Statement for the Record

Beyond ISE Implementation: Exploring the Way Forward for Information Sharing

for the

House Committee on Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment

July 30 2009

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA

Ambassador Thomas E. McNamara

Program Manager
Information Sharing Environment

Testimony
Before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Committee on Homeland Security, U.S. House of Representatives

Beyond ISE Implementation: Exploring the Way Forward for Information Sharing

July 30, 2009

Statement of Ambassador Thomas E. McNamara
Program Manager,
Information Sharing Environment

Madam Chairman, Ranking Member McCaul, and Members of the Subcommittee.

Let me begin by thanking this Subcommittee and the entire Committee for your continued support of our efforts to build the Information Sharing Environment (ISE) over the last four years. This subcommittee has been a real champion of information sharing, and the ISE in particular. I especially want to thank you, Madam Chairman, for your tireless advocacy of our efforts. Such initiatives as the Interagency Threat Assessment and Coordination Group and the Controlled Unclassified Information framework would not be where they are today without your personal leadership. As you know, I will be stepping down as Program Manager at the end of this month, and I appreciate this last opportunity to update the Subcommittee on progress made in implementing the ISE and the challenges that still remain almost eight years after the terrible events of September 11, 2001.

INTRODUCTION

Since I assumed the position of PM-ISE in March of 2006, I have worked to ensure that ISE implementation is consistent with our vision of the ISE as "a trusted partnership between all levels of government in the United States, the private sector, and our foreign partners." Time and again, we have demonstrated that when the Executive Branch and the Congress work collaboratively to share information with State or local agencies and *vice versa*, the results exceed all expectations. As the Chair has so eloquently stated,

> While we want police and sheriffs officers nationwide to keep their communities safe from the traditional "bad guys", don't we also want them to know about potential terrorists in their midst who mean us harm? That's what "homeland security intelligence" is all about: getting accurate, actionable, and timely information to the officers in our hometowns so they know who and what to look for in order to prevent the next 9/11.

The context for my testimony is the third Annual Report on the ISE which was forwarded to the Congress on June 30. Although devoting considerable attention to a description of progress made since June 2008 and plans for the next year, the report goes beyond what the Congress directed to be covered in the ISE Annual Reports in two important ways:

- First of all, the report includes a three year retrospective on the ISE summarizing what was originally intended, what has already been accomplished, and what remains to be done; and
- Secondly, it introduces a management construct called the ISE Framework, which, while building on the work already done, represents a new approach for managing ISE implementation activities. The Framework—comprising a set of

goals, sub-goals, outcomes, objectives, and activities—is the follow-on to the three-year ISE Implementation Plan for the next phase of ISE implementation.

Copies of the full report, containing much more detail on these and other important ISE initiatives, have been provided to the subcommittee. In the interest of keeping my formal statement brief I have intentionally kept my remarks at the summary level. For a more detailed description, I direct the Subcommittee's attention to the full report and respectfully request that it be made part of the record of this hearing.

In the past three years we have created a functioning—but still evolving—ISE that has strengthened our national security by ensuring that much more of the right information gets to the right people at the right time to counter threats to our people and institutions. Despite these accomplishments, the task is far from finished. Formidable cultural and policy hurdles still remain as we conclude the foundational phase and begin a new implementation phase, under the new Administration.

Our goal remains an ISE that shares all information securely and properly among all ISE participants. This requires developing mostly common policies, business processes, and technologies, something that is neither easily nor quickly achieved. Our persistent, cooperative efforts have, however, established a solid foundation of compatible policies and practices, which must continue to evolve for several years to create a fully functional ISE.

Having no template to pattern our efforts on, we invented and designed this foundation—using a general methodology that is apparent throughout the report—to rationalize, simplify, and harmonize existing policies, practices, and technologies drawn from all of our participating agencies and organizations. Indeed, this is our legislative mandate.

The Controlled Unclassified Information (CUI) framework; the Suspicious Activity Reporting (SAR) initiative; expanded access to classified information by State and urban area fusion centers; an enterprise architecture framework for the ISE; a common information sharing standards program; and comprehensive privacy and civil liberties guidelines are examples of the foundations we have built and the methodology we have developed to allow for secure and proper information sharing among our participating agencies at all levels of government.

