BEYOND ISE IMPLEMENTATION: EXPLORING THE WAY FORWARD FOR INFORMATION SHARING

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

JULY 30, 2009

Serial No. 111–33

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html

U.S. GOVERNMENT PRINTING OFFICE
53–649 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

Bennie G. Thompson, Mississippi, *Chairman*

Loretta Sanchez, California
Jane Harman, California
Peter A. DeFazio, Oregon
Eleanor Holmes Norton, District of Columbia
Zoe Lofgren, California
Sheila Jackson Lee, Texas
Henry Cuellar, Texas
Christopher P. Carney, Pennsylvania
Yvette D. Clarke, New York
Laura Richardson, California
Ann Kirkpatrick, Arizona
Ben Ray Luján, New Mexico
Bill Pascrell, Jr., New Jersey
Emanuel Cleaver, Missouri
Al Green, Texas
James A. Himes, Connecticut
Mary Jo Kilroy, Ohio
Eric J.J. Massa, New York
Dina Titus, Nevada
Vacancy

Peter T. King, New York
Lamar Smith, Texas
Mark E. Souder, Indiana
Daniel E. Lungren, California
Mike Rogers, Alabama
Michael T. McCaul, Texas
Charles W. Dent, Pennsylvania
Gus M. Bilirakis, Florida
Paul C. Broun, Georgia
Candice S. Miller, Michigan
Pete Olson, Texas
Anh "Joseph" Cao, Louisiana
Steve Austria, Ohio

I. Lanier Avant, *Staff Director*
Rosaline Cohen, *Chief Counsel*
Michael Twinchek, *Chief Clerk*
Robert O'Connor, *Minority Staff Director*

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

Jane Harman, California, *Chair*

Christopher P. Carney, Pennsylvania
Yvette D. Clarke, New York
Ann Kirkpatrick, Arizona
Al Green, Texas
James A. Himes, Connecticut
Vacancy
Bennie G. Thompson, Mississippi *(Ex Officio)*

Michael T. McCaul, Texas
Charles W. Dent, Pennsylvania
Paul C. Broun, Georgia
Mark E. Souder, Indiana
Peter T. King, New York *(Ex Officio)*

Michael Blinde, *Staff Director*
Natalie Nixon, *Deputy Chief Clerk*

CONTENTS

Page

STATEMENTS

WITNESSES

BEYOND ISE IMPLEMENTATION: EXPLORING THE WAY FORWARD FOR INFORMATION SHARING

Thursday, July 30, 2009

U.S. House of Representatives,
Committee on Homeland Security,
Subcommittee on Intelligence, Information Sharing,
and Terrorism Risk Assessment,
Washington, DC.

The subcommittee met, pursuant to call, at 10:05 a.m., in Room 311, Cannon House Office Building, Hon. Christopher P. Carney presiding.

Present: Representatives Carney, Clarke, Kirkpatrick, Green, Himes, McCaul, Dent, and Souder.

Also Present: Representative Pascrell.

Mr. Carney [presiding]. The subcommittee will come to order.

The subcommittee is meeting today to receive testimony on the current status of information sharing and to explore the future outlook for information sharing at today's hearing entitled "Beyond ISE Implementation: Exploring the Way Forward for Information Sharing."

In the early hours of the morning on September 9, 2001, a Maryland State trooper pulled over a red sports car headed north on I–95 at 90 miles an hour. It was a routine traffic stop. The officer asked the driver for a license and registration and asked him a few questions. Eventually, a ticket was issued to him and he sent him on his way. The driver was Zaid Jarrah. Two days later he was at the controls of hijacked United Flight 93 when it crashed in western Pennsylvania.

Jarrah was on the CIA watch list, but that information was not available to Maryland State Police. If it had been, who knows what might have happened?

Information sharing at the Federal, State, and local level has come a long way since that night in 2001. This administration's Homeland Security agenda supports that trend and endorses many promising efforts, including the ITACG, the Nation-wide SAR initiative and fusion centers.

Today, if a police officer were to pull over a suspected terrorist like Jarrah, there is a reasonable chance that the officer would have the necessary real-time information to do something about it, but there is a reasonable chance that he might not. In June of this year, the Program Manager for the Information Sharing Environment reported that, "The challenges to appropriate information sharing remain formidable," although in many hearings of this subcommittee we have learned that the greatest challenge is cultural, transitioning the relevant agencies from the old, "need-to-know," mentality to one that embraces the need to share. That is no small task indeed. The ISE report makes it clear that the old mind-set remains entrenched, citing turf conflicts and agency tunnel vision.

These problems are not new, and for the past few years this subcommittee has focused on identifying and removing the obstacles that hinder information sharing. I believe it is vital to national security. The next terrorist attack isn't going to be stopped by a bureaucrat in Washington; it will be a cop on the beat familiar with the rhythms of his or her neighborhood and armed with timely, actionable information.

In an effort to get that information into the hands of the people who need it most, this subcommittee drafted a bill to reduce the problem of intelligence overclassification, H.R. 553, which is currently being negotiated in the Senate. The bill calls for a framework that would, as the ISE report puts it, minimize the effect of excessive originator controls. In short, it seeks to ramp up the way training for those who classify documents is done and create incentives for classifying intelligence the right way only to protect sources and methods, not to protect turf. It also clarifies the need for portion marking, separating out paragraphs in a classified document that are unclassified and that can be shared with law enforcement.

Some agency officials have already begun to embrace the need to share. Last month this subcommittee had heard encouraging testimony from DHS Acting I&A Under Secretary Bart Johnson. He outlined an impressive vision for a new era of State and local cooperation within the Office of Intelligence and Analysis that is consistent with our efforts.

The questions before us today are, how can we further break down the barriers to information sharing and what can we do to make sure the right people are getting the right information at the right time. To answer those questions, I would like to welcome someone who was, for a long time, a lone voice in the wilderness, Ambassador Ted McNamara.

Mr. Ambassador, today you are on friendly territory. Thank you for your long service and, particularly, for responding to the call to work on this issue of vital importance. I hope that in the summary of your testimony you will talk about the unfinished business you leave to your successor. You are the foremost expert on this issue, its founding father, but as we have discussed, much more needs to be done.

I also welcome and thank Colonel Rick Fuentes and Jeff Smith for joining us this morning. Thank you.

Colonel Fuentes understands the need to share. He is a forward-thinking officer who has led the charge to support ITACG by leading some of the first manpower to this critical mission. Jeff Smith is a trusted friend and adviser. His work as CIA general counsel, expert on FISA and board member at the Markle Foundation make him superbly qualified to testify on this subject. Markle recently released a report about information sharing that is, in fact, required reading.

So welcome to the witnesses, and I look forward to hearing a summary of your testimony.

I now recognize the Ranking Member of the subcommittee, the gentleman from Texas, Mr. McCaul, for his opening statement.

Mr. MCCAUL. I thank the Chairman. I welcome the witnesses here today, in particular, Ambassador McNamara for your tremendous service that you have given to our Nation.

At today's hearing we will examine, as the Chairman said, the current status of the Information Sharing Environment and the challenges that still exist for information sharing across all levels of government. As we all know, ensuring that critical information is shared with all key stakeholders is absolutely essential to the security of our Nation.

The National Commission on Terrorist Attacks upon the United States, also known as the 9/11 Commission, identified 10 lost operational opportunities to prevent the 9/11 attacks, the majority of which were the result of the failure of Government agencies to properly share information with one another, one example pointed out by the Chairman in his opening statement.

Additionally, one of the Commission's key recommendations was for agencies to have a more unified effort in information sharing.

It was under this impetus that the ISE was first established in 2005. Almost 8 years have passed since the attacks of 9/11, and the urgency of this key mission seems to have died down. This complacency is worrisome because it prevents the transformation in the information-sharing culture and processes that were so critically needed. However, the threats facing our Nation are still very real, and the need for the ISE framework is still as crucial now as it was after 9/11.

Much has been accomplished since the ISE was first implemented, including the establishment of a network of State and major urban area fusion centers and the implementation of the Nation-wide Suspicious Activity Reporting Initiative, SAR. These initiatives are key elements in how information sharing is extended to State and local partners.

Nonetheless, we still face many challenges in achieving the ISE framework as it was envisioned, and we must not forget the urgency of this critical mission.

I look forward to hearing the testimony from the witnesses, and I yield back.

Mr. CARNEY. I thank the gentleman.

Other Members of the subcommittee are reminded that under committee rules opening statements may be submitted for the record.

[The statement of Chairman Thompson follows:]

PREPARED STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JULY 30, 2009

Thank you, Madame Chair. I agree that the topic of the hearing today—information sharing—is absolutely critical to our Nation's security.

No matter how we say it—"knowing what we know," "connecting the dots," "getting the right information to the right people at the right time"—we're talking about the same thing.

An environment in which information is shared is an environment in which better decisions can be made and, ultimately, in which people are safer.

However, without such an environment, our first preventers—those who are most likely to detect and stop a terrorist plot in its tracks—may not be able to connect those dots; they may not be prepared to stop the next attack.

This is not a new message.

Fortunately, our persistence is starting to pay off. We have seen some progress in information sharing.

The Program Manager for the Information Sharing Environment's most recent report to Congress describes some admirable work that has been accomplished, including the efforts to create a network of fusion centers and developing a respected ISE Enterprise Architecture Framework.

Nonetheless, and this also is not a new message, we must do more.

Although I am pleased to acknowledge progress the ISE has made under Ambassador McNamara's watchful eye, I am concerned that many of the challenges noted in the ISE report are not new challenges.

For example, formulating a means to protect the privacy and civil rights of American citizens in the design and operation of the ISE was required under the legislation that mandated the original ISE Implementation Plan.

However, while the ISE has issued Privacy Guidelines, the 2009 ISE report says nine Departments or Agencies under the ISE are still developing their privacy protection policy required by those guidelines, and three do not even have a policy in development.

It is challenges such as these that we are here to explore today. I hope each of our witnesses will be forthcoming in your assessments of these and other challenges that lie ahead for the information-sharing environment.

Only by helping us fully understand the challenges ahead can we hope to work together to craft solutions to these problems.

I welcome you all, and I look forward to your testimony.

Mr. CARNEY. Without objection, the gentleman from New Jersey, Mr. Pascrell, is authorized to sit for the purpose of questioning witnesses during the hearing today.

Hearing no objection, so ordered. I believe Mr. Pascrell, at the proper time, will want to introduce Colonel Fuentes, as well.

Mr. PASCRELL. Thank you.

Mr. CARNEY. I now welcome the witnesses this morning. Ambassador Thomas McNamara has been the Program Manager for the Information Sharing Environment since March 2006. After more than 3 years of overseeing the ISE, he sits before the subcommittee today to deliver his last testimony in this capacity—certainly not his last testimony before us, I hope.

Mr. Ambassador was a career diplomat, having held several senior positions at the Department of State and the National Security Council. He retired from Government service in 1998 and spent 3 years as the President and CEO of the Americas Society and the Council of the Americas. However, after the attacks of September 11, 2001, he was asked to return to Government service.

Mr. Jeffrey Smith forms part of the Markle Foundation Task Force on National Security in the Information Age steering committee. He took a leading role in preparing the report "Nation at Risk: Policymakers Need Better Information to Protect the Country", which was released in March 2009. He is also currently a partner at Arnold & Porter, LLP. Prior to this, he held Government positions such as General Counsel for the CIA and General Counsel for the Senate Armed Services Committee.

Without objection, their full statements will be inserted into the record.

I now ask Mr. Pascrell to introduce Colonel Fuentes.

Mr. PASCRELL. Thank you, Mr. Chairman.

Mr. Chairman, Chairman Carney, Ranking Member McCaul, I want to thank you for allowing me to be part of this particular subcommittee. I think it is very critical, this subcommittee.

It is my privilege to be able to introduce my fellow New Jersey native, Colonel Rick Fuentes, who serves as the Superintendent of our State police. He became the 14th superintendent of New Jersey State Police in 2003 and is currently one of the highest ranking law enforcement officers in Governor Corzine's administration. I must say, he has brought the State police in our State to an entirely new level: Total respect, integrity of his department, the finest men and women I know in the State of New Jersey are State troopers, period.

Colonel Fuentes enlisted in the State police in January 1978, rose through the ranks, and prior to being named Acting Superintendent he was assigned as the Chief of the Intelligence Bureau. We can learn much from him. He oversaw nine units, I believe, in the intelligence section.

He is the recipient of numerous awards, as has been recognized by the U.S. Justice Department, the Drug Enforcement Administration, and in 1993 was a corecipient of the New Jersey Police Trooper of the Year award.

Superintendent Fuentes earned a Bachelor of Science degree from Kean College in New Jersey in 1977; a Master of Arts, Criminal Justice, from John Jay College of Criminal Justice in New York in 1992; and a Doctorate of Philosophy in Criminal Justice from City University of New York in 1998.

I want to note that he is here, testifying at this hearing, in his role as Chairman of the Homeland Security Committee for the International Association of Chiefs of Police. So he joins two others.

What a great panel of people who know what they are talking about. Isn't that something new?

Colonel Fuentes has the experience necessary—on many levels necessary to speak on this critical subject. I look forward to hearing his testimony.

Mr. Chairman, so many times we have heard since 9/11 that one of the major problems confronting all of us—and we tried to tackle it in a bipartisan way—is the lack of cooperation and sharing of information between those intelligence communities that are out there doing their job.

I think we have moved the ball a little bit, and I know your commitment to this goal. I am glad you put this particular panel together, and I am honored to have introduced Colonel Fuentes.

Mr. CARNEY. Thank you, Mr. Pascrell.

I now ask Ambassador McNamara to summarize his statement for 5 minutes.

