Keynote Address and Q&A by Kshemendra Paul,
Program Manager – Information Sharing Environment

A Dialogue on the New National Information-Sharing Environment (ISE) Strategy: Building Beyond the Foundation

Welcome/Moderator:
Rick "Ozzie" Nelson,
Homeland Security and Counterterrorism Program, CSIS

Center for Strategic and International Studies (CSIS)
Washington, D.C.

October 5, 2010

RICK "OZZIE" NELSON: Well, welcome, everyone. I'm relatively new to the think-tank world, but we're actually going to start on time at 8:30. (Laughter.) Used to be, in my military days, if we started five minutes early, it was on time. And now, five minutes early here is 15 minutes early.

So – but anyhow, my name is Rick "Ozzie" Nelson and I'm director of the Homeland Security and Counterterrorism Program here at Center for Strategic and International Studies. And we are absolutely thrilled about this conference, and we're thrilled to have Kshemendra here to kick off this event, which is – their key event in the recrafting or the redrafting of their National Strategy for the Information Sharing Environment.

We have a very, very aggressive agenda today, with two different – two different sections. But before I get into the details, I wanted to thank everyone for coming. Again, it's a very robust – robust audience here and a very – heavy in government, a lot of industry folks and even some folks from Capitol Hill, so we're very, very excited to see that.

And we even have C-SPAN2, I think, is here, which is – it's why we were joking earlier, it's like the "Dodgeball" quote where they said ESPN-Ocho. But – for those of you've ever seen that movie. But no, we're happy to have C-SPAN here.

I would like to first – we are a nonprofit at CSIS, so that means we – you know, we need help to have events like this, and I really want to thank our sponsor for this information series of events we've had. We had the Tom O'Reilly event a week ago. We're going to have Sean Joyce and Kira DeMeen (ph) And Bob Mackne (ph) in the future. And that's IBM, and I want to thank Alan Heath And Dan Prieto for their continued support here for allowing us to do this. So thank you, IBM, for that.

To go over the plan of the day here, that's what we used to have in Navy days. The plan of the day, we're going to have – the first part of this event is on the record. So for those of you in the media, we obviously are taping this. This is being filmed, taped live, so feel free to take notes and quote and do what you want. And that'll be Kshemendra's remarks.

And then after that we're going to go into a panel of government officials. That also is on the record, and you should – it will be taped and played live, and you should feel free to quote from that.

However, after those events we're going to have three off-the-record panels, and that's for a specific purpose. One of the things we're trying to do here is to create an environment – this is Dr. Hamre's vision – that CSIS can facilitate and add value, not just pontificate endlessly about things, but actually add value to the government process.

And what we want to do is create an environment where people in the room, especially those from government and industry, can speak freely without having to be concerned about being quoted out of context, and we can have an open and honest dialogue that Kshemendra and his team can use to formulate the upcoming strategy.

So folks say, well, strategies are always disconnected from the real world. This is an opportunity we have to connect our comments and our thoughts to that strategy. So it's very important that we adhere to that off-the-record form. And I apologize for being a little preachy about that, but sometimes everyone listens.

After Kshemendra's remarks we're going to do a question-and-answer, a very robust question-and-answer. I'll moderate. It's important that you state a question, no statements-and-answers. It'll be questions-and-answers only, and I will – and I will be ruling with an iron fist.

So before I turn it over to Kshemendra, I'm going to go ahead and just give you a, you know, this is a brief introduction of him. Obviously, we're thrilled to have him here.

He's the program manager for the Information Sharing Environment. He was appointed – and a lot of people don't know that about PM-ISE, it's a presidentially appointed position – by President Obama in July. And he has – I love this charter – his charter is "government-wide authority to plan, oversee the growth of, and manage the use of the ISE." I'm sure that there was a long line to get this job. (Chuckles.)

It's a very challenging task, but I think that we've – at least I have, from my perspective – seen some significant progress in the last few months with Kshemendra there. At least a more open and more robust dialogue, which is obviously absolutely critical to making this work.

You know, prior to this job, he was the – served as the federal chief architect in OMB, where he focused on issues surrounding interoperability across networks and databases. And he also has extensive experience in the private sector.

In fact, he's trained as an engineer, so unlike myself, who's just trained to fly helicopters and write and talk, Kshemendra actually understands some technology behind this and has designed stuff like this. And that engineering background, obviously, is something that's critically important to developing this ISE architecture.

So would everyone just go ahead and join me in welcoming Kshemendra Paul? (Applause.)

KSHEMENDRA PAUL: Good morning.

AUDIENCE MEMBERS: Good morning.

MR. PAUL: Thank you, Ozzie, for the kind introduction. I'm grateful to CSIS for hosting the event today.

This is a wonderful forum which will allow us to explore the opportunities and challenges around Building Beyond the Foundation: Accelerating Delivery of the Information Sharing Environment, including clarifying its scope and mission, the target vision towards which we are building together, and how we measure the created value.

Our high calling is to support our mission partners – the federal, state and local, tribal and territorial agencies, and our partners internationally and in the private sector – to protect the American people and enhance our national security through the use of information.

Thank you to our sponsors today. We're grateful that you're supporting CSIS in continuing to shine a light on information-sharing.

There's a great lineup of speakers and moderators today. I'm very excited about this. It's a great event, Ozzie, that's come together. And I appreciate all of them taking the time and all of you taking the time to participate in this dialogue.

Now, my communications team asked me to shamelessly promote the ISE community website, so get out your pens. (Laughter.) It's www.ise – Information Sharing Environment – ise.gov. It's a great resource for folks who want to dig a little deeper and participate in the dialogue, while they're not here physically, and for you all to get a little bit more additional information and stay connected to the dialogue.

While you're at the site www.ise.gov, be sure to sign up for e-mail alerts. (Laughter.)

So – before I get into the meat of my remarks today, let me walk you through the structure of my presentation.

