

Center for Strategic and International Studies (CSIS)

Rethinking Identity Management Keynote

Moderators:

**Rick “Ozzie” Nelson,
Director of the Homeland Security,
CSIS;**

**Brian Seagrave,
Vice President for Homeland Security,
Raytheon**

Speaker:

**Howard Schmidt,
Cyber-Security Coordinator for the Obama Administration**

**Location: B-1 Conference Room, Center for Strategic and International
Studies, Washington, D.C.**

Time: 9:30 a.m. EST

Date: Tuesday, January 31, 2012

*Transcript by
Federal News Service
Washington, D.C.*

RICK "OZZIE" NELSON: OK. Well, welcome everyone. We're going to go ahead and get started on time. Hopefully everyone has got something to eat and a beverage in front of them. We've got a great conference today on a very interesting, fascinating and important topic. My name is Rick "Ozzie" Nelson. I'm director of the Homeland Security and Counterterrorism program here at CSIS. We're nonprofit at CSIS, so we're really dependent upon outside supporters to make terrific events like this happen. So first thing I need to do is to thank our sponsor for today's event, is Raytheon.

With that, I'd like to introduce the – one of our – the senior – the vice president for homeland security, Brian Seagrave. He's going to come up here and introduce our special guest, Mr. Howard Schmidt, special assistant to the president for cyber. He is on a very tight timeline. We're actually thrilled that he made time in his schedule to come over here and give us some remarks. He's going to do about 20 minutes of remarks followed by about 10 minutes of questions and answers, moderated by me. And those of you that know me means it's questions only, no statements.

So without further ado, I'm going to ahead and introduce Brian Seagrave who'll introduce Howard. Thank you.

BRIAN SEAGRAVE: But I get to make a statement first. So first, thank you, CSIS, for hosting this event. And we're very pleased to work with CSIS as an industry partner in giving visibility to the topic of identity management today. Raytheon works with civil security agencies around the world to address their mission challenges, and management of identity – the credentials and access – is a core enabler that spans across all the security missions that we help customers with – border security, immigration control, critical infrastructure protection, you name it.

And while we're out there around the world, we're amazed at the functionality that other countries are offering their citizens – for example, single national identity credentials that authenticate for financial services, health services, voting, electronic voting, drivers licenses and even physical and logical access within government agencies, all on the same credential.

And yet, across our base, we also see customers confronting a number of overlapping challenges: challenges in how agencies move to interoperability and a person-centric view from their legacy systems; challenges taking advantage of advances in biometrics technology in addressing the overload of biometric systems; and doing all these things while protecting privacy and confidentiality. These challenges are compounded in the cyberarena, and the WikiLeaks incident actually really underscores the importance of strong identity management and insider monitoring as a precondition to information sharing.

And then there is our need to foster trusted identity in cyberspace. As a core member of the defense industrial base, Raytheon believes that the way the DIB addressed federated identity authentication provides a model that can address many of the broader challenges that we have today. We believe all these challenges can best be addressed through a partnership between government and industry where both critical systems and critical know-how reside.

And that's why the United States is fortunate to have someone that – who has had such a long and distinguished career in both government and industry now coordinating cyberpolicy cybersecurity efforts for the White House. Howard Schmidt has had a distinguished career spanning more than 40 years in defense, law enforcement and corporate security. Since 2009 he has served as the president's coordinator for cybersecurity, and he's a long-standing expert in the areas of computer security, cybercrime, critical infrastructure protection and business risks related to cyber security.

Mr. Schmidt was formerly the president and CEO of Information Security Forum, a nonprofit consortium that conducts research and develops best practices in information security, risk management and critical infrastructure protection. He has held executive roles in the private sector, including vice president and CISO at eBay and chief security officer for Microsoft.

Mr. Schmidt's government service has included previous assignments at the White House, the FBI, the Air Force Office of Special Investigations, including tours as a supervisory special agent, supervisory special agent and director of the computers forensics lab, and computer crime and information warfare division.