STATEMENT OF AMBASSADOR THOMAS E. MC NAMARA, PROGRAM MANAGER, INFORMATION SHARING ENVIRONMENT, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Mr. MCNAMARA. Thank you very much, Chairman Carney and Ranking Member McCaul, and Members of the subcommittee. I find, as I wrap up my career in my term here as Program Manager, the great pleasure to appear before this subcommittee.

I want to begin by thanking the subcommittee and the committee for their sustained support in building the Information Sharing Environment over the past 3½ years that I have spent in this job. I can say, quite frankly and correctly, that were it not for your support and that of your Senate colleagues on the Homeland Security Committee in the Senate, the attentiveness and oversight that you showed, the support you have given me and others throughout the country who are trying to build the ISE, we could not have reported the progress that we have reported in our annual report to the Congress.

The ISE is groundbreaking, not just for the information sharing it is effecting, but because it is a catalyst for change. Indeed, it is a radical change in Government information management.

I am pleased to report that the information culture of the bureaucracy is changing, but slowly. Having no template to pattern our efforts we in the Program Manager's Office have invented and designed a foundation by a methodology of rationalizing, simplifying, and standardizing—and harmonizing, excuse me—harmonizing existing policies and practices and technologies at all levels of government. That was your legislative mandate to us, and we are implementing it.

The business processes we have defined, for example—as the Chair mentioned—SAR; the policies we have changed, for example, privacy policies; and the technology platforms we have established, such as new architectures and new standards in the Federal Government's IT arsenal; these are, in fact, the new Information Sharing Environment. These are the elements that will make it up.

We are already seeing its contribution. It has helped with the FAA's modernization effort, it has helped with the health IT initiative that is under way, and it has helped with the creation of the maritime and air domain environments.

The ISE is fundamentally changing information management throughout the Federal Government. This is relevant to you because Congress never envisaged the ISE to be another bureaucracy, but rather a change agent; and in that respect, it is already a success. You have done your part, as have many others, including my two colleagues who represent our strong partnership with nongovernmental and the State, local, Tribal, and territorial partners.

I am going to step down as Program Manager tomorrow, so I appreciate this final opportunity to update the subcommittee on the highlights of the challenges that remain 8 years after the horrific events of 9/11. As I look back, I see that we have made substantial progress, but as I look forward, I see that even more remains to be done. So let me list some of the priorities and also some of the obstacles that we faced. I will start with the obstacles.

Accomplishing anything in the Federal bureaucracy requires a formidable effort. The complexity of the challenges for the ISE are indeed formidable. This is because cultural change is by far the most difficult problem for any bureaucracy; and the bigger the bureaucracy, the harder the cultural changes. By "cultural change," I mean the way we do business every day.

What I have encountered are differing agency missions, conflicts over turf, resource shortfalls, bureaucratic inertia and agency tunnel vision. These remain the major impediments to a functional

ISE, not the technology. The technology is there to be used. It is the cultural problems that hold us back. But we have made, as I said, some accomplishments, and let me list a few of them.

First of all, we have been able with our State and local partners to ensure that fusion centers are, in fact, up and running. The priority for the future is to be sure that they are well-staffed, mission-oriented and, above all, sustainable. They need access to classified and controlled unclassified information in the same way as Federal officials. They, in turn, must analyze and produce high-quality products to share with localities and other fusion centers and the private sector, while at the same time being aware of and observing privacy and civil liberties requirements.

The second priority for the future, I think, is to adopt a Nation-wide, common, security clearance set of standards, and also common-identity management and common, role-based access. These are essential in the IT world if we are to share information—somewhat arcane, but nonetheless it must be done, and it can be done.

Third, what we need to do is to fully implement the CUI, controlled unclassified information, framework. This is especially critical for the Federal Government working with the State, local, Tribal, and territorial authorities, because they work primarily in that domain.

Fourth, a priority must be given so that there are more resources for privacy officers in the agencies of the Federal Government so that they can draft, review, and publish their ISE privacy policies. Right now, they are woefully understaffed across the Federal Government. Secondly in this priority, we need to stand up to the Privacy and Civil Liberties Board which was mandated by the Congress.

The fifth priority area is to reduce overclassification, to replace "need to know" with "need to share," as you have mentioned, Mr. Chairman. To take "need to share" and "authorized use," those terms, and define them carefully so that they can assist us in moving information in the Information Sharing Environment. We need also to limit originator controls that needlessly impede discovery and sharing of information.

The sixth priority is to institutionalize a Nation-wide capability to gather and share SAR information. This is a very practical and achievable objective within the next 6 months to a year. We are well on the way to achieving that objective, even now.

The seventh priority, to coordinate agency budgets, reduce funding overlaps and gaps, and monitor investments to drive the agencies towards compatible technologies and business processes and to maximize resource use. In section 1016 of the Intelligence Reform and Terrorism Prevention Act, the IRTPA of 2004, I was asked to recommend, "a future management structure for the ISE," including whether the position of the Program Manager should continue. I have been in this position since 2006; and so as I depart, I would like to leave some personal observations in response to that request in 1016.

Mr. CARNEY. Mr. Ambassador, we will get to those in a moment. We need to move on to the next witness, if you don't mind.

Mr. MCNAMARA. Okay, fine.

Mr. CARNEY. Thank you so much.

[The statement of Mr. McNamara follows:]

Prepared Statement of Thomas E. McNamara

July 30, 2009

Madame Chair, 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 4 years. This subcommittee has been a real champion of information sharing, and the ISE in particular. I especially want to thank you, Madame Chair, 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 8 years after the terrible events of September 11, 2001.

INTRODUCTION

Since I assumed the position of PM–ISE in March 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 Nation-wide 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 3-year retrospective on the ISE summarizing what was originally intended, what has already been accomplished, and what remains to be done; and
- Second, 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 3-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 3 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 2, 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.

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

[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).

approach that will drive all future ISE implementation activities. The Framework creates critical linkages between four primary and enduring ISE goals, 14 subgoals, 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, subgoals, and goals, as called for in the GAO report.

SUMMARY OF 2008–2009 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 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.

[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).

[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 PCC also provided on-going 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

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

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 Nation-wide implementation;
- 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, DC 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 on-line 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 to address issues in a timely manner.

ON-GOING 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 Nation-wide 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.

Mr. CARNEY. Colonel Fuentes for 5 minutes, please.

STATEMENT OF COLONEL JOSEPH R. FUENTES, SUPERINTENDENT, NEW JERSEY STATE POLICE

Mr. FUENTES. Good morning, Mr. Carney and Ranking Member Mr. McCaul. I find myself sitting in the room once again with my distinguished congressional Representative from New Jersey and trying to live up to his expectations.

Thank you, Congressman.

When it comes to information sharing and intelligence, I am also sort of the thorn here between two roses. These are the experts, my colleagues, Mr. Smith authoring the Markle Report, a much dog-eared and referenced document on many committees that I serve on, and it is a very preeminent document.

As to Ambassador McNamara, I want to thank him certainly from the bottom of my heart and on behalf of all the initiatives that are going on in State and local right now. Much of what I am about to say here relates to a robust Information Sharing Environment, and that is largely an attribute of the Ambassador's talent and strong sense of collaboration as Program Manager of the ISE.

He has effectively and successfully navigated the PM–ISE to a watershed of national information-sharing initiatives that will continue to have a profound impact on improving our Nation's homeland and hometown security. Make no mistake about it those two things are connected very strongly.

In many ways he established within the PM–ISE Office the integrity and reputation of a neutral third party, certainly not easy to do, creating and refereeing a mutually beneficial information-sharing environment across the spectrum of intelligence and first responder agencies.

I know I join everybody that I work with and on the many committees that I am on in wishing him well in the future and thank him very much for what he has done.

I would like to just frame the remainder of my remarks around the issue of fusion centers and their critical link to the effect of Federal, State, Tribal, and local information sharing in this country.

First off, the success of information sharing will hinge on the adherence to privacy interest and civil liberties. I have attended numerous information-sharing summits and stakeholder meetings sponsored by the IACP, DOJ, and DHS, and the issues of policy and privacy are always and foremost closely linked to those discussions.

Each fusion center is required to submit a privacy policy that is guided by a Federal matrix which must be approved by DOJ and DHS. Since 2007, the Bureau of Justice Assistance has developed privacy policy templates and provided training and technical assistance to the fusion centers. In conjunction with the national Suspicious Activity Reporting Initiative that the Ambassador mentioned, there has been numerous training that was provided by the Bureau of Justice Assistance that has been a tremendous aid to those of us who must manage fusion centers.

As a matter of fact, the first time that the SAR initiative was used was on Inauguration Day in January. More than 4,000 police officers were trained in recognizing suspicious behaviors, and it was one of the first times that the SAR was used. Obviously the success and the safety of that event is testament to the success of that initiative.

Presently, there are 72 fusion centers in this country, 50 of which are State-designated fusion centers, 22 are urban area security initiative fusion centers that are either located in the major cities or in densely populated regions. They are at varying levels of maturity, which raises some concerns for purposes of this discussion, but they are guided in their evolution by a set of baseline capabilities that have been put out by the Global Committee, Bureau of Justice Assistance, PM–ISE, and DHS.

I am impressed by this administration's commitment to fusion centers, as is evident in both the words and the actions of Secretary Napolitano.

Besides DHS and DOJ support for the fusion centers, I would like to once again highlight the work of BJA that has been a leading partner in providing training and technical assistance in helping all the fusion centers to achieve baseline capabilities.

Fusion centers bring all the relevant partners together to maximize the ability to prevent and respond to terrorism and criminal acts, using an all-hazards, all-crimes approach. By embracing this concept, these entities will be able to effectively and efficiently safeguard our homeland and maximize anticrime efforts.

So often terrorism is found to have linked itself—and, sir, Mr. Carney, you mentioned it was Zaid Jarrah. He was stopped for a traffic offense, and had we had that information just a very few days before 9/11, there may have been more action that could have been taken.

So there is constantly a nexus between terrorism, crime, and traffic, that we are sort of on the front lines with that, all the police in this country; and aggressive traffic and criminal enforcement is a way to resolve some of the issues of terrorism.

The national strategy for information sharing calls for the fusion centers to be the backbone of information sharing involving State and local governments. The fusion centers help to organize and channel the information flow from the numerous Federal partners so that it is usable and actionable to the States and to the locals.

The fusion centers have a very difficult job, and that is to harness the 18,000 State, local, and Tribal law enforcement agencies into an effective collection process so that the eyes and ears in the community of 1 million police officers in this country can collect the dots of information that arise in the routine course of their duties, where those leads are going to generate good investigations, and then be assured through the fusion center that there will be a place to connect those dots, if warranted, and produce lead value information so that terrorist plots or criminal plots or conspiracies can be interdicted.

In 2006, our Homeland Security Adviser, Dick Canas, came before this subcommittee and announced the soon-to-be-opening Regional Operations and Intelligence Center in the State of New Jersey. That center has been open now for 3 years. It contains the New Jersey Office of Emergency Management, the State EOC, Emergency Operation Center, Mobile 911 Call Center, a Watch Operation Center and an analysis element.

If I can just quickly talk about two of those components, sir?

Mr. CARNEY. In the question phase, please.

Mr. FUENTES. Absolutely.

Mr. CARNEY. Thank you.

[The statement of Mr. Fuentes follows:]

PREPARED STATEMENT OF JOSEPH R. FUENTES

JULY 30, 2009

Good morning Madame Chair Harman, Ranking Member McCaul and distinguished Members of this subcommittee. My name is Rick Fuentes and I serve as the Colonel and Superintendent of the New Jersey State Police (NJSP). I also serve as the Chair of the International Association of Chiefs of Police (IACP) Homeland Security Committee and am a member of the Global Intelligence Working Group and Global's Criminal Intelligence Coordinating Council. Global includes over 30 law enforcement and criminal justice professional associations that have developed data standards, privacy policy, identity management, and the National Information Exchange Model (NIEM) which has allowed the Program Manager for the Information Sharing Environment (PM–ISE) and the U.S. Department of Homeland Security (DHS) to move faster in the State local and Federal information-sharing effort focused on terrorism and all crimes.

I am grateful to this subcommittee for their strong advocacy for and pursuit of more effective and efficient means of information sharing between all levels of law enforcement in the interest of public safety. I want to thank you, Madame Chair, for including a representative of State and local law enforcement in your hearing today. That sends a very positive message to the more than 18,000 agencies represented by IACP as this Nation's largest constituency of law enforcement and of this subcommittee's willingness and eagerness to solicit that viewpoint and perspective.

First, I would like to thank and congratulate my distinguished fellow panelist, Ambassador McNamara. Much of what I am about to say relates to a robust information-sharing environment that is largely an attribute to the Ambassador's talent and strong sense of collaboration as Program Manager of the ISE. He has effectively and successfully navigated the PM–ISE through a watershed of national information sharing initiatives that will continue to have a profound impact on improving our Nation's homeland and hometown security. In many ways, he established within the PS–ISE office the integrity and reputation of a neutral third party, creating and refereeing a mutually-beneficial information sharing environment across the spectrum of intelligence and first responder agencies. I wish him well.

I would like to frame the remainder of my testimony around the issue of fusion centers and their critical link to effective Federal, State, Tribal, and local information sharing in this country. First off, the success of information sharing will hinge on the adherence to privacy interests and civil liberties. I have attended numerous information sharing summits and stakeholder meetings sponsored by IACP, U.S. Department of Justice (DOJ) and DHS and the issues of policy and privacy are closely linked in those discussions. Each fusion center is required to submit a privacy policy guided by a Federal matrix to DOJ/DHS for approval.

Since 2007, the Bureau of Justice Assistance (BJA) and DHS have developed privacy policy templates and provided training and technical assistance to the fusion centers. In conjunction with the National Suspicious Activity Report Initiative (referred to as SAR), BJA and other partners have opened up the training and data formats to the privacy community and privacy advocacy groups. BJA, in conjunction with the PM–ISE, the Washington, DC, Metropolitan Police Department and others introduced the SAR effort to support the security of the Inaugural Day activities in January 2009. More than 4,000 police officers from the National Capital Region were trained on behaviors and privacy issues. This training was also shared with the American Civil Liberties Union (ACLU) and recommendations on their part were incorporated into the training.

