Statement For The Record

By

Ambassador Thomas E. McNamara

Program Manager for the Information Sharing Environment

Before the

Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment

House Committee on Homeland Security

"Building on the Information Sharing Environment:

Addressing Challenges of Implementation"

2 P.M. May 10, 2006

Introduction

I'm here this afternoon to provide you my plans for a terrorism information-sharing environment (ISE) in which terrorism information can be shared broadly, effectively and seamlessly to protect our nation. Our ability to share terrorism information across all levels of governments and the private sector is fundamental to the success of our efforts to defeat terrorism. Congress has provided us a legislative basis, the President has provided more specific guidance, and my predecessor has provided an interim implementation plan, the final that will be delivered to Congress in July 2006. Now it is time to begin building capabilities that make the ISE operational to the men and women who support the national effort to detect, prevent, respond to and recover from acts of terrorism, and to convey the sense of urgency with which the Information Sharing Environment (ISE) must be developed.

I want to say, up front, that I assumed the position of Program Manager for the ISE on March 15, 2006, approximately two months ago. I thank you for this opportunity to share with you my initial thoughts and reflections. In time, I look forward to sharing with you more developed and detailed thoughts and opinions. As you may know, the Program Manager has a responsibility to report this summer to the President and to the Congress on the implementation plan and guidelines. This is a short timeframe, but I take my responsibility seriously. I also owe it to the President, and to my other superiors and colleagues to listen to and work with them before coming before you and speaking on behalf of myself and them.

However, I know that I have a responsibility to the Congress. In the past, on the several occasions when I have held senior positions in government, I have had a policy of consulting and working closely with the Congress to keep you appropriately informed of my work. I intend to continue that policy in this position. I have already told my staff that we will offer regular briefings to Members and staff of the committees that exercise

oversight responsibilities for the ISE and I am happy to report that we have already started that process.

Role of the Program Manager

As the Committee is aware, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) established the office of the Program Manager and designated by Presidential Directive to assist, in consultation the Information Sharing Council (ISC), in the development of polices, procedures, guidelines, rules and standards for the ISE at the Federal level, and to coordinate closely, in collaboration with the ISC, with State, local, and tribal governments and the private sector and relevant foreign partners, in the development and operation of the ISE. The Program Manager must also manage the development and implementation of that same environment by monitoring and assessing the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency, and policy compliance.

To do all this, the Office of the Program Manager is currently made up of about 15 Federal employees, plus contract support, and is situated within the Office of the Director of National Intelligence, although we are not an intelligence office. My authorities are government-wide with respect to overseeing development of the ISE. To be successful, the ISE must satisfy the needs of Federal, State, local, and tribal governments, and the private sector. Given the size of the office, you will appreciate that we do not operate as another bureaucratic layer that could impede progress and we do not substitute for responsibilities that each agency has to implement the ISE. We have limited time (two years) and a specific mandate. Each Federal agency, and State and local agencies, must take the responsibility for implementing the ISE. Our office will, however, do our best to oversee, manage, facilitate, and coordinate agency implementation of the ISE and information sharing mechanisms.

To advise me in this effort the IRTPA also established the ISC, which I chair, and which is composed of senior officials from 17 agencies and departments of the Federal government. To facilitate coordination with state, local, and tribal officials in

development of the ISE, we have established a State, Local and Tribal Subcommittee. It is my intention as chair of the ISC to keep in close contact with State, local, tribal, and private sector partners through regular meetings with them, and by inviting them to work closely with the ISC in the coming months.

To understand the complexity of the ISE one needs to realize that it affects the operations of a very large number of agencies of the Federal government. I divide those agencies into what I call five "communities." Those communities are: the intelligence community, the law enforcement community, the defense community, the homeland security community, and the foreign affairs community. Each community is a collection of departments and agencies with a specific focus on terrorism and terrorism related information. The development of the ISE will impact a large number of similar governmental entities at State, local, and tribal levels of government, and many entities in the private sector.

