

MARKLE FOUNDATION
Task Force on National Security in the Information Age

September 7, 2005

The President
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Re: Building the Information Sharing Environment

Dear Mr. President:

We write on behalf of the Markle Foundation Task Force on National Security in the Information Age. At our August 2005 meeting, the Task Force asked that after Labor Day we convey to you some thoughts as you prepare the report due this month to Congress on the Guidelines and Requirements to Implement the Information Sharing Environment mandated by the Intelligence Reform and Terrorism Prevention Act of December 2004 (the Act). We reconsidered sending the letter in light of the terrible loss from Hurricane Katrina, but concluded that you would appreciate this input since so many of the issues may be similar to those Secretary Chertoff and others have suggested be examined in an after action report on the response to the hurricane.

As you know, the Markle Task Force has issued two reports that frame a decentralized network of information sharing, guided by policy principles that simultaneously empower and constrain government officials and provide meaningful privacy and civil liberties protections for our people. The information sharing environment requires, as we stated, clear and understandable rules and business practices on collection and sharing of data that is permissible, and that which is prohibited.

Your Executive Orders and the Act have generated genuine progress toward creating an Information Sharing Environment (ISE), and individual and agency initiatives show good promise. We remain concerned, however, that risk aversion and bureaucratic resistance to change continue to hamper the carrying out of announced new policies. The constitutional and statutory authorities to do what needs to be done exist. We urge you to reiterate to your Cabinet officers and all U.S. Government officers that they should interpret all applicable laws and regulations to enable information sharing rather than use ambiguities between the Act and prior law which Congress left unresolved as an excuse to protect prior approaches. They need to embrace rather than resist the change.

It is our view that we as a nation must move to create the ISE with great urgency, and that we should not be satisfied with the first steps – as major as they are – that have been taken in the four years since the 9/11 attacks. The same sense of urgency and focused attention exercised by our military men and women in the battlefield must be applied to reforming how government agencies work together to understand and prevent the threats to the nation.

In your report to Congress, we believe it will be helpful if you address the following:

1. Make clear that the Director of National Intelligence (DNI) has responsibility for the creation of the ISE. Since the ISE Program Manager (PM) has been placed administratively in the DNI's office, the DNI must assume the responsibility to ensure that the PM creates an effective ISE with the full recognition that such a system extends beyond the Intelligence Community. Because successful implementation of the ISE is critical to achieving intelligence goals and meeting other responsibilities of the DNI such as providing the President with a well-informed briefing, nothing in his portfolio is more fundamental.
2. Emphasize the development of government-wide policies and guidelines immediately as the foundation for the adoption of information sharing capabilities and procedures. Sweeping change is needed to remove any pre-9/11 confusion about information sharing that, regrettably, still exists in some departments and agencies. A single set of policies across the government, while recognizing the need for some additional rules depending on agency-specific missions, should end confusion and interagency battles about whose rules apply in particular situations.
3. Consistent with our earlier recommendations, and as required by the Act, these policies should address four key issues.
 - Clear and enforceable rules and procedures are needed 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. Perhaps most urgently, the government needs to create new guidelines governing information sharing of "U.S. persons" data since that designation is an outdated boundary for what is permissible.
 - A clear and consistent government-wide process must be created that guides classification decisions to protect sources and methods while enabling access and sharing without undue or arbitrary dependence on originator control (ORCON).
 - Technical and organizational 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 ISE for different participants, including policymakers is needed.

We believe that addressing these fundamental policy challenges will accelerate the implementation of the ISE consistent with privacy and civil liberties concerns and national security needs.

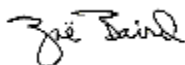
4. The PM should immediately be given the resources needed to get the job done by both Congress and the Administration. The White House staff and the DNI should ensure obstacles are removed. Because his responsibilities extend beyond the Intelligence Community, the PM should have enhanced authority within the Executive Office of the President. Thus, we recommend the PM chair the Information Sharing Policy Coordinating Committee in addition to chairing the Information Sharing Council.
5. Creating the Privacy and Civil Liberties Oversight Board in the Executive Office of the President was a key step in ensuring that effective information sharing for national security conforms to our nation's traditions and values. We hope the board will engage quickly as the policies and guidelines are developed.

The nation has only begun to mobilize the tremendous resources provided by the capabilities of its people and its advanced 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. We must train government employees to work in new ways, 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. It is our sense that people in government are already working hard and therefore instead of asking them to work harder, the leadership must create an environment that allows them to work smarter.

We remain concerned that if another terrorist attack were to take place in the U.S., the immediate reaction could cause the pendulum to swing toward measures that impinge on our privacy and civil liberties. Any potential 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, but cannot be realized without clear government-wide guidelines on how this can be maximized while protecting the security of information and the civil liberties of our people.

The Markle Task Force stands ready to assist in any way you may find useful.

Respectfully yours,



Zoë Baird



Jim Barksdale

Co-Chairs of the Markle Task Force on National Security in the Information Age

Cc: Stephen J. Hadley
Assistant to the President for National Security Affairs

Frances Fragos Townsend
Assistant to the President for Homeland Security

Joshua B. Bolten
Director, Office of Management and Budget

John D. Negroponte
Director of National Intelligence

Michael Chertoff
Secretary of Homeland Security

John R. Russack
Program Manager for Counterterrorism Information Sharing