Before I move on to the detailed portion of my statement, I would like to make one important point. The 9/11 Commission reported its findings at a time when the American people were acutely aware of the urgency of finding out what went wrong and eager to know that their leaders were taking steps to ensure that our nation would not fall victim to attack for the same reasons. It was in this context that the Congress called for an ISE.

While we have been fortunate to have not suffered another major attack since 2001, the sense of urgency that brought the ISE into being should be no less now than it was then. I hope that this report will help ensure that the work of the PM-ISE and of our partners at all levels of government and in the private sector will continue to move forward with speed and diligence so that we can continue to use our collective resources wisely to keep our nation safe from attack, while continuing to protect and defend our privacy and civil liberties.

CONTINUED IMPORTANCE OF INFORMATION SHARING

This Administration is firmly committed to developing the ISE as envisioned in IRTPA. In a memorandum to Federal agencies, President Obama emphasized that "The global nature of the threats facing the United States requires that our Nation's entire network of defenders be able rapidly to share…information so that those who must act have the information they need." Moreover, the Administration's Homeland Security agenda depends heavily on increasing our capacity to share information across all levels of government.[1] This strategy was reaffirmed by Secretary Napolitano at the National Fusion Center Conference in March 2009:

> At the Department of Homeland Security, information and intelligence sharing is a top priority and fusion centers play an important role in helping to make that happen, … In the world we live in today, it's critical for Federal, State, local and tribal entities to know what the others are doing so each can operate effectively and efficiently. Protecting our country requires a partnership of Federal, State and local resources that are fully integrated to not only gather and analyze information, but then to swiftly share that information with appropriate agencies.[2]

This Annual Report, therefore, should be seen as both an update to the Congress on progress made in designing and implementing the ISE, and as a part of this Administration's broader effort to improve the way the government manages information. In the words of the President, we need to "make sure our government is running in the most secure, open, and efficient way possible."[3]

On July 2nd 2009 Mr. John Brennan, Assistant to the President for Homeland Security and Counterterrorism issued the memorandum 'Strengthening Information Sharing and Access' to heads of Cabinet Agencies and notified Congress of the continued effort to review information sharing issues and prioritize the ISE at a senior level at the White House. This memorandum also included streamlining the interagency policy process by merging the Information Sharing Council called for in IRTPA Sec 1016 with the Information Sharing and Access Interagency Policy Committee at the White House.

[1] See http://www.whitehouse.gov/agenda/homeland_security/.

[2] Remarks by Homeland Security Secretary Janet Napolitano to the National Fusion Center Conference, Kansas City, MO (March 11, 2009), available at http://www.dhs.gov/ynews/speeches/sp_1236975404263.shtm.

[3] White House Press release, "President Obama Names Vivek Kundra Chief Information Officer" (March 5, 2009).

THE ISE FRAMEWORK

The ISE Implementation Plan was designed to guide the ISE through June 2009. Many of the Plan's 89 actions have been completed—albeit some of them in modified form; others have been changed by the NSIS or subsequent policy direction. It is time, therefore, to close the book on the ISE Implementation Plan actions and adopt a modified approach that will help guide and manage the next phase of ISE implementation. The ISE Framework, while building on the work already done, is a new approach that will drive all future ISE implementation activities. The Framework creates critical linkages between four primary and enduring ISE goals, fourteen sub-goals, and a resulting set of outcomes, objectives, products, activities, and associated performance measures. It provides a common understanding of the problems to be solved, the essential capabilities that constitute the ISE, and the actions needed to ensure that these capabilities are developed and deployed in a manner "consistent with national security and with applicable legal standards relating to privacy and civil liberties."[4]

In June 2008, the Government Accountability Office (GAO) issued a report on "actions taken to guide the design and implementation of the ISE" and "efforts that have been made to report on progress in implementing the ISE."[5] While acknowledging the progress made since 2005, the report concluded that "specific desired outcomes or results should be conceptualized and defined in the planning process … along with the appropriate projects needed to achieve those results, supporting resources, stakeholder responsibilities, and milestones." In addition to serving as the successor to the ISE Implementation plan, the ISE Framework responds directly to the recommendations by the GAO. It represents an evolutionary approach that builds on previous ISE implementation management efforts and ties individual ISE products and activities directly to specific objectives, outcomes, sub-goals, and goals, as called for in the GAO report.