WHAT THE ISE MUST DO TO SUCCEED

The ISE must accomplish four key things. First, it must facilitate the establishment of a trusted partnership between all levels of government, the private sector and our foreign partners to mitigate the effects of terrorism against the territory, people and interests of the United States of America. The ISE, as we envision it, will enable the trusted, secure, and appropriate exchange of terrorism information, in the first instance, among those five communities, and also to and from State, local, and tribal governments, foreign allies, and the private sector, at all levels of security classifications.

Second, the ISE must promote an information sharing culture that eliminates information gaps between partners and facilitates the creation and sharing of validated, actionable information. We want to get the right information, to the right people, at the right time to ensure success within a system of rules established to protect the information privacy and other legal rights of Americans as well as sensitive sources and methods. I believe that right now the main problem is not too little information flow

from the five federal community members to State and local ISE elements, but too much flow of uncoordinated information to the State and local levels. There is, also, too little flow of the right kinds of information in actionable form. Part of the cultural change we need is for all participants at all levels of government and the private sector to understand that the purpose of the ISE is to serve and satisfy consumers of information, who are at the same time all members of the ISE. In contrast, there is little information flow from the local and tribal levels to the State and Federal levels. This means that valuable information potentially is being wasted because it is not reaching the proper consumers.

Third, the ISE must function in a decentralized, distributed, and coordinated manner. In effect, we need to implement a federated ISE that incorporates the full cooperation and coordination of the Federal, State, local, tribal, and private sectors entities. This way ISE participants can be governed by an agreed set of common standards and practices that conform to mandated guidelines. Where these cannot be common, they must, at least, be compatible. Where necessary and consistent with proper information flow, these standards and guidelines must take into account the needs and desires of the constituent elements, including the security, where required, of the information in the ISE. The ISE should provide direct, continuous, online access to information that is readily available for analysis, investigations and operations without sacrificing privacy and security.

Finally, the ISE must be developed and deployed incrementally by leveraging existing information sharing capabilities and deploying centralized core functions and services to provide new capabilities and value-added business benefits to all ISE members. Only by building from what we now have functioning can we continue to share information effectively and uninterrupted.

ISE Implementation Approach

A critical question for implementing the ISE is how best to get it up and running while addressing the myriad policy, process and technology differences among multiple organizations tasked to perform disparate missions. These differences pose challenges and impediments which include: conflicting or incompatible policies, processes, and

procedures for information classification, access vetting, security and privacy; incompatible or non-interoperable legacy systems and data formats; conflicting approaches to information sharing; and conflicting management structures for overseeing information sharing partners.

In many cases these differences have evolved over decades. It is not realistic to think that we can overcome them in a short period of time. But, we must proceed with intelligent, focused, and determined energy and dispatch. I believe this means that we must prioritize the many tasks before us. I am in the process of deciding those priorities. In the past few weeks I have set several priorities – not all of those that need to be set, but several of the highest ones. Let me turn to those areas now.

To realize the ISE, the challenges mentioned above, must be addressed. Common policy, process, data and technology standards for terrorism information sharing must be implemented across all ISE agencies. The President's December 16, 2005, Memorandum entitled, *Guidelines and Requirements in Support of the Information Sharing Environment* (The President's Memorandum) established the ISE requirement to "implement common standards across all agencies regarding the acquisition, access, retention, production, use, management, and sharing of information." The comprehensive and complex nature of such a *transformational effort* will require significant time to fully implement. However, the ISE is an urgent national imperative that cannot wait for such an effort to be completed before enhanced information sharing is achieved. The key is to achieve initial operating capability for the ISE in the short term, and continue to build on existing capabilities, while the comprehensive, transformational effort proceeds in the longer term.

We have begun the work to assist in more clearly defining roles and responsibilities among departments and agencies by developing policies, business processes, and technologies to implement the ISE. There are already capabilities and initiatives underway to improve the Nation's ability to share terrorism information.

- The DNI has enabled the National Counterterrorism Center (NCTC) to step up to

the Federal leadership role that the President and Congress have laid out. Admiral Scott Redd and his staff hold video teleconferences three times a day with analysts across the homeland security, law enforcement, intelligence, foreign policy, and defense communities. NCTC collects intelligence information and analysis from 28 different government networks which come into NCTC and post it on a single website where it is then accessible by individual agencies.