As Ozzie described, I'm an engineer by training. I was an enterprise architect at the Department of Justice and the Office of Management and Budget. My old colleague Jeff Cook's sitting here in the front line.

At times like this I feel a need to stay current in my functional domain, so please – please bear with me a little. I'm going to use a little EA parlance to describe my remarks this morning.

First I'll spend a little time looking back at how we got here. In EA-speak we call that the as-is. Next I'm going to walk you through what we're hearing from thought leaders like yourself and mission partners in the agencies, state and local, tribal, territorial. We call that the to-be, and we're going to talk and sketch out a straw-man that we hope to refine today and in future dialogues, eventually to be reflected in the national strategy.

Then I'm going to outline for you some really hard questions I need help answering. These are the questions that GAO gave us just a little while ago. (Laughter.)

Just kidding. (A big hello. ?) I think there are some colleagues from the GAO here in the – hey, there you are, back there. Good. (Laughter.)

Now, they are hard questions, but – but they're not the ones I'm going to present today. There's a different set of hard questions, so in the remaining time we've move to questions and answers.

You don't often find engineers behind podiums addressing large crowds on C-SPAN2. You'll find us in dark offices at odd hours, noodling over white boards on hard technical problems, or out in the field working to understand customer requirements and delivering solutions.

As an engineer, my approach to solving hard problems is rooted in an appreciation of first principles, diving headfirst into the details of the challenge, and then lifting up to solve the problem. This is the approach I'm bringing to Building Beyond the Foundation: Accelerating the delivery of the Information Sharing Environment.

One more sidebar. The ISE is a – is a somewhat abstract topic. People have a hard time getting their heads around what exactly is that ISE? It's useful to set a mental model. I like to think about concrete examples, so I'm going to give you four to help process what you are going to hear today.

Number one, a law enforcement officer, as part of a routine traffic stop, queries the National Crime Information Center, or NCIC, and is notified to contact the Terrorist Screening Center to evaluate a potential match against a terrorist watch list.

Number two, an intelligence analyst using the National Library of Intelligence or the A-space platform to collaboratively develop new counterterrorism intelligence products with fellow analysts across the ISE.

Three, Coast Guard personnel working on the Gulf – recent Gulf oil spill, using Department of Homeland Security's Homeland Security Information Network and FEMA's Web Emergency Operating Center, the same assets to be leveraged in both manmade and natural disasters.

Finally, a local law enforcement analyst and an FBI intelligence analyst, colocated at a state fusion center working prison radicalization issues, both developing finished intelligence products as well as supporting specific FBI Joint Terrorism Task Force investigations.

Back to the main part of my remarks. First up is to outline how we got here.

As an engineer, I make a concerted effort to stay away from authorities discussions. But after five years in Washington and three months as PM, I've learned to start with authorities and mandate.

In 2004, the 9/11 Commission delivered their report. The commission prescribed the need to transform government and brought to light multiple challenges around connecting the dots.

As an aside, I'm not a big fan of that term, because it oversimplifies the challenges that face us as a community. It does not provide a good frame for working through many of the legitimate policy concerns we're facing and is not so helpful with the so-called information overload problem.

The 9/11 Commission proposed that information be shared horizontally across networks that transcend individual agencies. The commission called for a decentralized network model which would allow agencies to own their own databases, but enable the databases to be searchable across agency lines.

It recognized, by moving to a data-centric – I repeat, a data-centric – model, a new framework would have to be established to control access to the data, not the individual networks, systems or databases.

The commission called for a government-wide effort to address the legal, policy, and technical issues that would arise from this type of system. The idea was to have someone looking across all the agencies, creating a trusted information network to facilitate the sharing of terrorism-related information.

This recommendation, among several others, was adopted from the 2003 Markle Report, Creating a Trusted Information Network for Homeland Security. I know because I reread the report for the third time this summer at the beach. (Laughter.)

Now, we have some folks from Markle in the audience, and many of you have participated in the Markle Task Force. It's a very good piece of work.

This concept, as well as (federal ?) identity management, decentralized information, privacy protections, extensibility to state and local, tribal, and territorial partners, and a focus on prevention – a focus on prevention – were incorporated into the Intelligence Reform and Terrorism Prevention Act of 2004, or IRTPA.

They called it – Ozzie, can you give me drum roll, please? – (laughter) – the Information Sharing Environment. Yeah.

The Congress agreed with the 9/11 Commission that horizontal integration required government-wide authority, so they created the role of program manager to plan for, oversee the agency-based build-out, and manage the information-sharing environment, and granted that role government-wide authority.

The PM-ISE was told to work across five core communities: Intelligence, defense, foreign affairs, law enforcement and homeland security, to enable the effective sharing of terrorism-related information.

The recognition that this effort has to have horizontal capabilities lay as much in the understandings and implications of the technical challenges – which are substantial, but not the main event. It's the legal, policy, cultural and organizational hurdles which need to be overcome for progress.

Subsequently, the Implementing the Recommendations of the 9/11 Commission Act of 2007 amended IRTPA to expand the scope of the ISE to include homeland security and WMD information. The 9/11 Act also enhanced the authorities of the PM-ISE in two important ways.

First, it enhanced the ability to issue government-wide standards, procedures, guidelines, instructions and functional standards. And second, it mandated that we identify and resolve with our mission partners information-sharing disputes. Many refer to this as the honest broker function.

Okay. I'm done channeling my inner policy wonk. Let's pause for a second.

Now, for the second part of the as-is, what's been done to date:

A strong foundation has been built, and I'm going to describe a number of steps we've taken together as a government.

In 2005 the presidential guidelines directed the ISE to leverage existing systems to the maximum extent possible and directed that common information-sharing standards be developed.

I need to pause here and emphasize the implications of these requirements. It's essential to understand that the ISE is owned and operated by mission partners – federal, state, local, tribal and territorial agencies, our partners in the private sector and internationally.