SUMMARY OF 2008-09 PROGRESS

The Third Annual Report to the Congress on the Information Sharing Environment responds to the requirement in the *Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)*, as amended, for "a progress report on the extent to which the ISE has been implemented." It reflects the collective accomplishments and challenges of an information sharing partnership between the PM-ISE and a range of Federal and non-Federal partners committed to the continuous improvement of information sharing

[4] IRTPA (as amended), §1016(b)(1)(A).

[5] Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress, GAO-08-492, (June 2008).

practices with the overriding goal of increasing our national security while protecting privacy and civil liberties.

The report organizes its discussion of progress and plans around the four goals—*Create a Culture of Sharing; Reduce Barriers to Sharing; Improve Sharing Practice with Federal, State, Local, and Tribal Partners*; and *Institutionalize Sharing*—that form the top level of the ISE Framework .These four goals, in turn, drive the creation of more specific sub-goals, outcomes, objectives, and performance measures that will shape the plans and activities of the ISE over the coming years.

GOAL 1: CREATE A CULTURE OF SHARING

Appraisals, Training, and Incentives

Fostering a culture of sharing is a mandate of both IRTPA and the 2005 Presidential Information Sharing Guidelines and Requirements. It is a long-term effort to change government business practices in the interest of more effective and efficient information sharing among agencies. To accomplish this goal, in 2008-09:

- The Office of Personnel Management (OPM) and the PMI-ISE partnered to produce policy guidance that directed agencies to make information sharing a factor in Federal employees' performance appraisals. This issuance guides agencies in how to develop competency elements regarding the proper sharing of information for use in employee appraisals.
- The PM-ISE released an ISE Core Awareness Training Module to help move Federal agencies from the traditional "need to know" culture to one based on a "responsibility to provide."[6] The Module provides Federal agencies with a common tool for developing an understanding of the ISE as well as an overview of the Federal Government's counterterrorism and homeland security organizations, systems, and challenges.
- Three-quarters of Federal ISE agencies have now incorporated information sharing into their awards programs. For example, the Department of Defense Chief Information Officer established annual awards that include "information sharing and data management" among criteria for consideration.

[6] See http://www.ise.gov/docs/Fact_Sheet_ISE_Core_Awareness_Training_FINAL__(07Aug08).pdf.

GOAL 2: REDUCE BARRIERS TO SHARING

Integrated Security Framework

The PM-ISE—working with the Department of Homeland Security (DHS), the Information Security Oversight Office of the National Archives and Records Administration (NARA), the National Security Council, and other key stakeholders—has begun improving access and management of classified information shared with State, local, and tribal (SLT) and private sector partners by replacing inconsistent policies and processes with a common set of security rules and procedures for handling and safeguarding of classified information. In addition, a number of agencies have taken steps to improve security reciprocity practices. To cite two examples,

- The Director of National Intelligence issued an Intelligence Community Directive that mandates reciprocal acceptance of Information Technology (IT) systems certification and accreditation by all Intelligence Community elements; and
- DHS and the Federal Bureau of Investigation (FBI) published a joint secure space standard that provides a common solution for the installation and certification of facilities that house classified networks at fusion centers.

Uniform Marking and Handling of Controlled Unclassified Information

In May 2008, President Bush established a framework for designating, marking, safeguarding, and disseminating Controlled Unclassified Information (CUI), and named NARA as Executive Agent. A CUI Office at NARA, along with an interagency Council, manages and oversees implementation. The Office and Council, in an effort to be completed in 2009, are developing draft CUI policy guidance on: Safeguarding, Dissemination, Dispute Resolution, Marking, Designation, and Information Life Cycle. In May 2009, President Obama established an interagency Task Force led by DHS and DOJ to review work completed, and make recommendations on the way ahead.

Implementing Comprehensive Privacy Guidelines

ISE Privacy Guidelines Committee (PGC) met with privacy and civil liberties groups to listen to and incorporate new ideas into revised ISE policies and processes. The PGC also provided the guidance and tools needed to support the development of privacy and civil liberties policies to be used by Federal and SLT agencies. Specifically, the PGC:

- Published a "Privacy and Civil Liberties Implementation Workbook" to assist Federal agencies with the process of ISE privacy policy development and implementation;
- Completed an ISE Policy Development Tool, ISE Privacy Policy Outline, and a list of Publicly Available Federal Privacy Policies;

- Incorporated ISE Privacy requirements into the *Baseline Capabilities for State and Major Urban Area Fusion Centers*; and
- Provided fusion centers with a privacy policy development template and training on its proper use. The PGC also provided ongoing technical assistance and performed reviews of policy documents. To date, 30 centers have developed and submitted privacy policies.