His military career includes active duties with the U.S. Air Force, with the Arizona Air National Guard as a computer and communications specialist, and in the U.S. Army Reserve as a special agent, Criminal Investigative Division, where, until his retirement, he served with the Computer Crime Investigations Unit.

Mr. Schmidt is a professor of research at Idaho State University, adjunct professor at Georgia Tech Information Security Center, adjunct distinguished fellow with Carnegie Mellon CyLab, and a distinguished fellow at – of the Poneman Privacy Institute. He's also received numerous awards and recognitions from government and private industry, including the CSO magazine Compass Award and Baseline magazine's 50 most influential people in business IT, to just name a few.

Ladies and gentlemen, please welcome Howard Schmidt. (Applause.)

HOWARD SCHMIDT: Brian, thank you very much for that kind introduction. And Rick, I'd like to thank you and CSIS for putting this group together. I think your opening comment about, you know, these things are made possible because of support from other people bringing together, but we need more of these. And we very much appreciate you hosting this. And my dear friend John Hamre runs a great shop here. And we're very proud to be over here today.

I don't want to spend a whole lot of time telling you stuff you've heard before, so I'm going to try to focus my comments specifically around the topic. A couple little highlights, because there's a lot of – I used the comment yesterday – noise going on right now about cybersecurity – everything from legislative issues to some of the threats we see out there in the real world. So I'm going to talk a little bit about some of the things that are going on, just to sort of update you as some of the things we're doing.

But clearly, the crux of a lot of things we're doing come into the area of identity management or what we call trusted identities in cyberspace. And I think a lot of this, as we've seen technology grow, as we've seen the advances in interconnectivity issues move forward, we've seen a need for identity management like we've never seen before. But on the same token, the exact same things we're using for stronger authentication also create their own set of challenges that we've got to overcome. Part of it is designing the systems that can accept the things that we're working with.

So it's been a busy year for all of us, at least in the little group that I work with at the White House and across the U.S. government. I know you all have been very busy. And as I made in a comment during a VTC (ph) yesterday, was: notwithstanding all the things that we've been talking about that are out there in the risk, because of the work that all of you do on a day-to-day basis, and Brian, and all the folks that are part of companies that keep this thing going – everything still works.

And we may have hiccups in it. You know, in some cases I liken them to the disruption we have during snowstorms which, those of us that live hear locally – remember when we used to have snowstorms in January? (Laughter.) Sixty-five degrees outside today. But when we look at the disruptions, we recognize that we are able to recover from them quicker than we've ever been in the past, but we cannot lose the fact that things could get worse. And so we have to make sure that we continue to work to reduce that likelihood.

So a little bit about the office. When the president created this office, as part of the National Security Staff, at the time there was the split National Security Council and Homeland Security Council. We've all merged. We're also dual hatted with the National Economic Council. And I think that is one of the things that really sets us apart from some of the previous efforts that have taken place, is we have the focus – not only national security and public safety, but also the economic components of cybersecurity.

The staff – and we are very, very fortunate to have some of the best across government – from the Department of Justice, Homeland Security, the intelligence agencies, the Department of Commerce, FTC – that help us work on individual problems as we move forward, developed a good policy, worked with the departments and agencies to take very discrete views that departments and agencies have.

As we were talking before we came in here, there's a lot of herding of cats involved. And some would say, geez, isn't there a tension between this particular department and this one over here, and the answer is, yes, I hope so. We do want to hear what their expertise is. We want to hear how they deal with a specific issue. But we want to normalize it so we can come up with a good policy that takes into account all the components that we work with. And we've got a good team to pull that together.

For those of you that listen to or watched the State of the Union speech last week, the president stated very early that the executive branch and the White House is focused on

achieving these strategic initiatives, particularly with the proposed legislation that we've put forth that Congress will be putting a lot of attention here in the next week or two back.

