will take time to determine the right course of action on proposals for an MI-5 or an DNI, and once that course has been plotted, implementing any structural reforms could take years. But we do not have the time to wait to improve information collection and sharing. We need to impress upon responsible officials the urgency of this task and we need to act now. The actions we take can accelerate the ability of any agency organization, present or future, to improve our security.

Fortunately, by capitalizing on America's technological capabilities, we can begin to make our nation safer. Using currently available technology, the government can set up a network that streamlines operational and decision-making processes and substantially improves our ability to share information in order to prevent terrorist attacks. And when paired with clear guidelines to govern the system and effective oversight, the use of information technology can also be the best way to protect privacy and civil liberties.

For the past few years, I have had the privilege to convene the Markle Foundation's Task Force on National Security in the Information Age. The Task Force, comprised of leading national security experts from the administrations of Presidents Carter, Reagan, Bush and Clinton, as well as widely recognized experts on technology and civil liberties, was created to focus on the question of how best to mobilize information and intelligence to improve security while protecting established liberties. In fact, one of our unifying principles is that information -- managed through information technology -- is the key to enhancing security.

In our most recent report, **Creating a Trusted Information Network for Homeland Security** (http://www.markletaskforce.org/), the Task Force recommended the immediate creation of a Systemwide Homeland Analysis and Resource Exchange (SHARE) Network, which would foster better analysis and sharing of information among all relevant participants at every level of government, with built-in practical and technological safeguards for civil liberties. Or, as one of your own Committee Members, Congresswoman Jane Harman, has called it, a "virtual reorganization of government."

The SHARE Network would represent a fundamentally new way of using information to facilitate better, faster decision-making at all levels of government. It has several key features:

- SHARE is a decentralized, loosely coupled, secure and trusted network that sends information to and pulls information from all participants in the system. Such an approach empowers all participants, from local law enforcement officers to senior policy makers.
- SHARE is based on the concept of "write to share." Instead of the Cold War based culture that placed the highest value on securing information through classification and distribution restrictions, SHARE recognizes that sharing information makes that information more powerful because it links it to other information that can complete the picture. SHARE moves from a classification system to an authorization system. By taking steps like incorporating "tear lines" in document formats, SHARE would encourage reports that contain the maximum possible amount of sharable information.
- SHARE is a hybrid of technology and policy. The system would use currently available technology to share and protect the information that flows through it. And when paired with clear guidelines that would determine the collection, use and retention of information and who should have access to information, it can both empower and constrain intelligence officers, and provide effective oversight. Such an approach is also the best way to protect privacy and civil liberties.
- SHARE allows for vertical and horizontal co-ordination and integration. Information would be able to flow not just up the chain of command, but also to the edges of the system.
- SHARE enables analysts, law enforcement agents and other experts to find others with common concerns and objectives, to come together in shared workspaces, to form "virtual" communities to exchange information and ideas.

While those are just a few of the technical and policy features of the SHARE Network, I think it would be useful to give you a real world illustration of how the system could actually operate.

Say a field agent at the Chicago FBI office and a CIA operative in Kabul become aware of separate leads that if put together might point to a bio-warfare attack in Chicago. Under the current system, reports from these two agents are unlikely to have enough actionable information to be moved through the system. However, using the SHARE Network, these reports would be linked through similar key words such as "virus" and "Chicago" or other linking tools. Instead of being housed in classified files and filing cabinets at the CIA and FBI, these reports would be distributed electronically to people who should see them. They also would be posted and available to be pulled by network participants with a particular interest. An analyst at TTIC, for example, might see both reports, contact the CIA and FBI agents and others to discuss their reports, begin to connect the dots and define actionable objectives. The FBI, CIA, and TTIC players could form "a virtual task force" by reaching out to other relevant agencies and individuals, perhaps at Department of Homeland Security, the Centers for Disease Control or a local police department, for more information. And they could organize the work themselves, without losing time or going to their superiors in Washington for approval.

Based upon their discussions, this group could now create actionable intelligence for their agencies: the CIA might elevate the information to a higher level, to the director, or perhaps up to the president. Through local contacts, the FBI would have the option of notifying local police, so they could watch for activities related to a potential plot.

Meanwhile, because access to certain kinds of personally identifiable information would be restricted, and systems built in to verify the identities of those permitted access, we will have improved information sharing while better protecting our privacy and civil liberties.

Members of our Task Force have met with a number of officials at federal government agencies regarding our recommendations—some repeatedly-- and have seen a high level of interest. In fact, a number of government agencies have been moving to direct the creation of processes that use key elements of the SHARE Network. The FBI, for example, has taken a number of positive steps in developing its new information sharing policies, including adopting a potentially extremely important policy of "writing for release," which encourages tear lines and "shar[ing] by rule and withhold[ing] by exception".

TTIC's posting of intelligence reports and other items on "TTIC Online," although not broadly available, is a step toward the kind of sharing we contemplate. And the Homeland Security Information Network, currently being developed by DHS, could strengthen the flow of real-time threat information to state, local, and private sector partners if they plan to share adequate information.