Presently, there are 72 recognized fusion centers in this country, 50 of which are State-designated fusion centers and 22 are Urban Area Security Initiative (UASI) fusion centers either located in the major cities or densely populated regions. They are at varying levels of maturity, but are guided in their evolution by a set of baseline capabilities formulated in collaboration with their Federal partners.

I am impressed by this administration's commitment to fusion centers, as evident in both the words and actions of Secretary Napolitano. Besides DHS and DOJ support for the fusion centers, I'd like to highlight the work of BJA. BJA has been a leading partner in providing training and technical assistance to the fusion centers in helping them to achieve baseline capabilities. Each year, BJA manages the National Fusion Center conference attended by more than a thousand law enforcement executives, Federal authorities, fusion center directors, and analysts. BJA has been able to harness the great work of Global to support and jump-start many initiatives needed to support the fusion centers, such as governance, intelligence commander training, and the use of fusion center liaison officers. It is important to note that this assistance is provided free of charge to the States and cities. To date, more than 160 individual technical assistance services have been delivered.

Fusion centers bring all the relevant partners together to maximize the ability to prevent and respond to terrorism and criminal acts using an all-hazards, all-crimes approach. By embracing this concept, these entities will be able to effectively and efficiently safeguard our homeland and maximize anticrime efforts.

The National Strategy for Information Sharing calls for the fusion centers to be the backbone of information sharing involving State and local governments. The fusion centers help to organize and channel the information flow from the numerous Federal partners so that it is useable and actionable to the States and locals. The fusion centers also aim to harness the 18,000 State, local, and Tribal law enforcement agencies into an effective collection process so that the eyes and ears in the community of 1 million police officers can collect the dots of information that arise in the routine course of their duties and be assured that there is a place that will connect the dots, if warranted, and produce lead value information that will reduce the threat of crime and terrorism.

Although guided by a Federal blueprint to achieve a baseline operational competency, the fusion centers are functions of State and local governments. In order to achieve sustainability, fusion centers will need to go beyond the baseline in responding to the needs and priorities in their respective States. Those needs will vary and may include criminal street gangs, drugs, guns, or cross-border illegal immigration.

In 2006, New Jersey's Homeland Security Adviser, Richard Canas, came before this subcommittee and spoke of the upcoming opening of the Regional Operations and Intelligence Center (ROIC), pronounced "Rock," New Jersey's State-designated fusion center. The New Jersey State Police has executive agency responsibility in the ROIC. The ROIC houses New Jersey's Office of Emergency Management, the State Emergency Operations Center (EOC), the mobile 9–1–1 Call Center, an Analysis Element and a Watch Operations Center.

Watch Operations is where the State-wide deployment of State Police hazardous material and emergency management specialists, tactical entry personnel, canine, aviation, marine, bomb, and arson assets are coordinated and where there is constant situational awareness of State-wide traffic and road conditions, weather events, toxic spills, school evacuations, bomb threats, National and international terrorist events, and general law enforcement operations. Information on these events are packaged in concise summaries and disseminated to pertinent customers through more than 70 email notification groups. The New Jersey State Police, New Jersey Office of Homeland Security and Preparedness, New Jersey Transit Police and the Port Authority of New York and New Jersey Police Department all occupy seats in Watch Operations. The Office of Homeland Security also manages and staffs the State's terrorism tip line.

The anecdote to the siloing of information takes place in the ROIC's Analysis Element, a vibrant and collaborative information-sharing environment comprised of representatives and analysts from State Police, DHS, FBI, ATF, Federal Air Marshals, Immigration and Customs Enforcement, Coast Guard, N.J. Division of Fire Safety, Philadelphia Police Department, and Newark Police Department. There are no shoulder patches or egos there. At 10:00 a.m. every weekday morning, these agencies gather in what we call "the huddle" to brief each other on the current threat environment and to set priorities, particularly those that require imminent analysis and dissemination.

Operating with an “all-hazards, all-crimes” approach and a customer philosophy of “give us a quarter’s worth of information and we’ll provide you with a dollar’s worth of analysis and lead value intelligence information,” the Analysis Element is the tip of the spear in Governor Corzine’s State-wide Anti-Crime Plan to reduce violence and promote safe neighborhoods. Information-sharing initiatives that carry acronyms such as NJ Crime Track, NJ POP Collective, NJ TAG, NJDEx and NJ–Trace are connecting police records management systems around the State through federated search inquiries, targeting criminal street gangs, providing hotspot analysis, trending on State-wide violent crime and tracking the illegal spread of firearms. Addressing the latter, I’d like to provide you with information on NJ–Trace, an effective Federal and State anti-crime initiative.

In order to maximize the lead value of a firearm recovered in a crime, the ATF has a program called e-Trace that tracks the history of a firearm back to its source purchase. This program allows ATF to discern patterns in firearms sales that have a short “time to crime;” in other words, the span of time from original purchase to its use and recovery in a crime. This statistic can effectively identify firearms traffickers and gun dealers engaged in illicit sales practices.

Unfortunately, to submit a firearm to e-Trace required a voluntary effort on the part of a busy police officer to navigate several computer screens beyond the routine stolen weapons inquiry or put together a handwritten sheet to be faxed to ATF. Until recently, only one-quarter of all firearms recovered in a crime in New Jersey were submitted to ATF for e-Trace.

Working with ATF, we interposed the ROIC Analysis Element in the exchange of information between the police officer and ATF, so that e-Trace requests to ATF and responses back to the police officer were captured and analyzed by the ROIC crime analysts. In this manner, we could share information on the spread of illicit firearms across local, county, and State boundaries. We named this fusion center initiative NJ–Trace and established a Gun Crime Center within the ROIC Analysis Element.

New Jersey State Attorney General Anne Milgram issued a directive to all county prosecutors and law enforcement agencies in New Jersey mandating the reporting of all crime-recovered firearms through NJ–Trace. Every time a police officer runs an NCIC computer inquiry to see if a recovered firearm is stolen, a message pops up in the center of the screen reminding the officer that they will not receive a response without first conducting a gun trace through ATF. That trace entry is transmitted to the ROIC’s Gun Crime Center and entered into the ATF e-Trace program by a ROIC analyst. ATF responses are sent back to the requesting officer’s agency and to the Gun Crime Center in the ROIC.

Less than a year after the implementation of NJ–Trace, police submissions to trace crime-recovered firearms have increased from 25 percent to almost 90 percent. The Gun Crime Center analyzes results and looks for State-wide patterns and trends for recovered firearms used in violent crimes and to seek out those individuals who traffic in those firearms. Last week, as a result of NJ–Trace, State Attorney General Milgram announced 11 separate State indictments against 12 individuals for trafficking firearms.

What I have just described in the ROIC is an all-hazards, all-crimes approach to information sharing and intelligence-led policing. All information is first filtered for a nexus to terrorism, as terrorism is a crime often facilitated by more overt criminal behaviors. The purchase or theft of firearms, the purchase or manufacture of fraudulent identity documents, funding streams through narcotics sales or transporting contraband such as explosives all provide police with many more opportunities to preempt or interdict actions that may be precursors to or actual terrorist activities. Those opportunities might be lost if police departments did not pursue aggressive criminal and traffic enforcement policies. And that enforcement could not achieve a greater law enforcement and public safety objective if the means and processes to collect, connect, and analyze disparate events did not reside in a State-wide, regional or local fusion center.

With much accomplished, and the need to continue the progress of the PM–ISE, the path ahead in information sharing is not clear of obstacles. Challenges to information sharing include the following:

1. A commonly recognized and accepted security clearance across Federal agencies.
2. Fusion centers are confronted with the need to query dozens of information systems. The solution is the adoption of a migration to a common data standard, such as NIEM, that would standardize search terms to enhance data interoperability between fusion centers and those systems at all levels.
3. Use of fusion centers as broadcast outlets for elevations in the DHS Homeland Security Advisory System and other alerts, warnings, and notifications.

> 4. Funding the continued deployment of Federal analysts to the fusion centers.
> 5. Funding the training and accreditation of analysts to promote uniform best practices in the fusion centers.
> 6. Going beyond the baseline to help fusion centers achieve customer satisfaction at all levels of law enforcement.
> 7. Nation-wide rollout of the SAR initiative.
> 8. The establishment of a research and development function within DOJ or DHS to explore social networking and communication technologies that could, with appropriate security safeguards, enhance analytical capabilities, and facilitate information sharing.

There are many success stories that demonstrate the progress we are making in the area of information sharing. There are still many issues to solve but the good work that has been demonstrated in the use of NIEM, the development of fusion centers, the roll out of the SAR initiative and the move to establish State-wide or regional intelligence academies bodes well for the future and our ability to sustain sound levels of homeland and hometown security.

I thank you for your attention and would be happy to answer any questions you may have.

Mr. CARNEY. Mr. Smith, please summarize for 5 minutes.

STATEMENT OF JEFFREY H. SMITH, STEERING COMMITTEE, MARKLE FOUNDATION

Mr. SMITH. I will try to do this in less than 5 minutes, Mr. Chairman.

Mr. Chairman, Mr. McCaul, it is an honor to appear here this morning on behalf of the Markle task force, and I am grateful that you put my full statement in the record.

I also want to join my colleagues and this committee in thanking Ambassador Ted McNamara. The Nation owes him our thanks for a job well done; however, as the Ambassador's report acknowledges, much work remains.

In March of this year, the Markle task force released a report that found nearly 8 years after the September 11 attacks the United States is still at risk. Policymakers from the President to local police chiefs still need better information to defend our homeland.

The good news is that new laws have been passed and, in our judgment, no further legislation is required at this point. Unfortunately, however, the sense of urgency has diminished. Congress and the President must provide robust oversight and leadership to help ensure that officials charged with implementing these laws do so vigorously. This hearing this morning is a step in the right direction, and again I commend the subcommittee for its leadership.

Our task force's report makes concrete recommendations for addressing the cultural, institutional, and perceived technological obstacles that are slowing progress on information sharing. Let me use the remainder of my time to discuss three areas where we think future work is needed.

First, strong, sustained leadership from the President and Congressional oversight are needed. Although the Program Manager—ISE has made great contributions, the position is widely but incorrectly seen as an adjunct of the intelligence community. The White House is currently taking action to improve the existing structure, but we think additional strength needs to be added to the position of the Information Sharing Council, and the White House—the good news is, the White House has taken increased ownership of this issue. We take heart from these early actions, but it is critical that the official charged with leading the Government-wide coordination of information-sharing policy have adequate horsepower to drive interagency coordination; otherwise, wasteful, duplicative efforts by individual agencies working independently are inevitable.

Many believe that this official should be appointed by the President and confirmed by the Senate. This will ensure accountability to Congress and will increase the position's clout, providing the necessary horsepower to overcome the bureaucratic resistance and turf wars that stymie progress. Giving the official some budgetary authority should also be considered.

The second point, all Government information relevant to National security should be discoverable and accessible to authorized users while audited to ensure accountability. Authorized users must have the capacity to discover and locate relevant information, a capability we call discoverability. The Director of National Intelligence issued a directive last year, ICD–501, that is a step in the right direction, but the implementation of this will be critical.

Third, enhanced Government-wide privacy and civil liberties policies must be developed. The PM–ISE has taken good first steps, but much remains to be done. The guidance, in our judgment, that has been provided by the PM–ISE is still too vague. We suggest a series of very specific measures in the privacy field that we think should be taken. Among those are, of course, the early creation and populating of the Privacy Oversight Board, which sadly has languished.

With that, Mr. Chairman, I will end a little bit early and look forward to your questions.

[The statement of Mr. Smith follows:]

PREPARED STATEMENT OF JEFFREY H. SMITH[1]

JULY 30, 2009

Chair Harman, Ranking Member McCaul, I appear today as a member of the Markle Foundation Task Force on National Security in the Information Age and would like to thank you for holding this hearing and taking the initiative to improve information sharing by dedicating your time and energy to this critical issue. Making information sharing a top priority is essential to safeguard our National and homeland security.

The Markle Task Force's most recent report found that, although we have made much progress, we are still vulnerable to attack because—as on 9/11—we are not able to connect the dots. At the same time, our civil liberties are at risk because we don't have the Government-wide policies in place to protect them as more powerful tools for intelligence collection and sharing information emerge.

Our Government cannot identify, understand, and respond to 21st century threats, such as cyber attacks, terrorism, and energy security, without the collaboration and sharing of information across the Federal, State, and local levels and with the private sector so fragments of information can be brought together to create knowledge. The Information Sharing Environment (ISE) was created by Congress to improve our ability to know what we know about terrorist threats. The ISE was intended to effect a "virtual reorganization of government," allowing communities of interest to work on common problems across agency boundaries and between Federal, State, and local governments, and the private sector—wherever important information could be found.

Ambassador McNamara recently released the Third Annual Report to Congress on the ISE. I am pleased to testify with him this morning and believe the Nation

[1] Member of the Markle Foundation Task Force on National Security in the Information Age and Senior Partner at Arnold & Porter LLP. I am grateful for the assistance of Nicholas Townsend, an associate at Arnold & Porter, and Daniel Friedman, a summer associate from Harvard Law School.

owes him our thanks for a job well done. But much work remains. Under his leadership as the Program Manager for the Information Sharing Environment (PM–ISE), progress has been made toward reducing the barriers to information sharing that persist throughout Government. The ISE has made substantial strides in developing the ISE framework and policies, training, and guidelines for sharing information. However, as the PM–ISE's report acknowledges, there is still a great deal of work to be done.