- The Terrorist Screening Center (TSC) used to receive terrorism information from NCTC via a computer disk. Today, the TSC receives this information directly from NCTC in controlled unclassified format and electronically. This has greatly enhanced the ability for TSC to efficiently produce the Terrorist Watch List and distribute it to local law enforcement partners.

- Fusion Centers have been established -- or are in the process of being established in 42 states. Additionally, a growing number of localities – particularly major urban areas -- are also establishing similar centers. State and local fusion centers are a critical component of the ISE because they can dramatically enhance efforts to gather, process and share locally generated information regarding potential terrorist threats and to integrate that information into the Federal efforts for counterterrorism. Federal law enforcement is working closely with these Fusion Centers.

- The Department of Homeland Security (DHS) offers a series of web-based portals and other tools that support information exchange, file sharing and chat services among State & local law enforcement, emergency operations centers, 53 major urban areas, local, state or regional intelligence fusion centers, and the private sector.

- Department of Justice's (DOJ) Law Enforcement Information Sharing Program (LEISP) implements a unified Department-wide technology architecture to enable DOJ partnerships with State, local, tribal & Federal law enforcement agencies, and identifies which IT investments to support. LEISP enhances DOJ's ability to share information across jurisdictional boundaries.

- The Department of Defense (DOD) has recently designated a full time Information Sharing Executive; an initiative I intend to encourage other large agencies to follow. DOD has also continued to invest in the development of Global Information Grid (GIG). The GIG is being developed in concert with ODNI IC Enterprise Architecture (ICEA) to support all DOD, National Security, and related IC mission and functions in war and peace.

But, I freely admit that there are many areas where we need to do better. I intend to determine the highest priority areas and to devote the time, resources, and commitment to make near term and long-term improvements in these areas. Among the highest priority matters that need attention are the following: defining government-wide

standards for Sensitive but Unclassified (SBU) information handling; assisting in the development of a national strategy that defines federal collaboration with State and local fusion centers; developing an ISE budget investment strategy; deploying of initial capabilities for Electronic Directory Services (EDS); and developing guidelines to protect the privacy and other legal rights of Americans.

Sensitive But Unclassified Information Efforts

The President's Memorandum contained specific direction related to the standardization of Sensitive But Unclassified (SBU) information. Specifically, Guideline 3 required each department and agency to inventory existing SBU procedures and their underlying authorities across the Federal government, and to assess the effectiveness of these procedures and provide this inventory and assessment to the Director of National Intelligence (DNI) for transmission to the Secretary of Homeland Security and the Attorney General. Guideline 3 further charged the Secretary of Homeland Security and the Attorney General, in coordination with the Secretaries of State, Defense, and Energy, and the DNI, with submitting recommendations for the standardization of such procedures for terrorism, law enforcement, and homeland security information. In response, an interagency working group led DHS and DOJ, working with my office, initiated a significant multi-agency effort to address these issues that I believe will lead to tangible improvements in the way SBU is marked and handled.

This working group completed the initial inventory task in March 2006, and is in the process of evaluating the results. The data collection also includes responses by agencies to the Government Accountability Office's (GAO) similar request, supplemental material volunteered by agencies, and publicly available data. The working group will use the analysis of the SBU inventory as well as review of related literature, including SBU reform proposals of concerned communities of interest, recommendations of the GAO, the Congressional Research Service (CRS), and a wide range of other legal, academic and policy sources to develop recommendations for submission to the President regarding the standardization of SBU procedures by June 2006.

Preliminary assessments indicate that there are no government-wide definitions,

procedures, or training for designating information that may be SBU. Additionally, more than 60 different marking types are used across the Federal Government to identify SBU, including various designations within a single department. (It is important to note, seventeen of these markings are statutory.) Also, while different agencies may use the same marking to denote information that is to be handled as SBU, a chosen category of information is often defined differently from agency to agency, and agencies may impose different handling requirements. Some of these marking and handling procedures are not only inconsistent, but are contradictory.

