Written Testimony of Thomas E. McNamara
Committee on Homeland Security and Governmental Affairs
Wednesday, October 12, 2011
Dirksen Senate Office Building – SD 342

I am Thomas McNamara and from early 2006 until mid 2009 I served as the Presidentially-appointed Program Manager (PM) for the Information Sharing Environment (ISE). This position is administratively located in the Office of the Director of National Intelligence (ODNI), but its statutory authorities and mission extend beyond the Intelligence Community to the entire federal government, and include responsibilities for information sharing with state, local, tribal, and foreign governments, and the private sector – i.e. the ISE Stakeholders. It is again a pleasure to testify before this committee. During my 3 1/2 years as PM, I had the pleasure to work closely with its members and staff, from whom I received encouragement, constructive criticism, and strong bipartisan support. For that, I thank the committee and especially the Chair and the Ranking Member.

Congress established the PM-ISE specifically to address deficiencies identified by both the 9-11 and WMD commissions. It mandated the creation of an ISE to ensure that those responsible for protecting our nation from future terrorist attacks have access to the information they need to be effective. Hence, I directed very intense, broad efforts to design, create, and develop sharing among ISE stakeholders.

I will not redundantly describe the ISE or the PM's Office to this committee. For others reading this statement, let me note for the record that the ISE has been built with the objective of sharing the right information with the right individuals at the right time throughout the government structures of the nation. This can only happen through balanced ISE access and control methodologies and technologies, which are well known, and already widely used in the private sector.

Two years ago in my final appearance before this committee as the Program Manager, I stated that we had built a strong foundation for the ISE, but that a fully functional, mature ISE was still a desideratum. I am delighted to observe two years later that the ISE has gone well beyond that point.

A truly mature and functioning ISE can only exist when we have fully rationalized, standardized, and harmonized rules, procedures, and operating systems to manage the ISE. To get from the start point to that fully mature system is -- we now know -- a long, complex, and difficult process. Today, ten year after 9/11 and five after I sent the required Program Manager's Implementation Plan to the Congress, we are, well beyond the foundation, but we are not near the finish.

What I find most encouraging in the last two years is that the pace and breadth of change are stronger and more widespread among all stakeholders. Concepts and programs that were hard-fought struggles in those first years are accepted as conventional wisdom, now. CUI, to cite one example, was met with widespread skepticism and open opposition, when in 2006 we set the goals and began building the CUI structure. Today, CUI is a fully accepted tool of information management in the federal government, and is championed enthusiastically by state and local governments. CUI problems lie in refining the structure, getting resources to transition to CUI from the SBU markings, and solving new problems that occur because CUI is up and running. I know of no agency, now, that opposes CUI, or believes the old way was better. From my perspective, that is huge progress. Even these new problems demonstrate progress.

At the macro level, my observation is that the ISE is alive, well, and growing stronger. There are many cases of agency resistance to change in particular circumstances, and there are significant systemic problems, only some related to inadequate resources. There is not, however, the pervasive resistance to change that we faced five years ago. We had to spend much time getting "buy-in" from stakeholders who were skeptical or hostile about spending resources on the ISE. This is normal in large bureaucratic organizations, which, like a supertanker, change direction slowly at first. When the ship finally swings, however, it keeps swinging and the job of the captain is to direct the energy and the attention to stay on the desired course. At the macro level, I believe current plans and strategy are sound for reaching our goal of a mature ISE. I believe we are on course.

At the micro level, however, we have not finished creating all the standardized and harmonized rules, procedures, and operating systems that we need. The incomplete standardization and harmonization are the central problems of today. To get all the energy focused on achieving the desired outcome, is not easy. Different agencies and levels of government have different priorities, different resource constraints, and different levels of capability. Also, growing the ISE causes it to "bump" into other programs and priorities, which are out of step with the ISE and/or have conflicting priorities. In short, a growing ISE interferes with other big "rice bowls."