The Markle Foundation Task Force on National Security in the Information Age, on which I have had the privilege of serving since its inception, recently released a report[2] that found that our Nation remains at risk. Unfortunately, the sense of urgency on information sharing has diminished in the nearly 8 years since the 9/11 attacks. Old habits die hard. The "need-to-know" principle and stovepiping of information within agencies persist. The Markle Task Force's 2009 report makes concrete recommendations to address the cultural, institutional, and perceived technological obstacles that are slowing the implementation of laws intended to facilitate the flow of information and create new ways of collaborating.

I would like to take the remainder of my time to briefly outline the Task Force's core recommendations and to discuss three specific areas in detail where future work is needed—

(1) Strong sustained leadership from within the Executive Office of the President (EOP) and Congressional oversight are needed to drive information sharing;

(2) All Government information relevant to National security should be discoverable and accessible to authorized users while audited to ensure accountability; and

(3) Enhanced Government-wide privacy and civil liberties policies must be developed.

I hope my comments will give this subcommittee a better sense of how far the Government has come toward a trusted information-sharing environment and what steps we believe still need to be taken to provide policy makers at all levels of Federal, State, and local government better information so they can make the best decisions to protect our country.

I. THE MARKLE TASK FORCE'S CORE RECOMMENDATIONS

Before turning to a detailed discussion of the three areas where we believe more work is needed, let me provide a brief overview of the Markle Task Force and the four core recommendations in our most recent report. The Markle Foundation Task Force on National Security in the Information Age is a diverse and bipartisan group of experienced former policy makers and National security experts from the Carter, Reagan, Bush, Clinton, and Bush administrations, senior executives from the information technology industry, and privacy advocates. Under the leadership of Zoe Baird and former Netscape CEO Jim Barksdale, the Markle Task Force has released four reports[3] recommending ways to improve National and homeland security decision making by transforming business processes and the way information is shared while at the same time protecting civil liberties.

The Task Force has worked closely with Government officials, and I am pleased to report that the Government has taken many of our recommendations to heart in both legislation and Executive Orders. Chair Harman and this subcommittee deserve special recognition for their hard work on improving information sharing.

In March, the Task Force published its most recent report in the hope that it would help the Obama administration, which now includes several former Task Force members, develop information-sharing priorities. The report's four core recommendations, which are summarized below, emerged from common themes that arose during the Task Force's interviews with officials in the Executive Branch and Congress on the current state of information sharing.

First, Congress and the administration must provide strong, sustained leadership to reaffirm information sharing as a top priority. There is unfinished business in implementing an information-sharing environment across all Government agencies that have information important to National security, including State and local or-

[2] *Nation at Risk: Policy Makers Need Better Information to Protect the Country (2009).* All of the Markle Task Force's reports are available at *http://www.markle.org/.*

[3] See *Markle Found. Task Force, Nation At Risk: Policy Makers Need Better Information To Protect The Country (2009); Mobilizing Information To Prevent Terrorism (2006); Creating A Trusted Information Network For Homeland Security (2003);* and *Protecting America's Freedom In The Information Age (2002),* available at *http://www.markle.org/markle_programs/policy_for_a_networked_society/national_security/projects/taskforce_national_security.php.*

ganizations. We are at a critical moment where top-down leadership and immediate action at the start of the new administration are required. If there is another terrorist attack on the United States, the American people will neither understand nor forgive a failure to have taken this opportunity to get the right policies and structures in place.

Second, authorized users must have the capacity to discover and locate relevant information quickly and efficiently—a capability called "discoverability." Data should be tagged with standardized information that can be indexed and searched. Using a decentralized system of discoverability, rather than large centralized databases, simultaneously improves our security and minimizes privacy risks by avoiding bulk transfers of data. When combined with an authorized use standard, discoverability ensures that users obtain what they need, but only what they need. This authorized use standard would permit an agency or its employees to obtain information based on their role, mission, and a predicated purpose. We also recommend strong auditing throughout the system, which would allow for improved enforcement of the authorized use standard and would contribute to enhanced information security.

Third, the Obama administration should develop Government-wide privacy and civil liberties policies for information sharing to match increased technological capabilities to collect, store, and analyze information. These policies should be clear, detailed, transparent, and consistent, and must provide direction on hard issues while allowing agencies the flexibility that their different missions and authorities may require. Such policies are necessary both for the American people to have confidence in their Government and for the users of the information-sharing framework to have confidence that their work is lawful and appropriate.

Fourth, the President and Congress need to overcome bureaucratic resistance to change by transforming the culture with metrics and incentives. Mission-oriented metrics are necessary to move away from the "need-to-know" culture and stovepiping of information that persists in many agencies and towards adoption of a "need-to-share" principle. Accountability and transparency should be joined with performance incentives and training to expose failure and reward success. Additionally, users should be empowered to drive information sharing by forming communities of interest. When individual users insist on better information, more effective practices are likely to be put in place to align information flows with user needs.

Although the Task Force's recent work has largely focused on the Federal Government, our recommendations are applicable at the State and local level as well. State and local law enforcement have an essential role to play in protecting our homeland security. A cop on the beat may have information that can stop the next attack, but he needs to know what to look for and how to report it. To keep our country safe, information must be shared effectively, not only within the intelligence community (IC) and among Federal agencies, but also among Federal, State, and local governments and with key private sector partners. As outlined in the PM–ISE's annual report, the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) has been a major focus of the ISE over the last year. The program has enjoyed enthusiastic support from the LAPD and other State and local participants. But more work needs to be done, including a careful examination of the role of fusion centers.

II. STRONG SUSTAINED LEADERSHIP FROM WITHIN THE EOP AND CONGRESSIONAL OVERSIGHT ARE NEEDED TO DRIVE INFORMATION SHARING

The PM–ISE has made great contributions to enhancing information sharing. Ambassador McNamara's recent report says that a comprehensive information sharing policy requires coordination between five communities—Intelligence, Foreign Affairs, Homeland Security, Law Enforcement, and Defense—that cut across all levels of government. However, the PM–ISE's report does not discuss the significant challenges the PM–ISE faces coordinating those five communities from within the Office of the Director of National Intelligence (ODNI). Today, the PM–ISE is widely, but incorrectly, seen by those in the other four communities as part of the intelligence community; as the subcommittee knows, his mandate is much broader.

The White House is currently taking steps to improve the existing structure by carrying out key information-sharing work under the auspices of the EOP. In a July 2, 2009 memorandum, Assistant to the President for Homeland Security and Counterterrorism John Brennan took important steps in three key areas. First, Mr. Brennan's memo identifies effective information sharing and access as a "top priority" of the Obama administration and says "senior-level attention" to this issue is crucial. To advance this priority, the Information Sharing Council (ISC) is being integrated into the Information Sharing and Access Policy Interagency Policy Committee (IPC), so that the "important work of the ISC will move forward under the auspices of the Executive Office of the President." The position of Senior Director for Information Sharing Policy has been established within the EOP. The Senior Director will be the Chair of the IPC and will lead the interagency policy process and identify information sharing and access priorities going forward. Second, the White House has initiated a comprehensive review of information sharing and the ISE, which the Markle Task Force recommended as a key step to ensure Government-wide focus and coordination. Third, Mr. Brennan notes that the importance of effective information sharing extends beyond exclusively terrorism-related issues.

The Markle Task Force takes heart from these early actions by the White House, which are largely in line with the Task Force's recommendations. Although the Task Force supports these efforts, we believe that it is imperative that the IPC and its Chair have adequate horsepower to drive interagency coordination at a senior level. As a general principle, the White House must assert strong sustained leadership across all agencies with a National or homeland security mission to assure that there is effective information sharing. Senior leadership from within the EOP will ensure Government-wide authority to coordinate the policies and procedures necessary for effective information sharing, and provide the policy clout necessary to overcome the bureaucratic resistance and turf wars that stymie progress. Otherwise, wasteful duplicate efforts are inevitable as individual agencies try to address information sharing independently. Congressional oversight will be critical to ensure that Government-wide efforts are being coordinated effectively.

It is our understanding that the administration is considering several possible structures for information sharing to leverage the accomplishments of the PM–ISE and recognize the role of the Chief Information Officer in the ODNI and other agencies. There are a variety of possible models, including: (1) An approach similar to the Director of the Office of National Drug Control Policy, (2) expanding the PM–ISE's mandate and making him the Co-Chair of the IPC, or (3) giving the Chair of the IPC greater authority.

It is critical that the official charged with leading Government-wide coordination of information sharing policy: (1) Have the President's clout behind him, and (2) be responsive to Congress. Many believe this official should be appointed by the President and confirmed by the Senate. This will ensure accountability to Congress, like other Senate confirmed officials in the EOP, such as the Director of the Office of Management and Budget or the Associate Director and Chief Technology Officer in the Office of Science and Technology Policy. Congressional oversight is essential to the success of information sharing because the oversight process can help ensure that the individual charged with making information sharing a reality is held accountable for producing measurable progress toward a safer country. In addition to improving oversight, a Presidentially-appointed and Senate-confirmed position will have increased policy clout, providing the necessary horsepower to drive interagency coordination.

Moreover, serious consideration should be given to providing some budget authority to the official charged with leading the Government-wide coordination of information sharing. Budgetary certification authority would greatly increase the official's ability to ensure that agencies are adhering to the administration's information sharing policies. Similar authority has been granted in other contexts to officials such as the Director of the Office of National Drug Control Policy.

Broadening the Scope of Information Sharing.—In light of the current financial crisis and growing budget pressures, we need to do more with less. An effective information-sharing framework is not only important to protect against terrorism; it can make the Government more effective in areas like energy security and preventing a full blown H1N1 pandemic this fall. Mr. Brennan's memorandum acknowledges the need to expand the scope of information sharing beyond just terrorism information. The lessons learned from National and homeland security information sharing should be applied—under White House leadership—to other Federal responsibilities, such as air traffic control and health care. Congress should carefully examine the potential for broader implementation of ISE best practices in order to improve information sharing in other areas beyond terrorism. Broader implementation will create an on-going need for a senior official at the White House to drive effective information sharing from the top by continuing to maintain pressure on agencies to effectively share information.

III. ALL GOVERNMENT INFORMATION RELEVANT TO NATIONAL SECURITY SHOULD BE DISCOVERABLE AND ACCESSIBLE TO AUTHORIZED USERS WHILE AUDITED TO ENSURE ACCOUNTABILITY

The PM–ISE's annual report focuses on developing infrastructure and technology that can help make accessing and sharing information easier. However, we believe greater attention should have been given in the report to data users and how they can find and access information. Intelligence Community Directive 501 (ICD 501), which was signed on January 21, 2009, mandates wide-ranging actions to promote information sharing throughout the IC. ICD 501 is not discussed in the PM–ISE's report. Connecting the PM's work with ODNI's efforts on ICD 501 more effectively could yield best practices with broad applications throughout the Government. Specifically, the Obama administration needs to take two steps—(1) Greater emphasis must be placed on discoverability, and (2) the PM–ISE's determination regarding the feasibility of an authorized use standard should be reassessed in light of ICD 501.

Greater Emphasis on Discoverability.—As discussed in detail below, the Obama administration and Congress should consider adopting a policy that requires all agencies with a National or homeland security mission to make their data discoverable. Discoverability is a critical precursor to effective information sharing; making information more accessible will help only if users are able to discover what information is out there and who has that information.

The traditional information-sharing model requires either the sender to know what information to send to whom ("push") or requires the end-user to know who to ask for what ("pull"). Whether push or pull, there are too many doors on which to knock. The chances of the right data holder and the right end-user locating each other and sharing the right information are slim at best.

Discoverability through the use of "data indices" is thus a critical precursor to an effective system of information sharing. These indices serve as a locator service, returning pointers to data holders and documents based on the search criteria used. Information not registered in data indices is essentially undiscoverable. Think of data indices as a card catalog at a library, where every aisle of the library is the equivalent of an isolated information silo. Without a card catalog to provide users with pointers to the location of books, users would be left to roam the isles in the hopes of finding a relevant book.

The technology to give users the ability to discover data that exists elsewhere is readily available. However, in order to make data discoverable, each agency needs to tag its data at the point of collection with standardized information that can be indexed and searched. Many agencies do not adequately tag and index their data, so it is not readily discoverable, which undermines not only an agency's ability to share the data with others, but also the agency's ability to share within its organization. The DNI recently took an important step towards implementing such a system by signing ICD 501, which requires all IC agencies to make all information collected and all analysis produced available for discovery by automated means.

ICD 501 only applies to the IC. An effective information sharing framework will require increased discoverability across the Government, so that data users will be able to find and have access to information across agency lines. Therefore, the Obama administration and Congress should place a high priority on broader discoverability as the first step toward effective information access. The technology is readily available—all that is needed is Government-wide policy guidance and implementation. The administration should establish a policy that requires all departments and agencies with a national or homeland security mission to: (1) Tag their data at the point of collection; (2) contribute key categories of data (e.g., names, addresses, passport numbers, etc.) to data indices; and (3) follow through on implementing widely available means to search data indices.

We are pleased that the PM–ISE's annual report discusses creation of output-related goals and metrics, such as the ISE Maturity Score Card. The administration should build on these metrics by adopting more concrete outcome-oriented metrics. One of the first metrics should focus on discoverability because data indices are an essential precursor for effective information sharing. This metric should measure what percentage of an agency's data holdings have been registered in the data indices directory. Additionally, just as the private sector uses Quality Assurance scenarios to test the performance of critical system requirements, the administration should conduct on-going tests across Federal, State, and local organizations to determine how the ISE scores according to certain critical system requirements.

The Feasibility of an Authorized Use Standard Should be Reassessed.—Improved discoverability must go hand-in-hand with a trusted system that will facilitate access to the data indices and the information to which these indices point (in the library analogy, access both to the card catalog and the book itself). An authorized use standard provides a model for such a system. Under such a standard, a Federal, State, or local agency or its employees obtain mission-based or threat-based permission to discover, access, or share information, as opposed to the current system which relies on originator control limitations, U.S. persons status, and place-of-collection rules.

