Testimony of

John A. Russack

Program Manager, Information Sharing Environment
Director of national Intelligence
July 27, 2005

STATEMENT FOR THE RECORD BY
PROGRAM MANAGER
FOR THE INFORMATION SHARING ENVIRONMENT
JOHN A. RUSSACK
BEFORE THE
SENATE COMMITTEE ON THE JUDICIARY
July 27, 2005

Mr. Chairman, Senator Leahy, and Members of the Committee:

Over the last year, both the executive and legislative branches of government have responded to the recommendations of the National Commission on Terrorist Attacks upon the United States (9/11 Commission) and the Commission on the Intelligence Capabilities of the United states Regarding Weapons of Mass Destruction (the WMD Commission) to improve information sharing while protecting the freedom, information privacy, and other legal rights of Americans. Last August the President issued Executive Order 13356 to ensure that terrorism information is shared broadly among federal agencies; state, local, and tribal governments; and the private sector. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (Public Law 108-458) devotes an entire section to this issue. So, while the institutional foundations are now in place to allow us to make significant progress in the way we share terrorism information, there are still a number of hurdles that exist that will require time and hard work to surmount. The Administration is committed to identifying and removing all impediments that prevent us from providing the necessary information to those who need it, when they need it.

In my statement today, Mr. Chairman, I first want to briefly describe the specific role of the Program Manager in implementing the Information Sharing Environment (the Environment). I will then highlight the major issues I believe must be addressed to achieve more open and transparent access to terrorism information as envisioned by both the 9/11 and WMD commissions.

ROLE OF THE PROGRAM MANAGER

In accordance with section 1016 of IRTPA, the Information Sharing Environment will be the combination of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of Federal, State, local, and tribal entities and the private sector to facilitate terrorism information sharing, access, and collaboration among users to combat terrorism more effectively. IRTPA required the President to designate an individual to serve for a two-year period as the program manager (PM) responsible for information sharing across the federal government. The PM's duties include:

? Planning and overseeing the implementation of, and managing the Environment;
? Assisting in the development of policies, procedures, guidelines, rules, and standards as

appropriate to foster the development and proper operation of the Environment; and
? Supporting, monitoring, and assessing the implementation of the Environment by Federal departments and agencies, and regularly reporting the findings to Congress and the President.
In April, I was designated by the President to be the PM. In June, the President directed that the PM be part of the Office of the Director of National Intelligence (ODNI). Although I report to the DNI, the mandate covers access to terrorism information across Federal, State, local and tribal governments and the private sector. We are now working to define specific objectives in support of IRTPA direction, develop a work plan, organize the staff, and fill key leadership positions with experienced people from a variety of backgrounds. FBI expertise will be an essential element of the PM's knowledge base.
In addition to defining the role of the Program Manager, IRTPA calls for the establishment of an Information Sharing Council (ISC) to assist the President and the PM in carrying out their responsibilities.
MAJOR ISSUES IN INFORMATION SHARING
On June 15, we submitted the PM's first deliverable to the President and the Congress. This preliminary report identified five broad issues that define the agenda for the Program Manager's office over its current two-year period. The first of these is that existing authorities, policies, and procedures governing roles and responsibilities can be ambiguous and conflicting. Because information protection standards vary, decisions on reconciling the need to protect information with the need to share information are applied inconsistently, contributing to information segregation rather than integration. The PM, in consultation with the ISC, will review these conflicting policies and develop recommendations to clarify the roles and authorities of participating agencies. With respect to the FBI, the policies relating to sharing of information between law enforcement and the intelligence community have been reviewed and commented on extensively already. I will make sure that existing policies fully reflect the current state of the law, so that information sharing is as robust as legally permitted, consistent with the need to protect information and other legal rights.
The second issue--trust between organizations--has been identified by a number of experts as a barrier to effective sharing. Organizations are often reluctant to share information because they believe that the recipients may misunderstand or misapply it. They perceive that the risks of sharing outweigh the advantages. Fostering trust across all organizations is a formidable challenge. Training and education, collaborative processes, personnel exchanges, and greater managerial accountability are all important factors in achieving the level of trust we need to win the war on terror. Increased trust should be a natural outcome of participation by all key stakeholders in the establishment and operation of the Information Sharing Environment. Trust plays a particularly important role in sharing between the law enforcement and intelligence communities, which have historically had distinct missions, cultures, and rules. My office will actively work to foster trust in the relationships between these communities.
The third issue concerns the inability of some or all users to access the information they need because of controls imposed by the originating organization. The need-to-know principle, that has influenced information sharing decisions since the early days of the Cold War, can no longer be the exclusive criterion for such decisions in the era of the war on terror. Moving to an Information Sharing Environment will necessitate shifting the paradigm to find the appropriate balance between the need-to-know and the need-to-share, but will still require rigorous safeguards to ensure protection of national security and the information privacy and other legal rights of Americans. The PM's office will work with the Information Security Oversight Office

and others to develop the policies and procedures required to achieve this fundamental change in thinking, recognizing, of course, that some access controls may be required by applicable laws or are otherwise necessary for protecting the freedom information privacy and other legal rights of Americans.

The fourth issue is one that has been highlighted by both the 9/11 and the WMD commissions, the Markle Foundation, and others. That is that improved information sharing can only be achieved in parallel with the protection of the information privacy and other rights of Americans. In response to IRTPA, a Privacy and Civil Liberties Oversight Board is in the process of being established to ensure that concerns with respect to information privacy and other legal rights are appropriately considered in the implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism. The Information Sharing Council will work in conjunction with this Board to address this issue as it applies to the Information Sharing Environment.

Lastly, the preliminary report identified the need to remove any technological barriers to information sharing. In large measure, the technology needed to improve interoperability and information sharing is already available today; it should be viewed as an enabler rather than a barrier. On the other hand, disagreements over roles and responsibilities coupled with inadequate or outdated policies, procedures, and standards often impede our ability to use available technology effectively. A number of experts have commented on the vast and confusing array of systems, databases, networks and tools that users must deal with. In most cases, however, this vast and confusing array is caused not by technological barriers, but by policies, protocols, and overly zealous security regulations. These and any other barriers must be removed so that technology can be used to its greatest advantage.

SUMMARY

Mr. Chairman, I appreciate the opportunity to provide the committee with a brief update on the activities of the Program Manager's Office, which is still in the early stages of being organized and staffed. My goals, for my two-year term, are to develop and coordinate an architecture and plan for implementing the Environment, and put performance goals and metrics in place so that we can measure our progress. I will be glad to discuss any specific concerns during the Question and Answer part of this session. Thank you.