We – as the PM-ISE, we don't build anything. We're not operational. Our role is to help agencies find common mission equities, to help them implement functional and technical standards and to drive resolution of policy issues. The actual point of implementation, the heavy lift, is with the agencies. They're the engines that deliver the ISE. They're the stars of the show.

The guidelines also directed us to address the proliferation of sensitive but unclassified markings, develop a framework for privacy, civil liberties and civil rights protections, and develop an approach to share with state, local, tribal and territorial partners.

Much of this work was captured in the 2007 National Strategy for Information Sharing and in subsequent ISE annual reports. You can find those on our website, www.ise.gov. (Laughter.)

I want to highlight four areas. First up, privacy and civil liberties. The ISE is envisioned as a trust partnership between all levels of government and the private sector. In order to participate in the ISE, the law requires that federal departments and agencies and our non-federal partners have privacy protections at least as comprehensive as the ISE guidelines.

Next, CUI, or controlled unclassified information. The new CUI framework will standardize more than 100 unique markings currently used for sensitive but unclassified information. These are the markings you see on top of documents around town – FOU, or for official use only; OUO, official use only; LES, law enforcement sensitive – and others. Of course, you'd only see those markings if you were a government employee. (Laughter.)

The standardization will be critical step towards removing barriers to information-sharing.

That wasn't a joke, Ozzie. (Laughter.)

MR. NELSON: (Off mike.)

MR. PAUL: Next we developed the ISE architecture – (inaudible) – methodology to connect the diverse systems and (distributive ?) systems across the ISE. Now, I'm not going not get into that here in detail, but I am available for command performances on the architecture. (Laughter.)

Finally, common information-sharing standards that document the rules, conditions, guidelines and characteristics of business processes, production methods and products supporting information-sharing. The program was successfully used to standardize suspicious activity reporting. More on that later.

There are so many other critical foundation blocks to the ISE. Some examples are performance measures, identify management, access controls, information assurance, performance measures (sic), culture, training. You could find the rest of the story at the ISE community website.

Beyond the ISE's foundational enablers, much work has been done to enable ISE core capabilities in the areas of sharing with state, local, tribal, territorial partners.

To develop the common framework, we worked closely with our stakeholders. In particular, I'd like to acknowledge a lot of our stakeholders in the – you know, in the non-federal arena. We worked with a lot of individuals and organizations. I'm going to miss someone, but I want to try to highlight our partners.

We worked with the Criminal Intelligence Coordinating Council, known as the CICC; great organization. It was foundational to our work with fusion centers and suspicious activity reporting.

The Global Justice Information Sharing Initiative. Just as an aside, when I came into Justice five years ago, the way I made myself relevant was partnering with the state and locals through Global. Great organization.

National Governors Association; Governors Homeland Security Advisers Council; the International Association of Chiefs of Police; Major City Chiefs Association; National Sheriffs Association,; National Association of State CIOs, chief information officers; National Association of Counties; owners and Operators of Critical Infrastructure; and many, many, many others.

Open government in action. The result was a series of recommendations to enhance the sharing of terrorism information across all levels of government and the private sector. One highlight of the work was the establishment of a robust network of state and major urban area fusion centers. DHS, Department of Homeland Security, is the executive agent with the lead on this part of the framework.

Fusion centers are the critical nodes that connect state, local, tribal and territorial partners with the information-sharing environment. Through these fusion centers, state and major urban areas will be able to, one, receive classified and unclassified federal information, including sensitive, time-urgent alerts, warnings and notifications.
Two, conduct risk assessments, understanding potential threats to vulnerabilities and consequences, based on their specific areas of operation.

Three, further disseminate critical information to state, local, tribal and territorial partners and private-sector entities within their jurisdiction.

And fourth, gather, interpret and disseminate state-and local-level information to the other localities, states and the federal government. More about this later. It's best manifested through the – or understood through the suspicious activity reporting initiative.

The fusion centers will operate these capabilities within the scope of privacy policies. Currently, 26 fusion centers have approved privacy policies and operation, up from 22 last month. These policies are at least as comprehensive as the ISE privacy guidelines. With DHS's leadership, we have solid momentum across the states to get the rest done in the coming year.

The framework just described is laid out in great and useful detail in the 2007 National Strategy for Information Sharing. The appendix to the strategy defines these roles and responsibilities, and it's in the process of being implemented.

Bart Johnson, DHS principal under secretary for intelligence and analysis, is leading these efforts on behalf of DHS Secretary Napolitano and Under Secretary Wagner.

Bart has an incredible perspective on these matters, having spent most of his career with the New York State Police, culminating in commanding the Upstate New York State Regional Fusion Center. And just as he was getting it humming, the feds hired him away, so – Bart's a friend. He's participating in the panel immediately following my talk.

We have all seen significant information-sharing improvements within individual agencies. Many of these are documented in the annual report and many more are out there waiting to be celebrated.

I'd like to highlight two examples from the intelligence community that, incidentally, my office had a little direct involvement in accomplishing. That's the nice thing about being government-wide, right? I get to, you know –

Seriously, a core part of my responsibility is identifying, integrating and extending best practices across the ISE. This is a kind of a soft – a soft power. There's no authority that's specific to this, but actually it's very, very powerful. I learned that lesson when I was at the Department of Justice working at the National Information Exchange Model, and then at OMB as the federal chief architect.

The most significant and visible change in terrorism-related information-sharing was the establishment of the National Counterterrorism Center, or NCTC. Russ Travers is also going to speak on the opening panel. He's NCTC's equivalent of a chief knowledge officer. Russ is a respected leader in our community. He was recognized as a Galileo Award finalist this year for his thought leadership on information-sharing.
Further, the intelligence community has led the information integration by implementing intelligence community directive, or ICD-501, discovery and dissemination or retrieval of information.

This policy promotes responsible information-sharing by distinguishing between discovery and dissemination or retrieval. It's based on – I'll be a little technical – meta tagging. It's a really good best practice and something that has potential to look –and be used more broadly.