Congress asked President Bush to consider adoption of an authorized use standard in the 2007 9/11 Commission Recommendations Implementation Act. The PM–ISE discussed what he viewed as potential obstacles to implementation of an authorized use standard in his 2008 Feasibility Report. The report concluded that an authorized use standard was not feasible. Yet none of the objections in the report were technical in nature; commercial off-the-shelf technology enables the use of such a standard and can address perceived obstacles such as identity management. Moreover, an authorized use standard would not require amendment of statutes, such as the Privacy Act, and it would be in full compliance with the vital principles underpinning the constitutional, statutory, and regulatory requirements currently in place.

We believe the PM–ISE's determination that an authorized use standard is not feasible should be revisited in light of ICD 501 and pilot projects that are testing these concepts in the field. The IC has started down the path toward phased implementation of an authorized use standard with ICD 501. ICD 501 incorporates many principles from the Markle Task Force's previous work on authorized use. For example, ICD 501 requires that information collected or analysis produced must be available to authorized IC personnel who have a mission need for information and an appropriate security clearance. As part of ICD 501, the National Security Agency has designed a new collaborative system that will link disparate intelligence databases to support field operations in Iraq and Afghanistan. This system, which is currently in testing, is designed to address the challenge of providing data gathered from multiple agencies to authorized users based on different privileges. It represents a good first step that indicates that implementation of an authorized use standard is feasible.

Other organizations are also undertaking pilot projects that will test the Markle Task Force's recommendations. As the subcommittee knows, the Project on National Security Reform (PNSR), led by Jim Locher, is working on the issue of improving national security decisionmaking. I am privileged to serve on the "Guiding Coalition" for PNSR and am pleased to advise the subcommittee that PNSR has adopted not only the spirit of the Markle Task Force's approach to information sharing, but also many of our specific recommendations. PNSR has been exploring with several Government agencies the possibility of a pilot project that would incorporate the basic elements of a fully integrated information sharing system. I hope that the administration will conduct such a pilot project, and I encourage this subcommittee to support this pilot project and to monitor its progress. Such real-world tests can help reassess the feasibility of an authorized use standard.

IV. INCREASE PRIVACY PROTECTIONS

As detailed in the PM–ISE's annual report, the PM–ISE has issued ISE privacy guidelines and the ISE Privacy Guidelines Committee has published a "Privacy and Civil Liberties Implementation Workbook" and several associated documents, such as Policy Development Tools and Privacy Policy Outlines, to help agencies implement their own privacy policies. These are a good first step, but much more remains to be done to develop policies to assure both the public and Government officials that privacy and civil liberties are protected while information is shared. Clear, detailed, and consistent policies are necessary to protect privacy and civil liberties.

Few agencies have produced privacy policies to date because there is little incentive for them to do so. Of the 17 agencies that were supposed to develop their own privacy policies, only three have produced such policies, a paltry 18 percent. By way of comparison, State fusion centers are required to submit privacy policies by a certain deadline in order to receive Federal grant money. Of 70 fusion centers, 80 percent have submitted policies. ISE agencies should be given a 30-day deadline to submit privacy policies to the PM–ISE for approval, and failure to meet deadlines should result in concrete penalties—including loss of funding.

Moreover, merely having a privacy policy is not enough. To date, the PM–ISE guidelines and associated documents are more advisory than directive—they tell the agencies to address various privacy and security principles, but do not tell them how to do so. A comprehensive privacy policy must provide direction and consistency on hard issues. Yet the PM–ISE guidelines do not address many of the most challenging issues. For example, the guidelines state that all agencies must comply with the Privacy Act, but they do not address many of the difficult questions about who gets what information for what purpose under what standard of justification.

The Obama administration should promulgate Government-wide policies on privacy and civil liberties that provide consistency and direction on hard issues while allowing agencies the flexibility that their different missions and authorities require. Such a policy should address: (1) Auditing of both data quality and data flows; (2) enhanced fidelity of watchlists; (3) deployment of access and permissioning systems based on carefully defined missions and authorities; (4) clear predication for collection and retention of data; and (5) redress systems that offer a meaningful opportunity to challenge adverse action and that ensure that corrections or qualifications catch up with disseminated data.

The President and Congress should also act within the next 60 days to nominate and confirm members to the Privacy and Civil Liberties Oversight Board. Congress re-chartered the Board to strengthen its independence and authority, but the new Board has never come into existence. The statutory charter for the new Board gives it a role both in providing advice on policy development and implementation and in reviewing specific programs.

Finally, the ISE should take advantage of technological tools to minimize the risk of unintended disclosure of personally identifiable information. In his March 2008 Feasibility Report, the PM–ISE found that although data anonymization has the capacity to improve privacy protections, it was technologically infeasible. This determination should be revisited in light of technological advances. There are now a number of commercially available technologies, including anonymization, strong encryption, and digital rights management, that can help protect privacy and civil liberties as well as information security. Moreover, both privacy and security protections can be enhanced through the decentralized approach to discoverability outlined above because this approach avoids bulk data transfers minimizing both privacy and security risks. When locator and topic information are transferred to the index, the underlying information isn't transferred until the user requesting it is authorized and authenticated, reducing the risk of unintended disclosure.

Building the information-sharing environment should entail the development of new and more powerful privacy protections. But existing guidelines do not require agencies to provide any more protection than they already offered. Much work is needed in this area.

In conclusion, Madame Chair, it has been a privilege for me to appear before the subcommittee today. I commend this subcommittee for its leadership on these issues. Sustained leadership is vital because a waning sense of urgency in the nearly 8 years since the 9/11 attacks means that old habits of withholding information are returning. The United States must not become complacent about improving information sharing in the face of the current financial crisis and in the absence of a new attack. This subcommittee has a critical oversight role to play in order to ensure that measurable progress is made on information sharing.

Much more needs to be done. Now, at the start of the Obama administration, is the moment for breakthrough progress on information sharing. The Markle Task Force will continue to work with Congress and the Obama administration to find practical solutions to the critical homeland security issue of information sharing. The Task Force has concrete recommendations for steps that can be taken today to ensure that decision makers at all levels get better information so they can protect the Nation. Our recommendations are neither complicated nor technically difficult. They require attention to implementation and strong, sustained leadership.

It is important to have a public dialogue about this vital issue. I would like to thank the subcommittee for having this hearing to facilitate that essential dialogue. I look forward to working with you and am happy to answer any questions you may have.

Mr. CARNEY. Thank you Mr. Smith.

I want to thank all of you for your testimony. Its length is only an indication of its importance, so we really wanted to drill down into the issues you raised.

I will remind each Member that he or she will have 5 minutes to question the witnesses, per round. I will now recognize myself for 5 minutes.

Mr. Ambassador, you offered in your testimony to share your personal observations. Please, that is my question to you; please share those observations.

Mr. MCNAMARA. Thank you, Mr. Chairman. I can be very brief. There are five points I would like to make.

One, I believe the PM should be a Presidential appointee who reports to the White House and the Congress, independent of any agency, as an honest broker. I think this is critical, and it is the one role that we have been able to perform which has, in fact, loosened up some of those cultural rigidities and enabled us to act in the successful, I believe, manner that we have.

Second, the Program Manager needs to be a senior official with extensive interagency experience and a recognized ability and stature to manage major bureaucratic issues. This is important because, in fact, the Program Manager works 90 percent of the time with the interagency. In fact, it is an interagency job. Every aspect of information sharing crosscuts different agencies so that there is no one agency that I go to and expect to get full implementation of these crosscutting issues. They are all multiagency issues.

Third, we need to strengthen, I think, the effectiveness so that the Program Manager, in addition to being the Program Manager should, I believe, be the Chair of the White House Interagency Policy Committee on Information Sharing that reports to the deputy committee.

Fourth, I think the PM Office should continue until the ISE is fully mature. Although it exists and is functioning it is not fully mature yet. Also it should remain until the ISE is well-anchored in State and local government practice and do all of this in as brief a period as possible.

Fifth and finally, at full maturity, I want to point out that the ISE functions will not end. What will come to an end, I expect, at full maturity is that the office will go out of existence, but the functions will be institutionalized in agencies throughout the Federal Government, and those agencies will be acting as Executive agents carrying out the functions that are now being performed by the PM–ISE Office.

That has, I think, already begun. If you take a look, we have turned over to NARA, that is the Archivist of the United States, the CUI function. That function is being performed primarily as an executive agent by NARA.

Suspicious activity reporting, we expect, as I mentioned, to bring that to maturity in the next 6 months to a year. I expect that the Department of Homeland Security and the Department of Justice will be able to take on that function.

The other functions—fusion centers, privacy, and civil liberties—remain to be institutionalized. As they are institutionalized, as I see it, the agencies will act as agents for the Federal Government working with the State and locals. Those, I think, are the answer to what is the future of the Program Manager's Office.

Mr. CARNEY. I appreciate those observations. One question that kind of popped in mind immediately was, in your opinion and based on your experience, how long for maturity? What sort of time frame are we looking at?

Mr. MCNAMARA. I have been asked that several times in recent weeks especially.

It is difficult for me to put a specific time frame on it. What I can say is that I believe we have gone just beyond the tipping point recently; that is to say we are not going back to the old way of doing things. That is not an option.

The option is to move forward. The tipping point having been reached, there are several paths to go forward, and there is not just one solution. I think we are about roughly halfway toward that maturity level.

Now, since it has taken us 3, 3½ years, and we are halfway there, one might imagine another 3, 3½ to do it. But I think, as has been mentioned here and certainly has been mentioned to me, the train left the station rather slowly. I would say that of that half that we have now accomplished of getting towards full maturity, fully half of that was done in the last year. So we are picking up momentum, we are moving faster. Therefore I would hope it would not be a full 3, 3½ before it comes to full maturity.

I welcome the incoming administration, the current administration's immediate and vocal support for this as a priority. I also, by the way, want to say how much I appreciated the support I got from the former administration throughout my 3½ years as they built with me and with the State and local and private sector people the foundation phase of the ISE. We have completed the foundation phase; now comes the final push to maturity.

Mr. CARNEY. I appreciate that so much.

I now recognize the Ranking Member from the subcommittee, the gentleman from Texas, Mr. McCaul, for questions.

Mr. MCCAUL. I thank the Chairman. I would like to ask some questions about the program managers—some of the current authorities.

But before I do that, I would like to ask Colonel Fuentes: The example of the hijacker, a 9/11 hijacker, was mentioned in the opening statements. He was on a CIA watch list, was pulled over by a State trooper, obviously was not forwarded.

Would that be—how would that be different in today's scenario under this new program?

Mr. FUENTES. Well, there is a database that is routinely checked when you do an NCIC, National Criminal Information Center inquiry, which is pretty routine on a motor vehicle stop. It is called a VGTOF. It is a database that has violent criminals, gang members in it, including the terrorist watch list.

So notification would be near instantaneous if that was run. Then there would be guidance that would be provided to the police officer or to the trooper to hold that person possibly for additional inquiry, perhaps by a member of the Terrorism Task Force, or simply to note a location, a license plate, a name, other occupants that are in the vehicle.

But that police officer would now be guided in ways that were probably unimaginable prior to 9/11.

Mr. MCCAUL. So you feel very confident if that type of person was pulled over today they would be detained?

Mr. FUENTES. My confidence is building every day, sir.

Mr. MCCAUL. The suspicious activity reporting, how is that working?

Mr. FUENTES. Well, the suspicious activity reporting is a very good initiative that really looks at what are the routine activities that a police officer does every single day.

Responding to a report of somebody taking photographs of planes taking off at an airport: There could be a completely normal reason for doing that and there may be a nefarious reason for doing that. That information is captured when a police officer responds, it goes into a records management system; and then, prior to the initiation of the SAR, it would have languished, it would have simply been part of that records management system. Now, with the SAR process, that information is captured in that records management system by the fusion center and it is compared to other records management systems.

So that car that might have been sitting, for instance, taking pictures of a refinery on the side of the New Jersey Turnpike 2 days later also comes up in the record, perhaps another record in another county or another municipality of being next to another refinery. So when you put those two things together, interest in that individual heightens considerably. Maybe they are writing a book or maybe they have, you know, another motive that the police need to take a look at.

That is the purpose of the SAR, to use the information that is routinely developed over the course of a police officer's shift and then collate and compare that within the records management system to see if there is any behavior that you should be taking a look at.

Mr. MCCAUL. Thank you. My time is limited. I don't know if we will have another round of questions, but I do want to talk about the Program Manager authority.

Ambassador and Mr. Smith, if you would like to weigh in on this, your authorities are set forth in section 216 of the Intelligence Reform and Terrorist Prevention Act, yet section 218—1018 seems to take away a lot of that authority, abrogate a lot of that authority.

I wonder if you could comment on that, in the future the Program Manager having more authority; and also, how is that going to—how is this position going to work in conjunction with now the new position of senior director for information sharing policy within the Executive Office of the President?

Mr. MCNAMARA. Well, let me quickly answer the second question because my answer is that I really don't know how it is going to mesh, because the White House is the one that is going to make the decisions and the calls on that and not I.

However, the senior director for information sharing and information issues is not entirely new since there was one in the outgoing administration also. But this one has taken on—appears to be taking on a higher role and a more pronounced role. But I really don't have the answer to that because no announcements have been made as to what the structure is, and I am not involved in that aspect of it.

Quickly, on 1016 and 1018, indeed, as you note, the authority on 1016 seems to be quite strong, but there is 1018 which says that this shall not interfere with existing authorities, and then it lists a whole bunch of agencies and agency heads. The result is that the Program Manager is less the manager of the ISE than the negotiator and conciliator and kind of compromiser to produce the ISE.