Managing and coordinating, when such differences exist, has it own difficulties. I know the committee has examined Wikileaks, and I do not intend to focus on it here. The Wikileaks disaster, however, makes this point emphatically. Two agencies – neither opposed to sharing information, and both trying to implement ISE goals and objectives -- had non-standard, non-harmonized ways of managing the same information. Also, policies and rules for information sharing lost out to a higher priority program, viz. giving the "war fighter" whatever data the war fighter might conceivably need.

Had there been standardized and harmonized rules, both agencies would have known how information is properly managed, would have managed it that way, and been confident that the other was managing it properly. Viewed in this way, Wikileaks is evidence of growing pains in the ISE. It was a huge mistake, but one that a developed and mature ISE can prevent. Indeed, the President's Eexcutive Oorder (EO) of last Friday mandates actions to avoid this and other growing pains. This EO is a big step in the right direction.

I take it, also, as a proof of the changed attitudes about information sharing, that there was no hue and cry to end information sharing or to close the Program Manager's office following Wikileaks. I dare say, had Wikileaks occurred in 5 years ago, the ISE would have been stopped in it tracks. As this committee knows, there were efforts to shut down PM-ISE while I was PM and, thanks to this committee, they were unsuccessful.

What has happened, I believe, is a transformation of attitudes. We have all seen the absolute necessity of managing information in the new information age, using policies and procedures that respond to the needs of the new age. We may pine for the "good old days," but we can never go back to them. There is simply too much information and too many organizations and individuals requiring information to think government can function properly without an ISE. The rest of our society has moved with alacrity into this new information-sharing world. Government must follow.

Let me list what I consider the major accomplishments, thus far, in building the ISE from its very inauspicious beginnings. All but one item on my list was non-existent, even in concept, in 2001. Only a few things on this list were nascent in 2006, either struggling to gain acceptance, or to prove themselves. Everything on this list is a functioning program today, providing improved security to the nation at every level of government.

- **National Network of Fusion Centers:** The concept of fusion centers predates 9/11, but the nationwide drive and investments in them by federal, state and local governments grew exponentially after that tragedy. Today, this "central nervous system" of the ISE is a true national network whose full potential is being realized. It is one of many examples in the ISE of the federal system working well. The task before us is to ensure fusion centers are not focused only on terrorism, but have a true mandate for all crimes, all hazards. We also need to foster better cooperation, collocation, and some forms of integration of fusion centers with other similar centers (e.g. JTTFs and HIDTAs) to create a truly national asset for all law enforcement and all first responders. There is no good reason why this cannot and should not be done.

- **Controlled Unclassified Information (CUI):** I have already spoken of this. CUI is a huge task because the amount of CUI is orders of magnitude larger and more complex than classified information, and is widespread in every agency of federal, state, and local government.

- **Suspicious Activity Reporting (SAR):** When the Program Manager took on the task of making a useful tool out of a nationwide blizzard of local police reports (SARs); others had already failed in the effort. The difference was the PM had people with federal and local police experience who thought outside the box. Within a year we had an implementation plan, a pilot program, and most importantly, the support and participation of major local and state police departments. It was these latter – another example of federalism -- that taught the PM/ISE how to manage SAR. Today, SARs are an extremely valuable tool at all levels of law enforcement.

- **National Information Exchange Model (NIEM):** The unsung hero of the ISE is the NIEM, which provides the technical foundation for ISE information exchanges around the country. From its modest beginnings in the Department of Justice in 2005, it has expanded with the strong support from PM/ISE through all levels of government, the private sector, and in the future, internationally among our allies and partners. It is the engine on which the ISE exchanges information. It too functions for non-terrorism information.

- **Privacy Rights and Civil Liberties (PR/CL)**: As NIEM is the technical foundation, so PR/CL Guidelines provide a policy foundation for a successful ISE. It has always been, and remains, job one of the Program Manager to formulate, propagate, and ensure PR/CL rules are observed by all ISE users. The past five years have produced a viable, replicable methodology to monitor and oversee the PR/CL policies, so essential for public acceptance and support of the ISE. Of all the things I took pride in as PM, the PR/CL program was at the top of the list. Without it, support for the ISE will wither and die. It has been so well constructed that it, also, is a valuable template for non-terrorism information.

