Written Testimony of Thomas E. McNamara
Committee on Homeland Security and Governmental Affairs
Thursday, March 10, 2011
Dirksen Senate Office Building – SD 342

I am Thomas McNamara and from early 2006 until late 2009 I served as the Presidentially appointed Program Manager for the Information Sharing Environment, which position was administratively located in the Office of the Director of National Intelligence, but whose statutory authorities and mission extend beyond the Intelligence Community to the entire federal government. It is again a pleasure to testify before this committee. During my years as Program Manager, I had nothing but understanding, encouragement, and bipartisan support from the committee. For that, I thank the committee and especially the Chair and the Ranking Member.

During that time, I directed a very broad effort to design, create, and develop the sharing of terrorism-related information among Federal, State, local, tribal and foreign governments, and with the private sector. Congress established the PM-ISE specifically to address deficiencies identified by both the 9-11 and WMD commissions by mandating the creation of an Information Sharing Environment (ISE) to ensure that those responsible for protecting our nation from future terrorist attacks have the information they need to be effective.

I need not, and will not, go into detail here to redundantly describe the ISE or the Program Manager's Office to this committee. For those few others who might read this statement, let me note for the record that the Information Sharing Environment (ISE) has been built with the objective of sharing the right information with the right individuals at the right time. This can only happen through balanced ISE access and control mechanisms, which are well known, and already widely used in the private sector.

In my last appearance before this committee, I noted that we had built a strong foundation for the ISE, but that a fully functional and mature ISE was still a desideratum. The Wikileaks disaster is an unfortunate confirmation of the truth of that evaluation. Let me try to convey my understanding of the circumstances that gave rise to the Wikileaks disaster. I base these observations entirely on unclassified sources, having had no access to classified information regarding Wikileaks, or of any events, since my departure from government service in 2009.

First, a truly mature and fully functioning ISE can only occur when we establish rationalized, standardized, and harmonized rules, procedures, and operating systems, without which we cannot manage the ISE. To get from the start point in 2005 to that fully mature system is a long, complex, and difficult process. We are, I believe, well along the path, but we have not, by any means, reached our goal. The foundation is there, and the goal was articulated in the 2006 Implementation Plan, and the 2007 National Strategy for Information Sharing Environment. As we progress in our endeavor, we need to modify and update those documents to refine and clarify our understanding of that goal.

We have rational plans and a strategy in those documents for reaching our goal of a mature ISE. But, we have not finished creating the standardized and harmonized rules, procedures, and operating systems that we need. That incomplete standardization and harmonization are the reasons for the Wikileaks disaster. The case is one where two agencies had two different ideas of how to manage the same information. Had there been standardized and harmonized rules, both agencies would have known how this information should be managed, and had confidence that the other was managing it properly. In this post-1990s information world, the government no longer has the option of letting each agency manage, as it wishes, the information of which it is a custodian (not an owner). Managing information in the 21st Century is a common enterprise.

Here are, in my opinion, some of the major ISE-related problems that allowed Wikileaks to occur. [I will cite one fundamental, non-ISE-related problem at the end of my remarks.]

1. The ISE was never envisaged to give very broad access to information in systems where control mechanisms are inadequate 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, including adequate auditing and monitoring, and some form of authorized-use. Unfortunately, they were not in place on SIPRNet. SIPRNet tends to have very restrictive controls in place for non-DoD personnel, but allows wide-ranging, non-job-related access to information for hundreds of thousands of Defense Department employees. Two misconceptions that plague many agencies' thinking about information sharing are apparent in DoD's management of SIPRNet. The first is that an agency's own cleared employees are more reliable and need fewer restrictions than another agency's cleared employees. The second is that an agency's "own information" is more tightly controlled than other agencies' information.

2. In the aftermath of the Afghanistan and Iraq invasions, a very high priority was placed in DoD on getting to the "war fighters" all the information they might need to get their jobs done – i.e. to fight the wars. This necessary and laudable objective relied on SIPRNet as the main network for moving secret information to war fighters in combat zones. The effectiveness of SIPRNet controls diminished, *inter alia*, because of the reduced capabilities for auditing and monitoring SIPRNet in the Iraq and Afghanistan theaters of operations. The priority of getting information to the war fighters was the justification for the relaxation of rules. One of the mistakes in the SIPRNet control system in combat zones is that large volumes of information transfers – i.e. "mass data downloads" – were permitted so that information could rapidly move to the war fighters, even without auditing and monitoring capabilities, which would have been used in a fully developed Information Sharing Environment.

3. In recent years government and private industry have placed increasingly stronger restrictions on the transfer of data to portable storage devices (e.g. thumb drives, disks, PDAs). Most controlled systems prohibit using uncontrolled portable storage devices to move data within and between information systems. Within SIPRNet these controls were not in place, or not used, in Iraq and Afghanistan, thus, allowing the transfer of classified information to unclassified systems with little or no auditing, or monitoring of the transfers.