One area that I think—as I mentioned in my list of things that needs to be done, I think the Program Manager needs to have a much stronger role in the budget process. Right now, as a result of our cooperative approach with OMB, we do get an insight into the budget process on information sharing issues and how the budget is being used by several of the agencies to implement information sharing initiatives, but it is a partial look at a partial number of agencies. We are not—we don't have a regular seat at the table when it comes to budget issues. I think that is something that needs to be done.

Mr. MCCAUL. I see my time has run out, but let me just make a final comment.

I think and recommend to the Chairman that we look into both these statutory provisions to see if there are changes we can make to strengthen the role of the Program Manager. Ambassador and Mr. Smith, I look forward to your recommendations as to how we can achieve that.

With that, I yield back.

Mr. CARNEY. I would like to assure the gentleman we will have at least one more round of questioning and continue with this. It is something that we can do from the Oversight Investigations Management Subcommittee as well.

I will now recognize other Members for questions that they may wish to ask the witnesses. In accordance with committee rules, I will recognize Members who were present at the start of the hearing based on seniority on the subcommittee, alternating between Majority and Minority. Those Members coming in later will be recognized in the order of their arrival.

I now recognize for 5 minutes the gentleman from Texas, Mr. Green.

Mr. GREEN. Mr. Chairman, I would yield to Mr. Pascrell and assume a later position.

Mr. CARNEY. Without objection, so ordered.

Mr. Pascrell for 5 minutes, please.

Mr. PASCRELL. I thank the gentleman from Texas, and thank you, Mr. Chairman.

Ambassador McNamara, I want to thank you for your service. You have really moved us down the field to what we want as a truly integrated system in this country. We still are part of the problem, this side of the table and throughout the Congress, in that the Secretary, your very boss over the last 3½ years, can still be brought before 108 different oversight committees in the House of Representatives. We are not moving off that dime, and that is why we are stuck.

This committee I know wants to move forward, but again it is only one of the committees. We created the Department of Homeland Security. When we did that, it was done with the idea that we could house all our critical domestic security agencies under one roof; and in that environment, we would have the kind of information sharing between the agencies that we feel could have prevented the 9/11 attacks.

Unfortunately, the lack of information sharing, not only between different agencies but within agencies, continues to be one of the biggest problems we face in the Congress.

Colonel Fuentes, you know that I am really proud of what you have cited today, because New Jersey is really a role model in terms of State agencies throughout the country on the forefront of providing bottom-up intelligence and operations. You have made that a core of the operation, yourself and Homeland Security Director Richard Canas. It makes the State of New Jersey's Homeland Security infrastructure so effective.

There are some things, Mr. Chairman, we do well in New Jersey, and there are some things we are trying to improve upon.

Colonel Fuentes, can you talk more about how information is shared within the State of New Jersey and how this is an integral part of Governor Corzine's State-wide crime plan? I would appreciate if you could especially hit upon two effective programs—I think they are effective—in our State: the New Jersey Data Exchange, New Jersey DEx; and the suspicious activity reporting, NJ–SARS; and finally how do you think we can best apply these practices on the Federal level.

Mr. FUENTES. Well, we are a small State with a lot of police departments, so we are shoulder to shoulder. Everybody knows everybody; that makes the environment a little bit easier.

Although the State is not a large State, there are 479 full-time police departments and 21 county prosecutors' offices and 21 county sheriffs' offices. That is a lot of information that needs to be collected. Our fusion center has operated as a junction box, so to speak, for pulling that information in.

But mostly the purpose of every fusion center, incidentally, not just ours, is to produce tactical and early warning products on issues that are of imminent concern. That is always going to be first and foremost: Terrorism.

New Jersey is a 9/11 State. New Jersey State Police have lost three troopers in the last 30 years in shoot-outs with domestic terrorist groups. The case that almost never gets mentioned is the 1988 arrest of Yu Kikumura, a member of the Japanese Red Army, on the New Jersey Turnpike, arguably the first attempt of attack on this country by an international terrorist group.

In addition to that, on 9/11, we lost communications to our force in the entire north part of the State.

So the experience of terrorism is not one that is certainly lost on us. So the idea of putting a fusion center together actually occurred right after 9/11, and it evolved to where we are right now with a great deal of Federal help and partnership and a lot of advice by the two gentlemen that are to my left and to my right.

I mention homeland and hometown security because, if you are aggressive on crime and criminal enforcement, you are going to develop the information that could get you to the terrorist plot.

You mentioned NJ–DEx, Congressman. That is in line with the National Data Exchange program at the Federal level, which is pulling together information from the States, you know, to the Federal agency. What we did in New Jersey is—and we are in the process; this is evolving—is to have a Google-type search with appropriate security clearance to police agencies, police officers, troopers who can run a name both for deconfliction purposes and to see if anybody else in the State may be working an investigation, a criminal investigation, that would aid their own.

We went up on this program literally months ago and just recently dumped 300,000 investigation reports, complete with narratives, into that database; and now two counties in New Jersey have done the same, and we are looking to build that through 21 counties. So that program is a very, very robust program and is one that I think is going to produce a lot of results in terms of reducing crime in the State of New Jersey.

You mentioned the SAR program. The SAR program—and the Ambassador can certainly tell you a great, you know, more about that program—has been used in a number of other cities, I think perhaps as many as 40 or 50 up to this point. New Jersey is just beginning to come on line with that program.

One of the places we are taking a look at employing that is actually Atlantic City. In the aftermath of both the Mumbai and the Jakarta attacks, we are very sensitive to the fact that we have 14 casinos in Atlantic City, and making sure that there is proper communication between those casinos. That information of suspicious activity in each one comes into the fusion center and that is compared to the others to see if we can produce lead value information.

So we are excited about both the programs that you mentioned, and they are evolving, and I think are going to hold great promise for the future for us and the State.

Mr. PASCRELL. Thank you, Colonel.

Thank you, Mr. Green.

Thank you, Mr. Chairman, for your courtesies.

Mr. CARNEY. Of course.

The Chair now recognizes for 5 minutes my good friend from Pennsylvania, Mr. Dent.

Mr. DENT. Thank you, Mr. Chairman. For the record, I want it to be known, I do love New Jersey. My mother-in-law is from Phillipsburg. When New Jersey does things well, we consider New Jersey part of greater Pennsylvania, I just want you to know that. Seriously. I had to get that off my chest.

Ambassador McNamara, what do you see as the next steps for this whole Information Sharing Environment, this ISE? What do you think the Obama administration plans are for ISE?

Mr. MCNAMARA. Well, once again, on the second question, I would like to leave that to the Obama administration officials who have just come in, who are now getting themselves settled, warming the chairs and taking action. I will leave it to them to talk about that.

I listed my priority areas that I think need to be looked at. Interestingly enough, in my conversations with the incoming administration, they seemed to have roughly the same priorities as I just listed. I think it is important that we look at this—and let me very briefly refer back to Congressman Pascrell's remarks about the problems with crosscutting issues, as I refer to them.

Both—I think both the Executive Branch and the Congress need to restructure the manner and the way they handle crosscutting issues. You have—in the administration, agencies get the authority, agencies get the funding. When someone like me comes along, or the individual who runs—is supposed to run and is running the cybersecurity program or a whole range of other crosscutting, interagency issues, we are appealing to agencies to do what is in the common good.

But the agency has its own missions, its own perspectives. Each agency—I am dealing with 17 of them every day of the year for the last 3½ years, 17 different agencies who have agency missions that they have to accomplish. Their budgets are limited, and for them to move their budgets the way I want them to move it is not easily done. Crosscutting issues, it seems to me, have got to be dealt with by the Executive in a different way.

I think also the committee system in the Congress leads to agency focus and agency attention. It doesn't address crosscutting issues in the way that it needs to be done. Now, I don't know exactly how one would restructure the crosscutting issues that the Executive Branch has to deal with, nor would I suggest—I am not expert enough to suggest—how the Congress should adjust its structures.

But it seems to me that in this 21st century these crosscutting issues are becoming more and more numerous. I cite as an example of that, in a demonstration of the truth of that, look at all the so-called "czars" that keep popping up downtown. They are not really czars; they are like me. I have been referred to as the "information sharing czar," and believe me, I am not a czar; I am almost a petitioner at times.

Because the agencies are the czars, just as the committees are the czars up here.

Mr. DENT. Can I just follow up on that line of thought?

So then, what kind of incentives or, in some cases, penalties are in place for organizations or individuals to encourage or reprimand actions, you know, to bring about a greater sharing of security-related information?

Mr. MCNAMARA. Well——

Mr. DENT. If there aren't any incentives or penalties, should there be?

Mr. MCNAMARA. There are some, but they are relatively weak incentives as compared with the incentives to fulfill the agency's main mission, which may not be information sharing, although information sharing underlies much and many of the agency missions.

What I think needs to be done is that a shift in the manner in which resources are allocated needs to be done.

If you are going to have a crosscutting issue such as information sharing, such as cybersecurity, such as—well, you name it, they are out there. There are dozens of them, drugs, et cetera. Then the way the resources are allocated have to take into account, starting with the legislation, in my opinion, and going on through the administrative allocations in the Executive Branch, have to take into account crosscutting issues; otherwise, the noncrosscutting issues will get priority.

Mr. CARNEY. Thank you.

The Chair now recognizes the gentleman from Texas for 5 minutes, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman.

I thank the witnesses for appearing.

I would like to, because he is retiring again, thank Ambassador McNamara for your services.

Sir, you may not and you probably would not want to be referred to as a kingpin, but you clearly are a linchpin in this process. You have become sort of the glue that has bonded a lot of our intelligence services together, and I thank you very much for your service to your country.

My suspicion is that this is not the last time we will see you. My suspicion is you have a lot of productive years ahead, and we will find you back in Government services at some point. Although I don't want to speak for you; that is just my suspicion.

Now, let me speak, if I may, quickly to Mr. Smith. Mr. Smith, I have information on you but very little on the foundation. Can you tell us just briefly a little bit about the foundation?

Mr. SMITH. Of course. The Markle Foundation is headquartered in New York. It is chaired by Zoe Baird, and has been—it is a foundation that has been in existence since the mid-1930s. The task—among it is other achievements are, it has done a lot of funding for Children's Television Workshop. In fact, Big Bird is one of their creations.

The Task Force on National Security in the Information Age emerged after 9/11 when Ms. Baird and Jim Barksdale of Netscape got together and decided that something needed to be done, and the task force was created. Most of us have volunteered our time. We have issued now four reports over the years and, frankly, are pleased at the reaction that our reports have gotten.

Mr. GREEN. Thank you.

To the Ambassador and to you, Mr. Smith, the Privacy and Civil Liberties Oversight Board, the first question is, has that board come into being in the sense that we now have it staffed and we have appointees to it?

Ambassador, I will start with you.

Mr. MCNAMARA. The board came into existence. It did have members and a staff, but it, for reasons not completely clear to me, sort of became inactive within 6 months to a year of its standing up. I believe now there are no members actively engaged and the board is moribund.

Mr. GREEN. Can you briefly tell us what the function of the board was or should be?

Mr. MCNAMARA. Yes. It was briefly to be an independent reviewer of the policies relating to privacy and civil liberties throughout the Government, and it was to act as—I have referred to it several times as kind of the Good Housekeeping Seal on privacy and civil liberties policies as practiced by the Federal Government.

Mr. GREEN. Do you see worth in this board?

Mr. MCNAMARA. I see enormous worth in that board.

One of the problems that I have had in dealing with privacy and civil liberties issues is when I have put forward policies and issued them, it would have been easier and I think more credible if I could have submitted those policies to this board and had them comment on it. We could have made changes, adjustments, et cetera, and then had them endorse it in effect; tell us that, okay, that is fine, go ahead and issue it.

Mr. GREEN. I am running short of time, and I apologize.

Mr. Smith, do you have comments that you would like to make about the privacy and oversight board?

Mr. SMITH. Yes, Mr. Green. I think it is critical that the President promptly name people and that the Senate confirm them. The problem is, in the last administration, some of the people that had been named got tangled up in confirmation issues on the Senate side.

I think it is critical that this board be named and that it be very active. So I encourage this committee to keep the heat up.

Mr. GREEN. Thank you.

I have many other things, but I want to go to you, Colonel, to be fair to everybody, make sure everybody has a chance to say something. You had two observations that you wanted to make. Did you have an opportunity to make the observations?

Mr. FUENTES. Basically, everybody has a copy of those opening remarks, which basically just describe some of the function of the two most important components in the fusion center, and I would—I certainly don't have to take up the time here.

Mr. GREEN. This is your opportunity, tersely and concisely.

Mr. FUENTES. I have already sort of inferred to what the analysis element does. That is really where the fusion takes place in the fusion center. That is a very collaborative environment involving a lot of Federal partners, DHS, FBI, Coast Guard, DEA, ICE. There are no shoulder patches, and there are no egos in that group.

Every morning they get together at 10:00 a.m. They have a huddle. They talk about what everybody knows from their respective agencies. They figure out what the priorities should be for the day, and especially if any information that is being generated in that meeting should be disseminated very, very quickly out to the law enforcement partners, to fire departments, wherever, in the State of New Jersey.

Most of the initiatives that I mentioned that Congressman Pascrell brought up, New Jersey SAR, NJ–DEx, NJ Trace, which looks at weapons that are recovered in crime, the gang work analysis that gets done up there, plus products that may relate to international or domestic terrorist investigations, Mumbai.

One case in point, without being asked, the fusion center in a couple of days put together a product, "What Does the Mumbai Attacks Mean to the State of New Jersey and the Infrastructure That is in the State of New Jersey?" Certainly instructions to tactical teams, police teams who may have to respond to these events. As you certainly all know from Mumbai, there was a secondary ambush that was set up on those responding teams.

In every single one of these events, there is a lesson to be learned. The fact that we are sitting in little old New Jersey and not in some other place of the world that experiences this more, the lessons of what goes on around the world are very, very important to us, and that is really the essence I think of information sharing and the best thing that we can get out of it.