Before we turn our attention to the future, there's one last element of the ISE strategy to round out the as-is. And it's important to highlight, because it helps make the ISE that much more real and that much more meaningful.

In response to the 2007 national strategy, we convened several federal agencies, law enforcement organizations, local police departments and others to develop a unified activity around – a unified process around suspicious activity reporting, or SAR.

This unified process builds on what law enforcement has been doing for years – gathering information regarding behaviors and incidents associated with criminal activity, and establishes a standardized process whereby that information can be shared among agencies to help detect and prevent terrorism-related activity.

Tom O'Reilly, who presented here at CSIS a couple weeks back, spoke at length about what is now the nationwide Suspicious Activity Reporting Intuitive, or NSI. Tom is a friend and someone I'm privileged to call a mentor.

In March of this year, the attorney general announced the establishment of a program office at the Department of Justice Bureau of Justice Assistance to facilitate the implementation of NSI across all levels of government and named Tom O'Reilly the director. Tom's charge is to roll out the NSI nationwide while ensuring that privacy, civil rights and civil liberties and strengthened.

You may be familiar with NSI, due to Secretary Napolitano's "See Something, Say Something" campaign. This is the public awareness component of NSI.

The NSI is one of our most significant accomplishments to date, and an example of the ISE in action. In an interrelated set of harmonized policies, mission processes and systems which leverage ISE core capabilities and enablers to empower the men and women on the front line to share and access the information they need to keep our country safe.

And I have late-breaking news, so I'm going to make a little news today. Little news, but it's – it's important and it's good.

The FBI is already well integrated into the NSI solution. Last week the FBI extended their integration to improve sharing of SAR – suspicious activity reports – generated from their field work. What's noteworthy here and slightly technical is that these SARs, while unclassified, are being worked and contained in the FBI's classified systems and databases.

It's a great example of being data-centric in our sharing and sharing federal data with other levels of government. These SARs are being shared with the fusion centers, state and local fusion centers, through the NSI – which brings us to to-be part of my presentation today and the purpose of this forum. My office is leading the process, with mission partners, of developing the National Information Sharing Environment Strategy.

This includes subsuming the 2007 National Strategy for Information Sharing and bringing forward the foundational pieces of that document as it relates to information-sharing with state, local, tribal and territorial partners.

We are working with our mission partners to conduct deep-dive conversations. We also want to include thought leaders outside of government; that's why we're here today and engaging in a process to do that.

This discovery process will assist us in developing a target vision and supporting strategies to build beyond the foundation and accelerate the delivery of the information-sharing environment.

To set the stage for the speakers and dialogue we'll be having for the rest of the day, I'd like to briefly describe three ideas.

The first idea: the president's national security strategy calls for a whole-of-government approach to build national capacity based on applying and integrating the efforts of all agencies with the national security mission.

To effectively support whole-of-government, our working hypothesis is that the ISE must, one, empower the front line with the information they need to do their jobs; two, deliver data-centric capabilities that support re-use; third is to strengthen privacy, civil liberties and civil rights protections; fourth, align with technology and information management trends; and finally, leverage standards-based innovation.

To make the ISE work, we need to focus on data – sharing it, discovering it, protecting it, fusing it and reusing it. We need a data-centric approach in alignment with the original mandate for the ISE.

I also highlighted standards-based innovation. We can dramatically improve (price ?), performance, increase agility, decrease risk, and accelerate deployment of the ISE by effectively working with our partners in industry. This is such a critical aspect of what we need to do to deliver, and I'm anxious to have that conversation. And we have a technology panel later today; I'm looking forward to that.

Okay. The second idea: the opening panel is focused on opening the aperture to the totality of terrorism-related information-sharing as directed by law. There are several aspects of the expanding aperture idea. In the past, we've advanced initiatives in the federal-to-state and local information-sharing space. The 2007 national strategy does an excellent job of laying out roles and responsibilities in this regard.

Building from our foundation, we want to enhance and extend partnerships across all five communities – defense, intelligence, law enforcement, homeland security, foreign affairs. I'm looking forward to hearing from today's speakers as well as members of the audience on this topic.

Also, the ISE mission partners rarely have the ability to segregate their terrorism-related activities, or their terrorist-related information. Mission partners ask us for complete solutions. It's a reasonable and right request. Such needs need to be factored into our strategy going forward.

Finally, the third idea is the role of sourcing, integrating and sharing best practices on the road to transformation. For example, our core standards framework, the national information-exchange model, is used well beyond the national security space. Another example is the potential to scale ICD-501-type meta tagging and discovery schemes more broadly.

We're looking for feedback and discussion. Are these the right ideas? What refinements are necessary? And what's the best way to clarify the target vision and enable incremental progress?

This last point is so critical. We need to be working in an incremental way while we're building towards the future. We need to be making changes that deliver value every day.

This brings us to the last part of my remarks today. We're in the home stretch. Stay with me. (Laughter.)

We need your help to better understand the landscape so that the ISE assists our mission partners in delivering the comprehensive and inclusive solutions to the issues they face daily. In addition to reacting to the ideas I just highlighted, here are a few questions for the speakers and participants in today's conference to consider:

So this is – get out your pens. (Laughter.) There'll be a test. We'll collect the papers at the end, right, Ozzie?

MR. NELSON: (Off mike.) (Laughter.)

MR. PAUL: What are the best practices to be replicated across mission partners? What best practices should we be looking at? What's the best way to enable discovery? How do we balance data aggregation with the decentralized NSI-type architectures? Is it possible for there not be a single architecture across the entire ISE, or do we need to take a heterogeneous approach?

A core issue, in my mind, with authorized use is not the technology; it's the variability in the policies and the lack of consistent, precise semantics for expressing those policies. How do we get past that issue?