GOAL 3: IMPROVE SHARING PRACTICES WITH FEDERAL, STATE, LOCAL, TRIBAL, AND FOREIGN PARTNERS

Recognition of the essential role of SLT and private sector partners is fundamental to the ISE and is a critical driver of information sharing in the homeland security and law enforcement communities. This was highlighted in the Executive Order governing U.S. intelligence activities, which was amended in the summer of 2008 to state that

> State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.[7]

Establishing a Nationwide Suspicious Activity Reporting Initiative

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is an outgrowth of separate but related activities that respond directly to the mandate in the National Strategy for Information Sharing (NSIS) to establish a "unified process for reporting, tracking, and accessing [SARs]" related to terrorism. The long-term goal is for Federal, State, local, tribal, and law enforcement organizations to participate in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing SARs while ensuring that privacy and civil liberties are protected.

In 2008-09, the PM-ISE and its Federal and SLT partners:

- Published an *NSI Concept of Operations (CONOPS)* that describes the NSI process; the requirements that drive it; and the roles, missions, and responsibilities of participating agencies;
- Under the leadership of the Department of Justice's (DOJ) Bureau of Justice Assistance (BJA), expanded the ISE-SAR Evaluation Environment (EE) to 12 sites, forming a solid foundation for nationwide implementation;

[7] Executive Order 13470 – further amendments to Executive Order 12333, United States Intelligence Activities (August 1, 2008).

- Fully integrated the FBI's eGuardian system into the ISE-SAR EE;
- Worked with the PGC to integrate privacy concerns into all levels of the NSI;
- Trained more than 10,000 officers and analysts in the NSI process with emphasis on protecting privacy and civil liberties; and
- Established governance to oversee and recommend how to institutionalize the NSI.

Of particular note, an ISE-SAR EE site was established at the Washington, D.C. Metropolitan Police Department (MPD) to support security before and during the Presidential Inauguration. From late December through Inauguration Day, MPD processed 88 SARs, 16 of which were forwarded to eGuardian as potentially terrorist-related.

Establish a National Network of Fusion Centers to Facilitate Sharing among State, Local, and Tribal Governments and the Private Sector

The Senior Level Interagency Advisory Group and the National Fusion Center Coordination Group provided leadership, coordination, and guidance to establish a national network of fusion centers with a baseline level capability. Highlights include:

- Publication of the *Baseline Capabilities for State and Major Urban Area Fusion Centers*. This collaborative effort, led by DHS and DOJ, included Federal and SLT agencies and provides benchmarks for assessing fusion center performance;
- Completion of a first-level assessment of 72 centers to evaluate progress against the baseline capabilities and to gather data on current fusion center funding; and
- Deployment of Federal personnel to support fusion center operations. State and local personnel have also been fully integrated into Federal operations such as the FBI's Joint Terrorism Task Forces, the DHS National Operations Center and the Interagency Threat Assessment and Coordination Group (ITACG) at the National Counterterrorism Center (NCTC).

Deployments of classified networks increased in the last year, and access is now available at more than 40 fusion centers. Also, the NCTC and its ITACG improved its Secret level online portal by increasing the number of products posted, expanding SLT awareness of the potential value to their missions, and introducing a new product line—Terrorism Information Sharing Products (TIPS)—specifically tailored to SLT needs.

GOAL 4: INSTITUTIONALIZE SHARING

Creating a Common Information Sharing Architecture

The ISE Architecture program helps align and create bridges between the diverse systems used by ISE participants to create a more uniform network of interconnected systems. Specifically,

- Version 2 of the *ISE Enterprise Architecture Framework (EAF)* provides technology and systems-wide architecture guidance across the entire ISE community;
- Version 2 of the *ISE Profile and Architecture Implementation Strategy (PAIS)* includes additional implementation guidance for ISE participants on implementing more standard processes, approaches, and techniques; and
- DOJ and DHS have incorporated the ISE EAF into their information sharing segment architectures.