Mr. GREEN. Thank you, Mr. Chairman.

I yield back.

Mr. CARNEY. Thank you.

The Chair now recognizes the gentleman from Indiana, Mr. Souder, for 5 minutes.

Mr. SOUDER. Thank you.

Part of the reason I am on this committee is I was working to coordinate narcotics efforts before 9/11, and this, Homeland Security, has become a lot like narcotics in stovepiping and laying another over in effect.

A friend of mine sent me a joke about Congress seeing a scrap yard in the middle of the desert. We hire a watchman. Then we decide the watchman needs training, and so we hire people to train him. Then he needs pay, and so we hire people to pay him. Then we need people to write the reports on all that. Then we need to have supervision over that and how he is going to interrelate. Then we decide to cut the budget and lay off the watchman, but the bureaucracy is there.

Sometimes in homeland security and in narcotics, it seems to me we keep layering. Part of the goal here is how to enforce it. There are some fundamental things in here, some that we have touched on. We have tried in Congress in the Drug Czar to give him the ability to decertify the budget, but no Drug Czar had the courage to do it because they have to get along with each agency. Afterwards, he doesn't have as much line because it is a staff like a czar. We have tried red-flagging.

That would be one way to give each kind of czar person the ability to put some kind of red flag that they are not meeting their criteria, which would be less than complaining about the budget. We have tried oversight in the Government Reform and Oversight grade cards. But that is hard to do if you don't have inside people leaking information to you, and then they tend to get destroyed in whistle-blowing even with the protection because you want to move up and not do that.

But, clearly, we have to find a way to do this, because it is true in Education. It is true in National Parks. It is true in every category of government, this crosscutting of different agencies. But it is really severe here, because Homeland Security has a big share of narcotics and immigration, which is really—and traditional Customs, which is really the bulk of what they do.

The No. 1 priority is prevention, which is a whole lot riskier and harder than trying to catch criminals, because you are dealing with more gossip, basically high-level gossip, trying to speculate and put pieces together that haven't occurred yet. The New York HIDTA is probably the best, where New Jersey and Connecticut and New York pulled together and basically have a terrorism and narcotics working together there. But now, when we lay these fusion centers over, and the fundamental question, because I am wondering how they are interrelating with OCDEF and HIDTAs and so on, all of which have two-thirds overlapping missions.

When we come here and say, let's change the need-to-know to share, and we move into terrorism—and we already have been having these problems for financial reasons—in other words, agencies know if they don't claim the credit in narcotics busts, they may not get funded by whoever is funding them. You have ego questions.

But when we get into terrorism, it is even harder, because here we are getting, the more you proliferate, the more you potentially risk and burn your source, who may in fact get killed, much like being in narcotics in the Mexican border. For example, it may expose, even just saying—describing somebody, when you put it on a notice, it may suggest to—if it leaks out, what phone you have to have, what information you have. Plus, a lot of it is gossip. It is kind of like a background check on people when they had that stuff leaked.

I would like to have each of you briefly describe how you ever think we can move from the practical need-to-know and sharing, particularly as something as risky as terrorism.

Mr. FUENTES. Yes, sir. As far as OCDEF, the terrorism task force, the HIDTA groups, that relationship is very good in the State of New Jersey. I have personnel that are assigned in large numbers, actually, to all of those entities. Their representatives in the fusion center basically hook into the databases that are proprietary to them.

You said something about information and the sharing of information. When there is terrorism information, incidentally, that should be the first filter that every single bit of information should go through first, whether it appears to be criminal or not.

My first concern is always going to be, when information comes in, what does it mean to the State of New Jersey? How do I have to redeploy my personnel to somehow counter that threat?

I will be honest with you; I don't need to know techniques. I don't need to know tactics. I don't need to know methodologies, how you got that information and where it might have come from. I just sort of need to know the bottom line, not what is below the tear line, for lack of a better term. That may be the accepted term. I want the information quick, and we want to be able to push it out quick.

I think, recognizing that, in a number of fusion centers and especially in the discussions that have occurred, whether it is in the global committee, IACP committees, the PM–ISE, is that there is a sensitivity to that.

You know, classification of information has been a concern of fusion centers and how you can get your hands on things that you need. We are not quite there yet. I think Ambassador McNamara referred to that. But I think we have come a long way. That information gets to us pretty quickly. I know that it is juggled elsewhere, and thankfully, I don't have to deal with that.

Mr. MCNAMARA. If I could just say a word or two on that. No. 1, the information that is most generally used and shared is not information that reflects on or leads to dangers for methods and sources. That is a very small percentage of the information that gets moved through the information-sharing system. In fact, it is a very small percentage of the information that generally is used by law enforcement, by the intelligence community, and by Federal Government at large.

So it is a problem, but it has been my observation, and that of experts much more knowledgeable than I, that in an information-sharing environment, with the technology geared to provide that protection, we are much better off than we are today, without having an information environment and its accompanying technology functioning for us.

I think the best example of that is the case of Hanssen, who functioned as a spy getting access to information for 15 years, I believe over 15 years, before he was caught.

In an information-sharing environment, I think most experts would agree that Hanssen wouldn't have lasted more than a couple of years because the system would have, through various algorithms and methods used to track the use of the information by Hanssen and his access to that information, it would have registered within the system and been sent to somebody saying, this is out of the ordinary, check it out.

So I am not one who thinks that information-sharing environments mean more information is loosely moved. I think it is more accurate to describe an information environment, the ones that we are trying to build and are building, as more information is more tightly controlled so that it gets to the individuals who need it to get their job done. Technology offers tremendous advantages for moving information. Since we can't go back to the pre-1990 way of handling information, we really do have to move into the 21st century of information management, as I refer to it.

The best example of that is your credit card. It is an information-sharing environment, works world-wide. You only get the information you need to work within the credit card system. The bank gets what it needs. The store where you use the credit card gets what it needs. But they don't get information that doesn't apply to their jobs. There is double- and triple-checking by the system to make sure that the information is not misused. If somebody starts misusing it, the system, the computers tell the humans that there is an anomaly here that needs to be checked.

That is what I see as the information—something parallel. It is not exactly like that, but it is something parallel to that that we need to build in to the Federal Government information management. It goes beyond information sharing. It goes to information security. It goes to privacy and civil liberties rules. It is very broad. It is a complex set of new methodologies for managing information.

Mr. CARNEY. The Chair now recognizes for 5 minutes the gentlelady from New York, Ms. Clarke.

Ms. CLARKE. I want to thank both you, Mr. Chairman and Ranking Member McCaul, for holding this very important hearing, which explores the current status of and future outlook for information sharing, the information-sharing environment.

I want to thank you, the witness panel, for appearing this morning.

This issue is of particular importance to me, because effective information sharing is a critical component of cyber intelligence and cybersecurity, as has been indicated and asserted by Ambassador McNamara in responding to Mr. Dent's question.

As the Chairwoman of the subcommittee to this committee on cybersecurity, the findings, it is important to highlight the findings of both the ISE annual report and the Markle Foundation's report, which only buttresses the results of the President's 60-day cyber review report, which lists information sharing as a key component.

The administration has stated that effective information sharing and access throughout the Government is top priority, and established the new position of the senior director for information-sharing policy within the Executive Office of the President to review current status of information sharing and make recommendations to the President. Certainly, the new senior director will work closely with the new White House cyber coordinator.

So my question is to both Mr. Smith and Ambassador McNamara and regarding the White House priority. One of the recommendations in the Markle Report is to move the ISE into the Executive Office of the President, and the report notes that this change will give the PM–ISE Presidential backing and therefore greater authority.

What additional positive effects would such a move have?

Mr. SMITH. Well, first of all, Congresswoman, I am pleased you raise cyber, because that really is a major threat we are facing, and it is very difficult to get on top of this. So I encourage you to keep focused on that.

We are also pleased that Mr. Brennan's announcement here of about a month or so ago moved this—increased the level of attention that the National Security Council would pay attention to this and the creation of the senior director.

Ambassador McNamara has testified that he believes his position should be Presidential appointment subject to the advice and confirmation of the Senate, and that his successor should also chair the Information Policy Counsel. I think that is a very good idea and worthy of consideration.

I don't think we have a fixed view on what the right answer here is, but the point is that the person should be in the White House, should have a lot of horsepower, should be able to speak for the President. One of the reasons behind the Senate confirmation, on the other hand, was to make sure that the individual was accountable to Congress. When we briefed our report earlier to this subcommittee and to the Senate committee, they were concerned that if this individual were moved into the White House, he or she may no longer be reachable by Congress. We don't think that is a good idea, and I think this is yet to be developed. But these are considerations that we believe ought to be taken into account.

Ms. CLARKE. Ambassador McNamara.

Mr. MCNAMARA. Thank you.

As I have said, I believe that the link between the White House and the Program Manager's office and the functions of the Program Manager is critical. It is a necessary link. It needs to be strengthened, and I understand that the intention of the current administration is to strengthen it.

I think there are two areas where that strengthening needs to be done. One is in the policy role of the Program Manager establishing the policies that will govern and implement the information-sharing environment. Strengthening that is important.

The second area where the strengthening needs to be done is, as I have said before, with respect to the resource allocation process. Those are the two areas where I believe that the Program Manager needs additional support from the White House. But also to be part of the White House process would strengthen the Program Manager's position.

Ms. CLARKE. Do you see any drawbacks to relocating the PM–ISE?

Mr. MCNAMARA. To relocating?

Ms. CLARKE. To the White House authority.

Mr. MCNAMARA. Well, with respect to the authorities to function, I think the White House has a substantial role. If you mean relocating, moving it out from the Director of National Intelligence where it is now located, that is a question for the White House to decide. It is primarily an administrative connection.

I want to take this opportunity, since you asked the question, to say that the three Directors of National Intelligence have been among my strongest supporters over the 3½ years I have been in this job. One of the things we have never had to worry about was the administrative issues and the administrative processes for our office. We have been able to focus on building the ISE because we knew that we were going to get the resources for the functioning of the office, that is, keep the lights lit, pay the employees, make sure the paper clips are all coming in, and make sure the computer systems work. We have gotten that without any trouble, and I think the three Directors of National Intelligence have been extraordinarily supportive of us.

Ms. CLARKE. Well, thank you.

I yield back, Mr. Chairman.

Mr. CARNEY. Thank you.

The Chair now recognizes the gentlelady from Arizona, Ms. Kilpatrick, for 5 minutes.

Ms. KILPATRICK. Thank you, Mr. Chairman.

I wanted to expand a little bit on the Ranking Member's question regarding the NCIC. We are both former prosecutors, and I know we have relied on that database. I represent a huge rural district in Arizona. In fact, my congressional district is bigger than the State of Pennsylvania. I have been working with law enforcement in terms of interoperability problems, and we have got a situation where we know that the drug cartels now are using the back roads. They are taking advantage of the wide open space, and they are moving faster than technology.

So my question to you is, what efforts are being made to provide rural law enforcement officers in the field access to NCIC databases, and then also the technology to allow them to report suspicious activity?

We will start with you, Colonel Fuentes.

Mr. FUENTES. Thank you, ma'am.

To the best of my information, they should have access to NCIC as a matter of the routine course of their patrol duties. Would you be referring to access to the VGTOF database that I described a little earlier?

Ms. KILPATRICK. Yes.

Mr. FUENTES. That, if I am not mistaken, also ties in with the NCIC, that those databases have a link where one will ping the other. If there is information in one, that will come back in an NCIC response. That should be available to everybody in this country to the best, again, to the best of my knowledge.

Where the fusion centers come in is, and this is very crucial, because you are kind of bringing up a point that I was going to make a little earlier on; if you have seen one fusion center, you have seen one fusion center, which means that beyond the baseline, there are individual customer needs in every single State. It may be distinctly different in Arizona than it is in New Jersey or than it would be in Iowa about what those police chiefs or county sheriffs are going to need from that fusion center. Obviously, cross-border illegal immigration, drug cartel violence is going to be an enormous issue in Arizona.

Quite frankly, Congresswoman, that is the responsibility of that fusion center to recognize that those law enforcement agencies in your State need that information. That is compelling to them to do their job, if only from an officer's safety standpoint.

Ms. KILPATRICK. Thank you.

Ambassador McNamara.

Mr. MCNAMARA. Yes. A couple of points. Generally, when one talks about fusion centers, we tend to look at the fusion center as being a State or a major urban area institution. But what your question brings up is the importance that the fusion centers play for the smaller organizations and the rural areas where the numbers and the sophistication of the agencies in those rural areas is not the same as the major police chief, major city police organizations, or the State police organizations.

As Colonel Fuentes said, it is very important that the fusion centers provide the services out to those rural areas, the fusion centers can make the connections with NCIC when a very small town police force doesn't have the capacity but does have the capacity to get to the fusion center and ask the fusion center's assistance to process data that it may not have sufficient resources to process.

I think that as the fusion center network increases and as fusion centers begin to look at their real role in their States and in their regions, that they will see the tremendous value that they can provide in services to rural police, rural homeland security officials, rural mayors, et cetera. One of the evolutionary elements in the fusion center network has got to be the ability to move beyond the major urban areas and get out to the rural areas of this country. In States like Arizona and Texas border areas, that is critically important.

Ms. KILPATRICK. One follow-up question. Are you aware of any efforts through your Department to expand that information sharing in rural areas, aside from the fusion centers?

Mr. MCNAMARA. That was going to be my second point. The second point is, in addition to the fusion centers, if any law enforcement agency that has the basic capability of linking its computers into the fusion center network and/or the FBI's JTTF networks, they can get the information directly if they want it directly. In other words, if they want the raw information that is in the NCIC, for example, but if they want it in a processed form and they don't have the capacity to do it, then they can plug into the fusion center.

So the two ways of getting it is either directly by simply joining and actually getting the network capability that allows you to join and connect with the NCIC or to go through the fusion center to do the same thing.