Are there successful examples that we can model on and build from around embedding legal restrictions and policies at scale and across domains? How do we leverage open government-type ideas to accelerate planning and delivery of the ISE? How do we incent and celebrate progress in spreading adoption of best practices? Is there a role for challenges?

What are the concrete, immediate steps that can be taken to accelerate change this year? And finally, what are the measures and metrics we should adopt across the ISE to measure the value we create together?

Well, thank you for listening to my remarks. I hope I kept my inner geek in check.

(Laughter.)

I've set the scene to allow us to talk about the future. What the ISE needs to be to support the counterterrorism mission and building beyond the foundation, how do we accelerate delivery of the information-sharing environment?

I welcome your questions, remarks and commentary. Thank you very much.
(Applause.)

MR. NELSON: Well, thank you, Kshemendra. We appreciate those remarks. It's a little bit – my reflection on your remarks is a little bit of a change of pace, having been kind of in the policy world for probably a bit too longer than I should have in my naval career.

But getting some remarks from an engineer, there was actually substance in there. (Laughter.)

And I'm not used to that.

MR. PAUL: Too much?

MR. NELSON: No, it was great. I was, like, wow, we're actually getting facts and details and a plan and – wow, how refreshing. And then you also gave us homework, which is good. So those of you that thought you were just going to get a free lunch and just listen, you didn't read the –

MR. PAUL: Yeah, that's open government in action. (Laughter.)

MR. NELSON: So we are going to take those questions and we are going to try to address those for you.

Another reminder to everyone here before we go into the questions, in addition to C-SPAN here, we also are live-webcasting this on our website. There's a link at www.ise.gov as well. And this will be available for download on iTunes in the future, if you want to go back over Kshemendra's very – and I mean this, Kshemendra, very substantive remarks. It's very refreshing that we actually –

I think people like to roll up their sleeves and actually tackle problems, as opposed to just talking in the theory of things. So we appreciate that.

We're going to go ahead and go into questions and answers. We have – because this is webcast, we ask that you please – we'll have microphones coming around. Please state your name and your affiliation, if you have one, so we can understand the context of the question, and Kshemendra's going to answer.

But I get to ask the first one. That's the – that's the big thing I get out of this, is the first question.

And you know, I guess, reading your speech and reading some of the information you sent in advance and just some of the stuff that we've done with ISE in the recent months, I'm struck by your charter. In many ways, it's very similar – and my good friend Russ is back here, a former colleague at NCTC – similar to the charter that NCTC had, where you had control of nothing but responsibility for a lot – responsibility for coordination and sometimes limited ability to compel.

So I guess I would ask you, Kshemendra, what do you see as maybe your one or two, just to limit you, greatest challenges facing you in this new position that you have as PM-ISE?

MR. PAUL: Thanks, Ozzie. Can folks hear me? Do I need to pull this up a little closer? Okay, there we go.

You know, you're right about the nature of the challenge of the information-sharing environment. It's nearly a horizontal – horizontal problem.

It reminds me of my time at OMB. I was in the Office of E-Government and IT there. Internally we call it the office of horizontal government. It's kind of a core challenge. It's working horizontally in a vertical world, and that's – you know, that's the heart of it.

I think, frankly, it's where there's the greatest opportunity for innovation in how we think about government services. And, you know, most of – a lot of our challenge in counterterrorism is a core example.

Counterterrorism inherently is a cross-boundary, cross-domain problem. It's national in scope. Lots of different folks have to come together out of different disciplines, different organizations. How do you work across boundaries? That's a – you know, that's really the cutting edge, I think, of public service and – you know, I'm just honored to be in a place to work on that problem.

MR. NELSON: Yeah, and I – and I found my time extraordinarily rewarding at NCTC, just because of what you described. So that's great, and I look forward to it.

Okay. We'll go ahead and go to questions. Who wants to go with the second question? Anybody from the audience?

The gentleman in the blue shirt back there, please?

Q: Hi. My name is Harvey Rishikof. I'm the chair of the American Bar Association Standing Committee on Law and National Security.

So my question's very simple. Do you see any particular laws that have to be changed in order for you to be successful?

MR. PAUL: So that's a – that's a great question, do I see any laws that need to be changed. I can answer that a couple of ways.

One is in terms of the authorities of my office and the mandate that the law gives to the PM-ISE and the authorities. I think we're all set that way. It's, from my perspective, a matter of mainly execution, of bringing together mission partners, finding the common mission equity and execution is the – you know, the core challenges – core challenges I face.

There are gating policy issues that have – that are out there, all right? This is – this is almost like the old analogy, you're draining the swamp and you see some stumps, you see rocks, old boot, right? And you drain the water a little bit more and you see some more, and so you've got to work those issues.

So I think, you know, in terms of that side of the equation there's a, you know, always opportunities, perhaps, to look at the – at the legal and policy frameworks. But – that's not where I'm at right now.

I'm, you know, in terms of the authorities of the office, we're all fine.

MR. NELSON: Okay. And for those of you that, you know, were going to stay for just a couple of panels then leave, I would encourage you to stay for the last panel. Because that's the one on civil liberties and civil rights, which is sure to be an exciting and interesting discussion – and one of the reasons why we stuck it near the end.

Okay, next question. (Laughter.)

Next question? The gentleman up here in the blue suit. I can't say that in D.C. Blue suit. Right? (Laughter.)

Q: Sir, Steve Cantrell, Office of Global Maritime and Air Intelligence Integration, Director of National Intelligence.

We're a partner with you, but one of the more interesting things I've found is recently out on a trip, other than being asked why I followed you to the same location, was another location where the comment was made that as we tackle this problem set and we look at all of our interagency, state, tribal, local and other partners, one of the individuals I was discussing this with compared it to the NATO of America, he said, because we all speak different languages; we come from different cultures.

For example, you made reference to the significant activity report and, of course if we take that acronym of SAR, the helicopter pilot sees it as search-and-rescue; synthetic aperture radar, special access required. Again, using the same terms but meaning completely different things.