These three problems are three lessons to learn from the major WikiLeak affairs of the past year (the Afghanistan messages; the Iraq messages; and the State Department messages). The information sharing environment cannot survive without fixing these failures by establishing rationalized, standardized, and harmonized rules, procedures, and operating systems across the federal government.

WikiLeaks is a case of information sharing outrunning the system used to manage the shared information. The statement, "there can be no sharing without security," is as true today as it was the day I began as Program Manager. Successful information sharing involves not only the sharing, but also the secure management of the information and the environment in which information is flowing. Much of the misunderstanding of the ISE, and of failures such as the WikiLeaks, comes from sharing when the systems cannot manage the volume and sensitivity of the information.

It has been a constant theme of mine, and others who `build the ISE, that two groups of stakeholders in the ISE must be satisfied. The first is the participants, the information users. They will not use the ISE unless they have confidence that the system will properly control and protect the information that they put into it. The second is the non-participants, i.e. mainly the American public, and others who have a major stake in the proper functioning of the ISE. They will oppose any ISE that cannot control and protect the privacy of information that pertains to them. The confidence and comfort of both groups must be satisfied, or the ISE will not succeed.

While attention is on the WikiLeaks affair, I want to point out that these problems are not just problems for classified information, i.e. for sensitive national security information. An even greater volume of sensitive information is unrelated to national security, and therefore, cannot be classified. I refer here to the huge category called Controlled Unclassified Information (CUI). This category requires its own rationalized, standardized, and harmonized controls because it concerns law enforcement, judicial, private-sector proprietary, personal, and much other sensitive information.

It is not hard to imagine an individual with access to CUI information downloading and releasing large quantities of data about, for example, grand jury deliberations, or organized crime investigations by local, state or federal law enforcement. Indeed, there is much CUI contained in the WikiLeaks documents. Hence, very early on, as Program Manager, I zeroed in on the chaotic state of sensitive but unclassified (SBU) information. We created CUI as a rationalized, standardized, and harmonized method within the ISE for managing this information across the federal government. We, also, made it adaptable for use by state and local governments. This CUI management is an essential part of the ISE, and is coordinated by the National Archives and Records Administration with oversight and assistance by the Program Manager's Office. It is another part of building a fully functional and mature ISE.

I want to take this opportunity to point out, again, to this committee and the Congress an anomaly in the building of the ISE. The legislative mandate for the Program Manager is to build the ISE for "terrorism-related" information only. We can all see that most of the documents in the WikiLeaks were not terrorism-related. Therefore, they were not documents that came under the ISE manadate. Although the Program Manager only has authority for managing terrorism information, no agency partitions off terrorism information from its overall management of all classified or CUI information.

This is why, when I served as Program Manager, I deliberately designed the ISE so that it could serve as an information management system for all classified and all CUI information. That reflects my conviction that it is impossible, and undesirable, to create a "Terrorism-only" ISE. The mission, therefore, is to create a comprehensive ISE, and the mandate and authorities should reflect that mission.

To correct this anomaly, I urge this committee and the Congress, in consultation with the executive branch, to examine this and consider expanding the authority of the Program Manager, or creating a National Executive for Information Management. Such a change will increase the ability of the senior information management official truly to manage all aspects of the ISE.

Nevertheless, when the Departments of State and Defense agreed on the arrangements for DoD access through SIPRNet to State's classified cable traffic, there was no role for, and no consultation with, the Program Manager's office. The practice was that interagency arrangements were the sole purview of the involved agencies. Thus, whatever benefits the experts in the Office of the Program Manager might have added were lost. I do not know if this would have changed the outcome; I simply note that no consultation took placed.

I will conclude with two points. First, it is a measure of the very profound changes of attitudes in government regarding information sharing that no one has called for an end to information sharing because of the WikiLeaks. Had WikiLeaks happened 4-5 years ago, there would have been numerous calls to close the ISE and the Program Manager's office. In fact, as this committee is aware of, even without WikiLeaks, there were such calls back then.

What has happened, I believe, is that 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.

Finally, we need to recognize that at its base the WikiLeaks affair was not a new phenomenon. It was in fact a very traditional espionage affair, which used new tools for the espionage. The parallels with other traditional espionage disasters of the past two decades are many. One example is the John Hanson espionage affair. That was also a case of document theft by a cleared, trusted individual, who turned over hard copies (instead of digital copies). Hanson's criminal acts over many years were similar to the criminal acts of the thief who stole and handed over to WikiLeaks CDs and thumb drives full of sensitive information. In both cases, the acts were meant to undermine the nation's security and weaken our society, even if it meant that people's lives were at risk, and some would be killed.

My point in raising this is to say that, even without the ISE, we had a John Hanson. And, with an ISE, we had a WikiLeaks traitor. As long as trusted individuals debase themselves and betray our trust, there will be Hansons and WikiLeaks. The fully functional and mature ISE, which I have referred to here, is a necessity in this new information age because it is an essential part of our efforts to prevent or limit these disasters in a future, where computerized data flows are the norm, and where human treachery will always be a possibility.