Furthermore, the impact of the ISE EAF extends beyond the ISE. The Office of Management and Budget (OMB) identified the concepts developed in the ISE EAF best practice, and has incorporated them into their *Federal Segment Architecture Methodology*. In addition, other government-wide information sharing initiatives—e.g., the Federal Health Information Sharing Environment and the Maritime Domain Awareness program—have adopted many of the concepts, principles, services, and standards originally developed for the ISE EAF into their architectural developments.

Issuing Common Information Sharing Standards

During 2008-09, the PM-ISE issued a number of new or revised information sharing standards as part of the Common Terrorism Information Sharing Standards Program (CTISS). These issuances included:

- Technical Standards for Information Assurance, Core Transport, and Identity and Access Management for the ISE; and
- An updated ISE-SAR Functional Standard that clarifies implementation guidance on the NSI business process and incorporates stronger privacy protections into ISE-SAR data exchanges. Privacy and civil liberties advocacy groups provided direct input into this standard, helping to strengthen privacy controls and refine terrorism identification criteria to better safeguard First Amendment rights.

Improving the Management of the ISE

The adoption of the ISE framework and its associated maturity model provides a solid foundation for managing ISE implementation and assessing progress. The Integrated ISE Investment and Performance Process supplements the Framework with a methodology that uses performance results to drive investments and to allocate resources to the most effective programs and initiatives. In addition to strengthening internal management of the ISE, the Framework provides Executive branch and Congressional oversight bodies with a clearer picture of ISE plans and progress allowing them address issues in a timely manner.

ONGOING CHALLENGES AND PRIORITIES

These accomplishments notwithstanding, the breadth and complexity of the challenges to effective and efficient information-sharing remain formidable. Differing missions, overlapping "turf" conflicts, resource constraints, bureaucratic inertia, and agency "tunnel vision" still exist and impede information sharing among ISE participants.

Cultural change remains the most difficult hurdle of all. To bring the ISE to maturity, a number of priorities need to be addressed in collaboration with State, local, and tribal governments and our private sector partners. The following list highlights some of these priorities:

- **Institutionalize the Nationwide Suspicious Activity Reporting Initiative (NSI).** We need to institutionalize a nationwide capability to gather and share SAR information in a manner that facilitates the maintenance of national security while continuing to protect privacy rights and civil liberties.
- **Improve Support to Federal, State, Local, and Tribal Partners.** This includes: ensuring that fusion centers and other State and local agencies have access to the classified and unclassified Federal information they need; increasing the flow of fusion center information and analyses to other SLT agencies and the Federal Government; and examining long-term sustainability issues regarding State and major urban area Fusion Centers so that they operate at a baseline level of capabilities.
- **Implement the CUI Framework.** Fully implement policies and processes in accordance with the CUI Registry (to include technology and training initiatives) to support agencies' transition to the CUI Framework.
- **Protect Privacy and Civil Liberties.** Institutionalize Federal privacy policies, incorporate ISE privacy requirements in agency training, and encourage States to implement mostly common privacy policies equivalent to those of the Federal Government.
- **Reduce Improper Classification to Enhance Information Sharing.** Eliminate "need to know" requirements and protocols, and eliminate overuse of originator controls that can impede the ability to discover and share information.

- **Improve ISE Security.** Adopt common standards and processes for security clearances, identity management, and role-based access to improve controlled sharing among all ISE participants.
- **Implement Reciprocity Policies and Practices for Clearances, Systems, and Facilities.** Align Federal security policy regarding facilities, personnel, and information technology (IT) systems, and adopt the principle of security reciprocity in all Federal agencies and with SLT and private sector partners
- **Coordinate Investments for Terrorism-Related Initiatives.** Track agency budgets, reduce overlaps and gaps in funding, and monitor investments in order to drive agencies to use compatible technologies and business processes and to maximize the use of scarce resources.

THE WAY AHEAD

The progress achieved in implementing the ISE since its inception has continued to move us toward the vision set forth in the ISE Implementation Plan in 2005 of "a trusted partnership among all levels of government in the United States, the private sector, and our foreign partners." But the work is not yet done. With the adoption of the ISE Framework we now have a management structure in place that will help us not only realize the goals of the ISE as conceived in IRTPA, but will also contribute to the goal of intra- and inter-government collaboration that is integral to the Administration's Open Government Initiative.