I was wondering if you could reflect on what you've seen in the short time you've been in the office.

MR. PAUL: Sure. Thanks, Steve. Yeah. Steve is a – Steve is a partner, and working on airspace domain awareness and other – other domain awareness-type initiatives.

This issue and the term we use when I'm with my architecture buddies is semantic interoperability. And you've provided a great explanation of what exactly that means.

It's where we started, frankly, when – going back, rewinding the clock five years ago, the ISC was standing up. I was over at the Department of Justice leading something called the National Information Exchange Model, the heart of which was, you know, creating this sort of Rosetta Stone between different functional domains.

So you know, if somebody is working in the Coast Guard in homeland security and has a certain definition for SAR, right? Or you're in the military and have a certain definition for SAR or, you know, you're in the finance domain looking at financial SARs, right? They use exactly the same definition for Bank Secrecy Act, suspicious activity reporting.

That there is a way to, you know, map those terms so that you could translate and you wouldn't use the same thing, so that two people communicating, if they're in different domains and different organizations, the message meant the same thing on both sides of that communication.

So we've actually come a far way in terms of the theory of how to do that and the practice of how to do that. You know, and that by using more formal methods, as we've done with the NIMAN (ph), and actually reflecting those in functional standards, business process standards.

And I'd even go a step further, working with our partners in industry. One of the examples is the suspicious activity reporting, so it's got to be standards that are based on that Rosetta Stone-type concept in the national information-exchange model. And now industry is actually implementing it.

A couple of major vendors sell a fusion-center-in-a-box offering that's compliant with that, right? So that the – you know, we've – getting the benefits of standardization in terms of, you know the acquisition. Really, that's so critical, right?

Think about the front line. A, you know, first responder has a radio. They just want to be able to press a button. They don't want to worry about the complexities, right? And that's kind of our challenge. One reason this space is so complex is that we have to deliver it in a – in a compelling way to the front line where we mask that complexity.

So yeah, it is a core challenge and it's one we've been working on for some time.
MR. NELSON: Next question, the gentleman in the blue shirt in the middle there, please.

Q: Hi. Scott Glick with the Senate Judiciary Committee.

I want to follow up on Harvey's question, because the civil liberties panel doesn't have anyone from the government on it.

Have you or anyone else in the government asked every agency to compile a list or identify the specific privacy laws that are impacted on the information-sharing environment?

In other words, do we have a baseline from which we can assess whether or not there are any laws that need to be changed? Do we have that compiled across the federal interagency?

MR. PAUL: I have some colleagues in the office in the audience here from – that are – that are a little bit more conversant on the specifics there. So if one of you wants to help out, that's great.

Let me answer the question this way. We have been working on privacy guidelines for quite some time; it's the information-sharing environment privacy guidelines. And through that process we've been working with chief privacy officers across the ISE participating agencies.

So through that process, you know, we've developed the privacy guidelines and then the agencies now are implementing privacy policies and have implemented privacy policies that are as comprehensive as our privacy guidelines. So I can maybe follow up with you.

Okay, Alex, do you want to –

ALEX JOEL: Yeah. I'm Alex Joel, And I'm the civil liberties protection officer for the director of national intelligence and I work very closely with Kshemendra implementing those privacy guidelines throughout the – throughout the government. I chair a privacy committee that oversees the implementation.

One of the provisions in the privacy guidelines is for those privacy officers, if they identify, particularly, laws or policies that might need to be changed, to float those up. So we do have a process in place to identify them.

We have not yet, though, gathered a list of any kind like that, but we have a process in place to do so.

MR. NELSON: It's very difficult at times, and that's (not ?) to happen to this panel, but to get someone from the government to talk about CRCL. It's a very challenging thing to do. But a good point on the panel as well. We'll take that for future reference.

Okay, next question. There's – any more questions?

Well, I have another question. You know, Kshemendra, again, in the substance in your speech, you talked about some things for the future and you asked us some questions and you gave us some homework to do today.

But I guess I would ask them back you. What – in your vision, what does ISE look like a year from now? What does it look like five years from now? What does it look like 20 years from now? I mean, what would you – what do you want to accomplish and what do you see?

MR. PAUL: So that's a – that's a good question, and – we have several initiatives under way that are bearing fruit. So let me describe those.

You know, I see Bart Johnson in the back; he's on the panel immediately following. He's leading a process where we're doing the baseline capability assessment across the 72 fusion centers, and that report should be coming out shortly.

We've identified certain critical operating capabilities, and we expect that those operating capabilities will get mitigated. So we have a robust, measured infrastructure of these state and local fusion centers, looking across things like privacy protections or the ability to receive classified information or, you know, some of the other critical operating capabilities I described earlier. So that's kind of – one thing in the next year is substantial progress on the network of state and major urban area fusion centers.

The nationwide SAR initiative. Earlier this summer, Secretary Napolitano kicked off the See Something, Say Something campaign. It by all accounts has been well received, and we're ramping up the nationwide SAR initiative across the country. We'll have, I believe, the majority of states actually integrated into the initiative, and there's lots of anecdotal evidence and measured information that tells us that it's making a difference.

A big initiative in our office has been interconnection of the so-called SBU – sensitive and unclassified networks. This is a – you know, been a core refrain from law enforcement, homeland security, first-responder types, state and local types, that the different federal networks don't interoperate as well as they should.

So we're seeing that interoperability, and we've delivered a lot of capabilities over the last little while and documented in the annual report. And over the next year we'll see simplified sign-on, right? So you don't have all the different passwords. It's easier to get access. A law enforcement officer coming to Leo can get to databases on, you know, the Homeland Security Information Network and so forth and so on. So those are just some examples of the incremental progress we're deriving.

You know, longer term, I think I'm going to defer that. I'll come back and answer that question, if you'll have me. But I want to defer that because I'm really hoping to hear from the audience about – about where we think we want to go.

I would say that I think within five years the idea that we're data-centric is, I think, a reality more than it's kind of a future.