Initial evaluation of the inventory data also suggests that different agencies rely on different authorities as a basis for developing marking and handling procedures. For example, some agencies rely on Freedom of Information Act (FOIA) exemptions to mark SBU information, while other agencies may apply markings to SBU data not necessarily subject to a FOIA exemption. Information characterized as SBU also can range in levels of sensitivity.

In coordination with my office, the Secretary of Homeland Security and the Attorney General will submit recommendations to the President in June on standardization of SBU procedures for terrorism, homeland security, and law enforcement information. The Guidelines also require that the DNI, in coordination with the Secretaries of State, the Treasury, Defense, Commerce, Energy, Homeland Security, Health and Human Services, and the Attorney General, and in consultation with all other heads of relevant executive departments and agencies, submit recommendations and standards applicable to all Federal controlled unclassified information by December 16, 2006. While many improvements can be achieved by Executive Branch actions alone, these recommendations may also involve recommendations for legislative changes.

The PM, in managing the development and implementation of the ISE, will closely coordinate all efforts under the President's guidelines to ensure progress, consistency, and effectiveness, and to ensure that all partners in the ISE benefit from the implementation.

State and Local Fusion Centers

State, local and tribal governments will continue to ensure that personnel responsible for protecting local communities from terrorist attacks have access to timely, credible, and actionable terrorism information. A number of State and local governments have sought to address this need for actionable information by establishing "information fusion centers." These centers coordinate the gathering, analysis and dissemination of law enforcement, public-safety and terrorism information. As I mentioned, Statewide fusion centers have been established, or are being established, in 42 states.

There is, however, no national strategy that defines federal collaboration with these centers. Each State and local fusion center has developed it own way of interfacing with the various Federal entities involved in terrorism prevention and response efforts. Additionally, fusion centers rely on multiple channels to exchange terrorism information with the various Federal entities involved in investigatory, prevention, response, and recovery activities. It is one of my highest priorities to greatly improve this situation.

I strongly support the concept of fusion centers and I expect these centers to become critical components of our national capability to gather, analyze, and disseminate actionable information. State and local fusion centers across the nation should achieve a baseline level of capability. The Department of Justice Global Justice Information Sharing Initiative/Department of Homeland Security Advisory Council "Fusion Center Guidelines" were developed with Federal funds and through a collaborative process involving Federal, State, and local officials and may provide this useful baseline. I intend to help the collaborative process move forward by working with DHS, DOJ, DoD and others to develop an integrated Federal approach that describes how the various Federal entities (law enforcement, homeland security, defense) can interface with state and local Fusion Centers.

Guideline 2 of the President's Memorandum requires the Secretary of Homeland Security and the Attorney General, in consultation with the Secretaries of State, Defense, and Health and Human Services, and the DNI (which includes the Program Manager), to perform a comprehensive review of the authorities and responsibilities of executive departments and agencies regarding information sharing and to submit to the President a

recommended framework for sharing information between and among executive departments and agencies and State, local, and tribal governments, law enforcement agencies and the private sector. This framework is to be submitted to the President through the Assistant to the President for Homeland Security-Counter Terrorism and the Assistant to the President for National Security in June 2006.

ISE Budget

In March of this year, OMB issued a budget data request (BDR) in support of the Information Sharing Environment. This request provided to my office information on the inventory of systems, programs and architectures that support terrorism information sharing. The BDR requested corresponding FY06 and FY07 budget information for those systems, programs, and architectures.

My office will use this data to develop an investment strategy for the ISE to shape future budget decisions through the identification of gaps and opportunities to better enable terrorism information sharing. Such mechanisms could include system modification and/or enhancement, as appropriate; new investments and acquisitions; and strategic leveraging of existing programmatic resources.