We've also done a pretty good job, I think, of actually prioritizing things. I see John Gilligan here and a few other folks that have run enterprises, and nothing is more troublesome than when you say, you know, here's 50 security issues you've got to deal with, prioritize them, and they're all priority one. That's life in the real world.

So we've actually set about and said, OK, what are some of the things? How do we prioritize these? How do we expedite the traditional low-hanging fruit while making sure we're reducing vulnerabilities that we know exist while still building for the future? So it's very important, as we do these things, that we actually have some milestones and specific priorities that we're looking at. And in this venue today, of course, the thing that we'll be talking about is the effective identity management and all the things we can benefit from that.

You know, I could spend some time talking about the threats out there. People talk about hackers, nation states, criminal organizations and everything else. The bottom line is, if we had less vulnerabilities, they would be less successful. When I look at the law enforcement community and when I look at the men and women that, on a day-to-day basis, have to manage these systems from a security perspective, provide the services – whether it's government or businesses – and the things that they have to deal with, clearly we'd like to take a whole lot of that off their shoulders by saying, we can stop the threats out there.

I think anybody that's been in this business for any length of time know, we – (inaudible) – not going to be able to stop the threats. We'll be able to get some small chunks of successes, as we've seen with the law enforcement going after some of the criminal activities that control some of the bot networks; working very closely with private sector; using civil actions; using criminal actions. But clearly, oftentimes we see another group will pop up to replace them.

But once again, the things that we can control is the vulnerabilities that exist in our systems, who's on our systems and how we wind up better hardening our systems – so wherever the threat comes from, the likelihood of success is reduced.

So zeroing in a little bit, I want to just take a few minutes to talk about the NSTIC, the National Strategy for Trusted Identities in Cyberspace. Jeremy, I saw you walk in – there you are. Jeremy came in a few minutes ago. We were very fortunate to lure him away to run our program office, the Department of Commerce on that.

When we rolled this out at the U.S. Chamber of Commerce last year, it was a true testament to the amount of support we had on this. We had the president's national economic adviser; we had one of the most informed and vocal senators, Senator Mikulski, as part of it; we had the chamber hosting this for us – so clearly a recognition there is a lot of moving parts to this trusted identities in cyberspace.

The basic vision is to build an identity ecosystem that provides individual with an option of using a federated, user-centric digital credential to conduct transactions with more security.

Simply stated is, we have a choice. If I want to just do a small transaction, I can choose to use one identity over here. If I have something more robust, I have the ability and also the institution I'm working with has the capability providing me the ability to have a higher level of assurance.

To move away what I think all of us recognize: A static user ID and passwords should have been declared dead years ago. Matter of fact, I remember another CSIS event, probably in about 2001, that we had that same discussion. And here we are almost 11 year – 11 years later, and I think we're finally making progress on this. We're finally having a mechanism to move this forward.

But the other thing it wants to do is, we want the private sector to give us the capabilities to be able to draw on a marketplace of identity providers – both public and private – to say, here's the choices you have. I was trying to explain to someone what a OTP, one-time password, was on a mobile device. They understood what we call a smart card, because it – you know, it resembles an ATM card. So they said, well, why would I use something that I don't know about when I have this card here thing that I can use? And that's the thing we're trying to do, is provide options for people.

But on the same token, in these options we want to make sure we're not sort of reliving the problems we had in the past. PIN and chip technology: great technology, but people have since figured out how to break some of the encryption on there. They've looked for the man-in-the-middle attacks. So we know that now.

So we should not saying, OK, the answer is, here's new PIN and chip cards, and everybody go out and use these because they're – it's different than what we've been doing. We have to build these things with the ability to say, here's what we've done to make these better than what they are now; to understand there's likely to be a man-in-the-middle attacks; to understand you're likely to be operating from a computer system, at least for now, that's likely to be compromised. And how can we still operate in that environment?