MR. NELSON: Speaking of data-centric, I'd love to hear some of the industry experts in the room talk about and address some of the terms. You know, mega-tagging (sic) and other things that me (as ?) an engineer don't fully understand in the NSI-type architecture. So that's a good dialogue we can have as well.

I think we had a question right here, though.

Q: Good morning. Kristina Tanasichuk, from the Homeland Security and Defense Business Council.

I don't admire your job. I think you have a tremendous amount of work to do just to figure out how we can share information currently.

But to follow on to your question about the future, how is social mapping or almost offensive data collection playing into the future of the ISE? I think right now we're collecting information. We collect a tremendous amount of information, and sorting that and sharing that is certainly our first priority.

But going forward to kind of face tomorrow's battle, how are we using kind of the social networking and mapping tools that are being developed?

MR. PAUL: So a great example of using the web 2.0-type technology is the A-space application inside the intelligence community. It's a wiki collaboration platform that's very useful for different intelligence analysts to be able to collaborate and securely share information.

So you know, our charge is yes, this is information-sharing, but it's also collaboration around information. So you know, there's the unstructured information and the social sort of thing. So I think that's – a critical part of the information-sharing environment is effective social media integration. And, you know, the A-space is a great example of that.

MR. NELSON: Great. Any additional questions? Anyone else?

Oh, yes, sir. Right in front here.

Q: (Off mike.)

MR. NELSON: I think if you could wait for the microphone. I'm sorry.

Q: Peter Sherlock, MITRE Corporation. One perception of the problem faced by national security generally is that there is a very high ratio of noise to signal in all this data we're collecting. Could you address a little bit how the various initiatives that will promote interoperability and – both at the bits and bytes level and at the semantic level, would also help the problem of extracting the necessary signals from the abundant noise?

MR. PAUL: Yeah. That's a great question. Your question is, how do we raise the signal and decrease the noise.
And this was part of the reason why the connecting-the-dots metaphor is not so useful, because it doesn't really get to the quality of the dots, right? And, you know, an established best practice around information management is working upstream, trying to – you know, at the point of collection, getting the data in as clean as possible format.

And then also the different tagging schemes, how you describe the data. Meta tagging is data, about data, but it's descriptors around the actual data you collect – so that to the extent that that tagging is well designed, so it supports downstream comparison.

And so a great example is with the suspicious activity reporting initiative that I talked about earlier. A key part of the work was getting all the different communities to agree on standard code lists for describing behavior-based activity or you call it a car, you call it a vehicle, right? And so no, no, we're going to call it a car, right? And things like that.
Those are some of the examples for how we think about that issue. But it's a core issue. It's about sharing and discovery of information, but discovery only works if the information is described in consistent ways from the point of view of the person that's trying to discover, right? The information comes from different domains, so there's that standardization issue.

You know, fusion only works if you're able to correlate data, right? But then that implies a certain high level of quality. So you're exactly right that the data quality issue is a core issue, and needs to be engineered into the solution. It can't be dealt with as an afterthought.

MR. NELSON: Yes, ma'am. Right in front here.

Q: Hi. Adriane Lapointe, CSIS.

I've got a question that relates to the discovery issue. At one point at least – it may be in 2007 when I was more familiar with what your office was doing, attribute-based access was the mechanism to determine who would be able to discover, as opposed to access information.

Is that still the approach? And if so, how is it going? If not, what approach are you taking?

MR. PAUL: So the question is attribute-based access controls or how do we, you know, make sure that somebody that's accessing the data has the proper authorization to, you know, access that data. Some refer to that as authorized use.

It's the right idea. You know, attribute-and role-based access control. The challenge comes in that the policies to describe do you have access, the right to access this information? Some of those policies are information assurance policies. Some might be a U.S. persons rule. Some might be, you know, a variety of other rules that are coming out of different domains, different agencies that are described potentially in different ways that would make it difficult to automate the evaluation of those rules to make a judgment, you know, in real time, right?

So this goes to the issue of looking across the different policies, there's a degree of harmonization that may need to occur so that the policies are described in consistent ways, so then those policies then can be automated in a consistent way across the ISE.

So that's a – the technology, it works. It's established. But doing it at scale and across these different domains, right? That becomes the hard issue.

We actually did a pilot with NIST over the last year, and I think we described it in our annual report. And the hard part of the pilot wasn't the technology. That's all – you know, that all works pretty well. It was the effort taken to take, you know, text-based policies that weren't written with an eye towards automation, and then turning them into rules. And then is that actually a valid expression of that policy that'll satisfy, you know, legal and decision-makers?

In some ways this is similar to the journey that we went through as a country with digital signatures. Now we accept digital signatures, but it took a long time for, you know, the legal and cultural to catch up with the technology. The technology was ready for digital signatures well in advance of the wide-based market – market support.

So I see it as an analogy, you know, and our challenge is to try to accelerate that by working with our partners in the policy community and elsewhere.

MR. NELSON: Yes – the microphone's coming from behind you.

Q: Hi. I'm Wendy Walsh from the Naval Post Graduate School. And you just mentioned the word "cultural," and you had mentioned it in your talk as well.

What are you finding as far as looking at the issues of trust and culture, and how can we build that in our information-exchange environments?

MR. PAUL: Thank you so much for asking about culture and trust. These are core – core issues.

It's – you know, one of the things that I've found so refreshing in my time in public service is that there is a commitment to sharing, and I've seen that commitment grow in the last five years that I've been working in the federal government.

And looking across , you know, mission partners, there's a commitment to sharing. It becomes difficult dealing with the legitimate policy issues that sort of get in the way sometimes or the need to express these policy issues and negotiate them because they're – we're coming at the same issue from different domains, and things like that. So I see the – a lot of sharing.

I think that from a cultural perspective, the – we're ready to take that next step to go from, you know, need-to-share, to need-to-share-well. Right? And this comes with ideas like establishing a learning culture, having metrics around how we share to help inform operational and management activity.