While this progress is positive, an agency-by-agency approach is not adequate. Individual agencies can only go so far before they confront obstacles to sharing with other agencies of the federal government or with state and local actors, not to mention the difficulties involved in working with private sector entities. In order for this networked approach to succeed, a national framework, such as our proposed SHARE Network, is critically needed.

Members of Congress can contribute to our nation's ability to prevent and respond to terrorism by calling for the creation of an information sharing network with the characteristics of the SHARE Network. In our Report, we called for DHS to be designated the lead agency of an interagency, public-private process to establish the concept of operations for the network. Policy guidelines need to be written that both empower government officials to share information and also strengthen protection of privacy and other civil liberties. Agency CIOs need to be given the direction, authority and budgetary commitments to build the network. CIOs also need to have the funds protected so that the funding is not reallocated. Agencies need to be encouraged to acquire information technology that is interoperable (across agencies, across systems, and with legacy systems), and has common data standards as well as security, access controls, identity controls, and audit capabilities. Availability of technology is not a hurdle to adoption of the SHARE Network; the hurdle is the manner in which agencies acquire technology.

In addition, proposed and current information sharing initiatives such as the Homeland Security Information Network, TTIC, US VISIT and CAPPS II need to be jointly reviewed as to whether they support these network objectives. Otherwise, waste, stovepiping and redundancy will occur if they are not built according to a common concept of operations.

The collection, use and sharing of information by government agencies needs to be guided by both Presidential directive and by Congressional oversight. We laud Congress's commitment to establishing internal oversight mechanisms within the DHS, including a privacy officer and a civil rights and civil liberties officer. We encourage the further development of informal and formal means of congressional oversight of the government's access to, use, retention, and dissemination of private sector data.

Other government bodies have a role to play as well. The Technology and Privacy Advisory Committee to the Secretary of Defense, on which I served, recently built on the Markle Task Force Report and made further recommendations for processes to protect privacy and civil liberties, including requiring in certain circumstances that an agency articulate the relationship to terrorism of information they seek on U.S. persons, and use of the FISA court for domestic information collection in sensitive circumstances.

Finally, as we have outlined in our Report, it will require continued engagement from the President himself, the heads of government agencies, as well as continual oversight from Congress to ensure follow-through. Indeed, agencies' performance towards a virtual reorganization should be evaluated by Congress after a reasonable implementation time, using specific and clear objectives for improved information sharing, based upon the set of metrics in our Report. If an agency has not performed adequately, the President and Congress should consider making any necessary changes.

While government migrates to the kinds of IT systems business has used for years to achieve the capabilities described above, there are immediate steps that can be taken to begin reaping the benefits of new business processes. We should immediately create electronic directories to link people in different agencies working on the same problem, to identify experts in the private sector and universities, and to indicate which agencies have information on subjects of interests. We should adopt clear rules empowering government officials to get the information they need from other agencies. We could begin by ensuring that detailees at intelligence fusion centers have online access to all information. To facilitate sharing, we need to revisit the application of the "need to know" principle. To protect privacy, these rules should allow access to information without identifying U.S. persons by name, and establish processes for learning identities when necessary. And, to ensure greater public and congressional confidence, we need clear guidelines on how people get their names off watch lists, and how they seek redress for adverse government actions. The US VISIT contract, the development of the Virtual Case File at the FBI, the ongoing work of the TTIC and the TSC all offer opportunities to achieve critical, immediate incremental reforms if they are required to serve a common vision instead of being developed in stovepipes.

Implementing a system like the SHARE Network would allow agencies tasked with protecting our nation from terrorism to build information sharing into their overall mission before, and as part of, any major restructuring of our domestic or foreign intelligence agencies that Congress might undertake in the future. It would prevent information from being kept in agency silos, as too much still is, and would encourage analysts to push information to the edges of the system— to FBI and customs field agents, to police— instead of only moving information up the chain to the next level in an agency hierarchy or to a narrow set of analysts or operational personnel who are not allowed to share it with others.

Information, managed through technology, is critical to enhancing our security while protecting important civil liberties. Information-sharing itself is not the goal; rather, it is the means by which we can most effectively enhance security and protect privacy, by maximizing our ability to make sense of all available information. The nation can never sufficiently harden all potential targets against attack, so the government must develop the best possible means to obtain advance warning of terrorist intentions through better intelligence.

The network the Markle Task Force has proposed would substantially improve our ability to uncover threats and prevent terrorist attacks. The technology to create such a network exists and is used in the private sector every day. Given the proper priority in budgets and leadership, we believe that it is possible to develop and implement major steps immediately, and many key elements of the SHARE network in about eighteen months.

Since September 11, many people in the government and the private sector have given a great deal of thought and effort to the problem of how our nation can use information and information technology more effectively to protect people from terrorism while preserving our civil liberties. Our Task Force has sought to contribute to the solution by providing the framework for a national strategy and an architecture for a decentralized system of robust information-sharing and analysis that makes the most effective possible use of information while instituting guidelines and technologies to minimize abuses and protect privacy.

Thank you.