And that's not something you're going to get five people in the government to say, yeah, here's the answers, go forth and do this. It's going to take the intellectual capital that we have in the private sector, in the security community, in the VC community – entrepreneurs coming and saying: Here's a better way to do this that's easy to use, cost-effective and gives us options.

The next thing is, looking at that interoperable framework. That's why it's very important that we've got Commerce and NIST working with private sector, saying: What are the standards that we're looking at? Had a meeting this morning with one of our international – my international counterpart. And we were talking about trusted identities, and what they're wrestling with at their government – everything from taxing to service that they provide for health services – basically the same thing we're doing. And when you look at some of the great advances we've made – and we still have a long way to go – is what VA does now with the big Blue Button button: you know, the ability to consolidate this stuff.

One of the things that I probably shouldn't say but I do is – just before the lighting ceremony in the Ellipse last year, there was an email that went out that says, any of us, we can

put in for this lottery to actually be there on the grounds when the lights get turned on. And I thought, wow, that was really neat; clicked the link, and it took me to a website that I had to create an account to be put in for a lottery – and my cynical (manner said?) to be turned down – and had to create an account with a user ID and password.

And the good news is, next year I can use that same account, if I remember the user ID and password – (laughter) – because, as a security professional, we tell people, do not re-use these things over and over again. So I try to stick to that as much as I can; I'm not perfect, but as much as I can. So I'll never remember that next year.

So we need to have a mechanism with a framework that's interoperable. We – as a matter of fact, we just released and released a memo from the OMB and in my office, telling government agencies: Stop creating these accounts; stop trying to manage this; stop being the help desk for every citizen in the world; use outside credentials. They exist. And we have the General Service Administration or GSA working with NIST and working with Homeland Security to make sure that these are ones that we can use.

So you shouldn't have to have, in the case of some of us, a half a dozen or so government logons to find out what your VA benefits are, or to get – find out what your tax liability is, or what your Social Security benefits are, when we have other options to do that. And varying degrees of assurances, we move through that.

So – and if – from the government's perspective on this, we will be a facilitator. We will bring the people together. We can help convene a lot of these things. But the government will also be a customer of these. And I think there's nothing better than having some identity that I use in an e-commerce environment, I can use that same environment in the government. So as a consumer, the government is very important, as saying: You build it, and we'll use it as well. And we have to actually put our money where our mouth is. And I know, Jeremy, we've made sure that the funding is there to actually do some of these things that we need to do.

The other piece is when we are looking to streamline the customer experience. I mean, that's tremendously frustrating. Private sector has spent a lot of time and a lot of effort trying to make sure the user experience is as positive as possible. It's a business thing: They want you to come back as a customer. And quite honestly, if they give me a good experience, I'll be back – whether it's to an airline, hotel, whatever it will be. But the bottom line is, we have to have a mechanism to do the same thing in the government. And that's what the government's looking to do.

The other thing we need to do is set up a governance framework. Once again, the comment we had this morning – we – we're still, in some cases, running around with 18th-century laws and 21st-century technology. So when it looks to identity management, we look to the private sector to build this. But how do we wind up dealing with some of the things that just are normal part of business?

A company may be our service provider. For whatever reason, they go out of business; they take a wrong turn somewhere. And how do we protect people against that? What is the

governance mechanism in place that says: OK, company's out of business, and their value in their company is the data that they've got about us. How do we deal with that?

We've seen that, couple years ago, with one of the trusted traveler programs. We saw it even a few years back with a child's website that had tremendous amount of information. It went up in receivership, and the bankruptcy court says, yeah, the only value you have is this information, all these children – that we as parents, as grandparents say, we don't want that being sold off to the highest bidder.