Ms. KILPATRICK. Thank you.

I will tell you that my district has the least amount of broadband coverage and cell phone coverage, telecommunications. So the basic infrastructure just is not there at this time. But we will keep working on it. Thank you very much.

Mr. CARNEY. I think we just have a couple more questions. I have a question I would like to direct to Mr. Smith and to the Ambassador.

Given the Markle Report and its recommendations, could you please tell the panel where you think Congressional efforts ought to focus on this issue?

Mr. SMITH. One is always reluctant to give advice to the Congress.

Mr. CARNEY. But we are asking this time.

Mr. SMITH. It is an honor, Mr. Chairman.

I think the overall point we want to make is that this needs to remain a high priority. Holding hearings like this is very important, asking detailed questions. These have been very good questions from the panel this morning. I really commend you for doing your homework and asking hard questions.

There are a few things I might call your attention to. One thing I had intended to mention in my opening remarks was there are a lot of exciting things going on. One of them, for example, is there is another group in Washington called The Project on National Security Reform, which is a private organization that has brought together people like Brent Scowcroft and people of that level to focus on how to reorganize national security to make and to improve decisionmaking. One of the things that they have been talking about doing is a pilot project working with some selected agencies and the National Security Council to try to implement some of Ambassador McNamara's recommendations on a very small scale on information sharing.

I think one of the things this subcommittee ought to do is, assuming that the administration does do this pilot program, keep an eye on it, see how it is done. Encourage that kind of thing. Because it is very hard to break through all of this.

I think another thing, Mr. McCaul mentioned section 1018. I think you ought to take a hard look at that. That raises questions more broadly than just Ambassador McNamara's position because it gets into the relationship between the Director of National Intelligence and the other agencies. That has caused some problems that you may have noticed, unfortunately, surfaced in the press, and these issues are now in the White House for resolution.

So there are some things that can be done. Again, I think certainly the Markle Task Force will remain in place. We are honored to work with this committee, and anything we can do to help move this process along we are happy to do.

Mr. CARNEY. Thank you.

Mr. Ambassador.

Mr. MCNAMARA. I would say one of the most important things that needs to be done in the coming months, in fact, I asked—I called back in the fall of last year, that the year 2009 be the year of sustainment for fusion centers. That is to say, the year when we all focus on, how do we take the fusion center networks that have developed and make them sustainable for the long run?

My fear is that, as the Colonel mentioned, there are 72 of them. No one has sat back and taken a look to see whether 72 is the right number. They have grown up. They represent huge differences in capabilities and focus of attention depending upon the State and area and the region in which they are in, all of which is quite proper. But I think it is time now, the fusion centers have developed, and they are a cost and expense for State and local authorities and for the Federal Government. We ought to look very carefully at what constitutes a sustainable fusion center network for this country for the next 15 or 20 years.

We have built something. We have built a capability that it has grown so fast because the need was so high, but it has gone far enough that I think we can now sit back and say, what do we have to do to make sure that, A, it is sustainable? B, that the fusion centers are doing what they ought to be doing and not getting involved in things they might not be as properly involved in?

So I would say, I would put that at the top of the list as something the Congress can do. You can shed a lot of light on what is the best fusion center network for this country over the long run.

Mr. CARNEY. Colonel Fuentes, you probably have some insight on that.

Mr. FUENTES. I couldn't agree more with the Ambassador. The issue of sustainability has something to do with the discussion with the Congresswoman about, is that fusion center in the State making itself accessible to all of its law enforcement partners and first responders?

Different fusion centers around the country have in the course of their own evolution developed some best practices. There needs to be, beyond the baseline, an export of those best practices to other fusion centers that may be having difficulty in their States. One of the things that was discussed a couple weeks ago in the IACP intelligence summit was the formation, perhaps within DHS, of the National Fusion Center Coordination Group within DHS, of an auditing team, composed not necessarily of members of the Federal Government but perhaps directors or analysts from State and local or tribal fusion centers who can go around the country on behalf of DHS and see that those practices are established or encouraged, and even to do a bit of a survey with the customers to see if that fusion center is up to the standards that are expected of them since a lot of them are funded in one way or another by Federal money. So it should be the expectation of the taxpayers that they are doing their job correctly.

Mr. CARNEY. Thank you.

My time has expired.

I now recognize the Ranking Member again for another 5 minutes.

Mr. MCCAUL. Thank you, Mr. Chairman.

Thank you, Ambassador, for that recommendation, certainly one of the strongest ones coming from the panel, sustainment of the fusion centers for the next decade.

Colonel, I am glad to hear that they are sharing best practices. I think it is important that fusion centers have independence to tailor their needs to local jurisdictions, but at the same time, I think it is good that there is an organization out there where you can share best practices and make sure they are up to the standards they should be.

Mr. Smith, I wanted to follow up because you didn't have a chance to answer my question last time about the program manager looking forward. You did reference to 1018, the language in section 1018; and also the role that, in going forward, the role that the program manager is going to have with the White House given this new senior director for information-sharing policy. I just want to give you the opportunity to respond to that.

Mr. SMITH. Well, I appreciate that, Mr. McCaul. I wish to associate myself with what Ambassador McNamara said.

Ideally, this is a job that should go away. I think one of the things that happens in Washington is that doesn't happen very often. So I think encouraging whoever the new program manager is, for he or she to understand that one of their jobs is to make their job go away by institutionalizing this across the Government as much as possible. That may wind up shifting the responsibility for the policy and the implementation into the White House in some senior person who should be, in my judgment, subject to Senate confirmation. I would give that person, again, as Ambassador McNamara has suggested, some budgetary authority. The drug czar is a pretty good model for that. We have, in my judgment, too many czars at the moment. But there does need to be some ability to work across all of the Government.

So I think that the object should be to find some way of creating a position that has the responsibility to ensure policy, to develop policy, to ensure it is being carried out by the agencies that, at the end of the day, have to execute it. It is going to be hard to do that. But, again, this committee, there are some ideas out there that are some pretty good ones, and I encourage you to look hard at them and keep the pressure up.

Mr. MCCAUL. Thank you for that response.

Ambassador, do you agree with that assessment?

Mr. MCNAMARA. I do indeed. I agree completely.

I would say the second area where the Congress can really make a contribution is to examine what I referred to as these crosscutting issues. How are they managed by the Congress and by the Executive? I think the system is broken with respect to crosscutting issues. I spent 3½ years with a high-priority crosscutting issue. The Congress can do a lot if it can sit down, examine itself and examine the Executive Branch, and come up with some new solutions to, how do you manage issues that cut across 5, 10, and, in my case, 17, all of them major agencies of the U.S. Government?

Mr. MCCAUL. Thank you for that. We look forward to working with you in the future on your recommendations.

I yield back.

Mr. CARNEY. Thank you.

We now recognize the gentleman from Texas, Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman.

I would like to address, if I may, Mr. Smith.

Mr. Smith, what I would like for you to do is, on a scale of 1 to 10, I would like for you to—let's make it 1 to 5—I would like for you to give me the grade that you would give with reference to each of the recommendations that you have made, I have five recommendations from your Nation At Risk report released March 2009. So let's start with the No. 1 recommendation, which is to reaffirm information sharing as a top priority.

I understand that ISE has been moved into the Executive Office. I understand the recommendation that Congress hold hearings, well, we are doing that. So on a scale of 1 to 5, how do you rate recommendation No. 1?

Mr. SMITH. I would give it a three-plus.

Mr. GREEN. Because time is of the essence, I probably won't be able to accept a commentary. So if you would let me just make a note that it gets a three-plus.

Let's move quickly to No. 2. We may come back if we have time. No. 2, this has to do with discoverable and accessible information. My understanding is that you would like to use off-the-shelf technology. One to five, how do you rate it?

Mr. SMITH. Three.

Mr. GREEN. Moving to No. 3, which deals with security and privacy and protection, as we talked about the board, how do you rate it? Within that you have three recommendations. I won't go through all three of them, but you want a consistent privacy policy. You want the President to nominate and confirm people to the oversight board. You wanted Congress to conduct the oversight. How do you rate this one?

Mr. SMITH. One-and-a-half, one-plus.

Mr. GREEN. One-plus. All right.

Let's move to No. 4, which deals with the culture. You would like to transform this culture from a need-to-know culture to one that is more productive in information sharing, still with only the appropriate persons having the appropriate knowledge. You suggested that there be metrics and incentives to do this. I appreciate many of the recommendations made, by the way. I am going to try some of this in my office. Good points. How do you score this one?

Mr. SMITH. Three.

Mr. GREEN. No. 5, which deals with empowering the users and what we call communities of interest. How do you rank this one?

Mr. SMITH. Two.

Mr. GREEN. All right. Now, given that I know you want to make comments, let me make one additional comment, and then I will let you comment on whichever one you would like to give me additional information on.

I would like to complement, if I may, Mr. Chairman, the staff. I was remiss in not doing this earlier, and my fear is that if I don't do it now, I may not, because they provided us with a great deal of intelligence. It was very beneficial to me. I don't come from the intelligence community, but they help us to appear to be intelligent. So I thank the staff.

Now, with this said, we will hear from you, Mr. Smith. Give us your comments, please.

Mr. SMITH. Well, as a former Senate staffer, Mr. Green, I greatly appreciate your appreciation of your staff.

I think there has been a great deal of progress. I may have been a little too harsh in some of my grades, but I think it is important to realize that we have a long way to go. The building blocks are there, the basic outline is there.

Ambassador McNamara and his people have put together some suggestions on architecture, on getting the technology in place. Overall, within the intelligence community, the world that I know best, there has been a great deal of progress, but it is still really hard.

What I am also encouraged today to hear from Colonel Fuentes is how the fusion centers are working, and I think that that is an area where the rubber is going to meet the road.

Mr. GREEN. With 38 seconds left, one final question. On a scale of one to five, how important is the oversight board?

Mr. SMITH. The privacy oversight board, I would give that a four.

Mr. GREEN. In terms of importance?

Mr. SMITH. Yes.

Mr. GREEN. Mr. McNamara, one to five?

Mr. MCNAMARA. I would agree, at least four.

Mr. GREEN. Colonel, if you would like to weigh in, of course, you may.

Mr. FUENTES. A lot of discussion on privacy, so I would also rate that pretty high. Everywhere I go, it is top of the list.

Mr. GREEN. Thank you, Mr. Chairman.

I yield back.

Mr. CARNEY. Thank you.

Ms. Kilpatrick.

Ms. KILPATRICK. Thank you, Mr. Chairman. I want to give my 5 minutes to the panelists to make any further comments they wish to go to the grading system that Mr. Green just presented.

So, Mr. Smith, any further comments? You have got 5 minutes.

Mr. SMITH. Well, I certainly don't want to grade myself. I would probably give myself a minus grade.

One thing that does occur to me as I listen to this committee, particularly with some of the broader issues you have raised, it might be worth to have a conversation with the group I mentioned earlier, the Project on National Security Reform. They have made a great deal of progress. They have issued a big report. This is led by a man named Jim Locher, who was the key Senate staffer for the Goldwater-Nichols Act, which reorganized the Department of Defense, which generally is recognized as quite a good achievement.

There are some things in there that relate very directly to information sharing and to improving decision-making on the National security issues. It doesn't deal with local law enforcement. But there are some lessons in here that I think the subcommittee might want to take a look at.

Ms. KILPATRICK. Colonel Fuentes.

Mr. FUENTES. Between these two gentlemen, I was glad to be an audience member most of the time today, and I learned a lot. So I thank you for the invitation to come here.

The one thing that I did want to bring up is that we depend a great deal on our crime analysts in the fusion center. Every day, depending upon their skill and ability, they have to navigate dozens of databases, many of those databases are Federal, in order to draw out the information that they need to put together the assessments that they are working on.

Thanks to the PM–ISE and BJA and DHS, they have come up with a National Information Exchange Model that between the States and the locals have developed a series of common terms so that a car in one database is also a car in another database and not an automobile and not a vehicle in a third database, because obviously, when you are looking to get information, you may not get access to information that you want.

I would ask that this subcommittee think about doing the same thing, certainly at the Federal level among those databases, is to come up with a common data standard that I think will make information sharing an awful lot easier within the fusion centers and even among the agencies that manage those proprietary databases.

Thank you again for the invite.

Ms. KILPATRICK. Mr. Ambassador.

Mr. MCNAMARA. Thank you, Congresswoman.

I would endorse Jeff Smith's recommendation about taking a look at the PNSR project and Jim Locher's recommendations or the recommendations of the project, not just of Jim.

It was a very credible and serious look at many, many aspects of Government functioning, and it does get—it does touch on information sharing and the need for revising the way we manage information in the Federal Government. I participated in it myself, so I know fairly well the recommendations that they made in these areas.

I would like to take, since Jeff doesn't want to do it himself, the opportunity to say that I found the Markle reports to be an enormous aid to me in my job over the last 3½ years. It is always good inside Government to have somebody outside Government looking critically at what you are doing. It is a burden at times, but in the end, it leads to better Government. The Markle Foundation is to be congratulated, in my opinion, for making a signal contribution to national security in its efforts.

Ms. KILPATRICK. Gentlemen, thank you so much.

Mr. SMITH. I would just like to add one, you didn't ask Mr. Green to rate Ambassador McNamara. But I would give him a five-plus.

Ms. KILPATRICK. Thank you.

Mr. CARNEY. Well, seeing that there are no further questions, I truly want to thank the witnesses for their testimony.

Occasionally we have edifying hearings in Congress, and this certainly is one of them. I think we all learned a lot.

I certainly want to thank the subcommittee Members for their questions as well.

I would like to remind the panel and the witnesses that we may have other questions that we didn't get a chance to ask today. As we discussed, things may come up. Please respond in writing expeditiously. Once again, thank you very much.

This subcommittee stands adjourned.

[Whereupon, at 11:56 a.m., the subcommittee was adjourned.]

○