So one of the ideas that we're trying to pursue, interested in pursuing as part of the national strategy here, is what does it mean to have a learning culture around sharing? How do we make sure that we have more cross-cutting metrics that are shared across agencies on similar capabilities, technically enable capabilities or mission processes.

A simple example is I talked about the SPU networks' interoperability initiative. So we want to make sure that we can count the number of users in an SBU network, whether it's FBI's LEO, DHS's HSIN, DNI's IntelliLink, or DOJ's grant-funded, state-owned RISSNet, in a consistent way, all right?

So we can (see ?) how many users do you have? Sounds like it's pretty simple, right? But it's – actually gets complex, to make sure that you're counting in the same way. Counting is – because you want to be precise about it. You've got to do deconfliction of duplicates and things like that.

Then you want to say, okay, I want to measure how often these networks are used, and used – and how many of those uses does somebody access a database in another network?

Again, these are pretty simple metrics, but it gets slightly complicated when you want to have the same, precise measure coming from different organizations and entities so you can roll it up.

Collecting those kinds of measures gives feedback, right? Feedback that can drive changes in a data-driven way. So that helps you with this idea of a learning culture and so we're looking at other opportunities to explore that learning culture idea.

Q: (Off mike.)

MR. NELSON: Sir?

Q: Hi. I'm Bruce Walker from Northrop Grumman.

It occurs to me in the – in the conversation that we've talked about discovery; we've talked about trust and sharing environments. But there's another use for the word discovery in the legal community, and I just – I wonder whether this horizontal integration that you talk about is potentially subject to a court order or some other change in our legal system that pierces the veil, so to speak, and opens this all up to examination for discovery in support of somebody's defense.

And I don't know if you all have thought through the unintended consequences of the application of the technology at that level, but it seems to me that we may be exposed here in a way that will be very hard to fix once it's – once the door's open.

MR. PAUL: Yeah. So the question is about discovery. Yeah, that's a really good question. People are aware of that issue, so there is an awareness of the issue. And it manifests itself in a lot of different ways, but there is an awareness of that issue.

One of the – one of the aspects of the information-sharing environment that was called for in law and is important to providing confidence to people that policies, whether they're – policies around strengthening privacy, civil liberties and civil rights or policies around information assurance or other information-sharing policies, are effectively implemented, is auditing capabilities, right?

So making sure that different activities across the information-sharing environment is logged in a high-integrity way that is consistent across different participants in the ISE so that you can look across and understand what's going on and understand that the policies and stuff are being followed.

MR. NELSON: See, now we're starting to get to the good questions. Any other questions from the audience? Other questions?

Kshemendra, again, will this – the reason why we're doing this, again, is to – and these are great questions. And I think these are the questions that ISE wants us to address.

Instead of building the strategy in a vacuum in their government offices, they're coming to the – to us, the public, you know, the industry, the government people that have to work this from different departments' agencies, the professional organizations, state and local governments, in saying give us – to get at – where are the questions we need to answer in this strategy, and what are some of the concerns that we need to take into account? And I think it's critical; I think it's very important.

So again, we need to keep that in mind that we are – we are doing a job here today for the ISE team and trying to help them out and to get these very critical issues addressed in there.

Any additional questions? All right, Dan.

Q: All right. The PMIC you talked about is an enabler, and you talked about getting to the point in the future where you really do have best practices.

Can you sort of envision the point, though, where the PMIC does get to that place where it doesn't just give broad guidance that you shall protect civil liberties, for example, or you – but it actually gets to the how – it starts recommending best practices, for example, for encryption or for anonymization or for data retention across what are very disparate organizations? When does it get to the point, if ever, of actually doing a little more of the how in terms of how it tells other groups to do things?

MR. PAUL: So the question is when do we get to the how, and the answer is we're doing that today, actually.

You know, we do that at the – at the business process level. I mean, when I – when we use the word "function standard" – or functional standards of business process, standard in exchange. So with the suspicious activity reporting, there's a certain business process that's mandated in terms of what the SAR looks like, to generate a SAR and to share it.

We're doing it in terms of technical standards and – we call them segment architectures, but they're a set of standards around interoperability for the SBU networks. And for our other initiatives in similar – kinds of things.

So I think we're doing it now, and I see us being more prescriptive in the future, right? That's the power of standards-based innovation.

One of the core challenges we have is when you look across the ISE, it's a – it's a huge space, lots of different participants – federal agencies, state, local, tribal and territorial governments, the private sector. It's a huge space.

To the extent that we can help standardize some – at the exchange, right? Not the internal processes, but the exchange – so that people can mesh what they're doing and then we can work with our partners in industry to say here's a standard. Here's an interface standard; it's at the business process, the technical level, right? It allows our industry partners to start to bake those capabilities into their products and services and make them more accessible.
You know, a great example of – when you think about state and local governments, there's 18,000 police departments in this country. We're inherently very federated, decentralized, from a law enforcement perspective.

You get past the major cities, the very big forces, and it gets to be very challenging for small, mid-sized police departments to effectively integrate into the ISE because they can't invest in customized solutions. They need to have solutions that are basically standards-based.

So that's, you know, part of what we – what we want to do, is to become increasingly prescriptive, not in a vacuum, but with our mission partners, right? This is really critical. We're not out in front; we're bringing them together, common mission equities, but coming to agreement and the leveraging industries so that – and working with industries so that we can bring those kinds of solutions to bear.

MR. NELSON: Okay, great. Any other questions?

Okay, well, before we thank Kshemendra, we'll take a short break and we'll reconvene here at 9:45. But I'd like to note that this is Kshemendra's first major speech as the PM-ISE. I think he set a high bar with so much substance in his speech, and I hope it continues in that trend, because it's very useful for those of us that are trying to help get our arms around this.

So let's give Kshemendra a warm round of applause, please. (Applause.)

(END)