Electronic Directory Services (EDS)

On March 31, 2006, we released the initial capability for the ISE electronic directory services (EDS) within a classified environment – something that has not existed before. The approach to EDS is incremental, starting first at the federal level to provide directory services information within a classified environment; and then eventually creating the capability at the SBU level. This first delivery of the EDS provides contact information for Counterterrorism related watch centers, and is similar to a telephone book's "Blue Pages" listing. These Blue Pages are available to anyone who has access to the Sensitive Compartmented Information (SCI) and SECRET security domains. The Blue Pages reflect agreements and cooperation among the Information Sharing Council members; in particular, the Office of the Director of National Intelligence (ODNI), who

is hosting the Blue Pages in the SCI security domain, and the Department of Homeland Security (DHS), who is hosting the SECRET security domain Blue Pages.

My staff has a strong sense of urgency to deliver full EDS-People and Organization (EDS-PO) capabilities defined as a set of registries that share a common, trusted, and up-to-date view of people and organization information, which includes identification of necessary attributes and standardized metadata on people and organizations, to assist in locating people and resources with relevant knowledge about intelligence and terrorism information. Current efforts are focused on White and Yellow Pages and are defined below:

- *White Pages Concept* - Name, personal attributes and at least one method of contact for named personnel. Additional contact information may include phone numbers, email addresses and postal addresses. For urgent needs, an alternate 24/7 method of contact may be included. Attributes may include such information as skill set, clearance level and areas of expertise. For certain users, some attributes may not be viewable or searchable.

- *Yellow Pages Concept* - Organization and contact information, which may include description of roles and responsibilities and organization charts. For urgent needs, an alternate 24/7 method of contact will be included. These may include a pointer to the organization directory. For certain users, some organization attributes may not be viewable or searchable.

The EDS-PO Implementation Plan developed in February 2006 calls for implementing the Blue Pages on the Sensitive But Unclassified (SBU) domain by end of July 2006. Due to lack of cohesive and centralized governance structure of the SBU domain, the solution for SBU Blue Pages is more complex than the SCI or SECRET domains. As a result, the SBU Blue Pages data will be a subset of that available on the SCI and SECRET Blue Pages.

By the end of October 2006 we plan to increase existing ODNI White Page capability at the SCI and SECRET domains to include non-IC information. Also planned

for October 2006 is the initial iteration of Yellow Pages at the SCI and SECRET domains. Currently, the implementation team is working with the Departments and Agencies to identify the cost of making appropriate content available to the right users.

Guiding Principles

Creating a culture of information sharing within the various departments and agencies of government will require us to assign dedicated personnel and resources; reduce disincentives to sharing; and to hold our senior managers and officials accountable for improved and increased sharing of information. And it will require a great deal more. I have established the following principles to guide the efforts of each of the entities engaged in developing the ISE.

- We will deploy a decentralized, distributed and coordinated model so that the handling of terrorism information in the ISE will take place directly among users, using a web-enabled, network model accessible to each of the stakeholders in information sharing.

- We are working to develop and use common standards and best practices to promote maximum distribution and access to terrorism information, including the appropriate method for government-wide adoption and implementation of these standards.

- We will deploy the ISE on the premise of information "access" by using the concept of "shared information space". In this model, information is a community asset—not the property of a particular agency. We will ensure security and privacy safeguards are in place to protect sources and methods while ensuring the privacy and other legal rights of Americans are protected.

- We will operate on the basis of "risk management" not "risk avoidance" to balance the risk of inappropriate disclosure of information against the risks associated with inadequate information sharing. This is the approach used now

within most departments and agencies, and it should be used within the ISE.

- I want to build trust through auditing, performance evaluation, accountability and transparency. Achieving that end will require significant training and education as well as strict enforcement of policies and processes relating to the handling of information that is shared.

- Finally, we are striving to facilitate easier user access to terrorism information for users faced with a wide variety of systems and tools and by different policies, procedures and access controls. I want to simplify ISE access for users regardless of their point of entry into the environment through the deployment of open standards and technologies and appropriate policies related to user access.

I want to thank the Members of this committee for your continued support and dedication to this important issue and look forward to working with you on building an enduring capability for information sharing for this Nation. I welcome and look forward to your questions.