There is also a list of the highest priorities remaining to move the ISE to the next higher, more effective, more secure level. Here are, in my opinion, some of the major problems, which need attention:

- **Monitoring and Auditing:** The ISE was never envisaged to give access to information until control mechanisms are adequate to ensure that only the right information flows to the right people at the right time. Such controls are accomplished, as mentioned above, through standardized rules, procedures, and operations. This must include programs for adequate monitoring and immutable auditing -- the information assurance function. In these areas the ISE has not reached the levels necessary for a fully functioning environment. The priorities, the attention, and the resources for these functions remain inadequate. In a huge bureaucracy, including federal, state, and local government, the challenges are formidable. But, the ISE will ultimately fail unless these critical functions are developed and implemented. I was pleased to see these areas included in last Friday's EO to protect against the "insider threat." That is another step in the right direction.

- **Discovery and Authorized Use:** Closely related to the above are two functions that are the most difficult and complex to implement, and yet are certainly indicative of a fully developed, mature ISE. In a sense "discovery" or "discoverability" is no more than a better variant of the "tear-line" approach in the old information system. Individuals can "discover" if information exists on a subject, even when they are not authorized to see it. Authorized use (also called ICA - Identity authentication/Credentialing/Access) allows a person to be recognized and authorized to use the ISE for the purpose and role attached to that individual. The beginnings of this function can be seen in several communities (e.g. law enforcement, intelligence, homeland security), but not for all users, and not across systems and agencies at all levels of government. Nevertheless, the startup of these two essential functions is progress, and I hope that the progress will continue and result in a true cross-government system of "authorized use" or ICA.

- **Interoperability across Networks:** With the security of the ISE assured through effective monitoring and auditing, and the identity of all users pinpointed through an effective authorized use function, greater interoperability across networks at given security levels is possible. This function is less complicated that those I mentioned above, but its use in the ISE will be possible only to the extent that the other functions are put in place.

- **Expanding the Mandate:** Finally, I take this opportunity to point out, again, to this committee and the Congress an anomaly in building the ISE. The legislative mandate for the PM is to build the ISE for "terrorism-related" information only. The above functions demonstrate that they transcend the "terrorism-related" mandate. Although the Program Manager only has authority for managing terrorism information, no agency partitions off terrorism information from its overall information management systems for all classified or CUI information. This is why, as Program Manager, I insisted that the ISE functions be designed to apply in an information management system for all classified and CUI information. That reflects my conviction that it is impossible, and undesirable, to create a "Terrorism-only" ISE. The mission is to create a broad-based ISE. The mandate and authorities should reflect that mission. Last Friday's EO took a

small step in that direction. It is, however, more than time for that expanded mandate to be created.

Let me close by summing up what I think can be the future of the ISE. Two years ago in saying we had built the foundation, I used a Churchillian turn of phrase: that we were not at the beginning of the end, but at the end of the beginning. When I look back now, I can see that we are well beyond the end of the beginning. But, when I turn around and look forward, I can see that we still have a long way to go to get to the beginning of the end. We are, however, moving faster, more efficiently, in the right direction.

I estimate that today we are at the half-way point. Since we are moving faster, I expect that we need less than five more years to reach that goal we set five years ago – a fully developed, fully mature ISE. With the support of the Congress and the White House, and continued focus on raising the ISE to higher levels, we can get the job done.

We must get the job done. The 9/11 and WMD commissions were correct, faulty information sharing was a major cause of that tragedy. Long before 9/11 and since, almost every failure to spot and stop attacks on the homeland shows that defects in information sharing were part of the problem. Every success, then and now, has shown that information sharing can make our job easier and more successful. We owe it to the nation to speed the process, stay the course, and achieve the goal.

Thank you, and I will be pleased to try to answer any questions you may have.