So these are some of the things that we have to build in this identity ecosystem to better protect us, because we don't want to have someone go out there with 99.9 percent legitimate businesses out there, and that .1 (percent) that says, that's a good way to commit identity theft and credit card fraud. I'll open up a company, collect all this stuff – you know, take advantage of all these people, then shutter my doors and move away. We have to have a mechanism in place to be able to deal with that.

We also want to make sure we have a system that does not have sort of this, you know, one-size-fits-all identity. One of the criticisms many of us have had for a long time is, I have a single logon that gives me access to everything in the world. That means, if and when it gets compromised, everything I own and everything I have access to is then compromised. And that's a choice that we get to make; and that's a choice that we have to have the system designed and built to have to deal with.

So when we look at some of the things we're looking to solve: First and foremost, deal with some of the issues of cybercrime, online identity theft, financial fraud, online theft of intellectual property – all these things that we deal with, we're looking to solve some of those things. We've seen – while a lot of people maybe call these things advanced persistent threats, some of us don't think they're that advanced.

We think they're very determined, but when you look at the – sort of the analysis of how these things really happen, oftentimes starting with a spear phishing email or a phishing email with a piece of malware attached that then gives you a back door to find vulnerabilities and escalate privilege – that's pretty determined.

But some of the things that we can do in identity management would actually be able to resolve some of that – including the ability, when I get an email – or any of us get an email – it's – the onus should not be on the end user (ph) – end user to figure out, is that real or is it a piece of malware? But that's what we do today. Every – most things get through, unless there's a signature out there that says, this is known bad. It goes through, and somebody says, yeah, this is my 2012 benefits, pay raise – you know, holiday schedule. And you can bet, most people will click on it.

We've seen some states that have tried some pilots, where they've sent emails out as part of an education system. And 86 percent of the people click on it because it appears to be legitimate, even though they sent it from an outside email address. I – good identity management should resolve that problem for us, so the end user is never confronted with this.

And whether you would call it certified email, or whatever term you want to associate with it, that's some of the thing that we're looking to solve.

But let's take it up to a more critical issue, and that's critical infrastructure. Whether it's the energy sector, transportation sector, financial sector – the bottom line is, we basically have seen the same thing happening in that environment. So having better trusted identities, having strong authentications into these systems. And more specifically, in industrial control systems that many generations have built – never designed to work in a network environment, let alone a network environment that's connected to the Internet.

So as we look to do trusted identities, while we think about individual interacting with a machine, we also have to understand the machine-to-machine interaction and build identity management into that as well, that gives us the ability to do authentication, gives us the ability to do encryption – some of the things that we really need to do on a regular basis.

The other piece of this when we start looking at some of the things about NSTIC and the things it can do for us is it has to be interoperable worldwide. And I mentioned that before, and I think that's vitally important. If we're going to continue to be successful in a digital world from an economic perspective, there shouldn't be 110 different systems. We should not say, yeah, when I go to the U.K., I get to do this. When I go to Australia, I get to do this. And that's going to be just as confusing and less likely people would adopt it if they need to do all these different things, because when you look at the basis of it, we're looking for something easy to do what we want to do. And these are the thing we need to do as we move forward.

So on that, just in closing, couple things that relate to that, the International Strategy on Cyberspace – openness and prosperity in cyberspace – that when we released that – released that strategy last year, it wasn't a strategy on cybersecurity. It was international strategy for cyberspace. Part of that also talks about digital identities and identity management on an international platform, while we pull into that. And the last thing that I want to touch on before I – (inaudible) – for questions and that's inside the government. I think many of us, both when we've been in government and outside of government, have said many times is, it's really difficult for the government to ask people to do – private sector to do stuff that the government's not willing to do. And that's truly the thing we need to do.

We released a memo on use of multifactor authentication. It was really an interesting thing to find out that 76 percent of the people that should be having a PIV card or issue a pid – PIV card, that very, very few of them are using it because there was no requirement. We flipped that around. So not only do you get it, but you actually have to use it. And some of the first things are for logical access. We're going to be bumping that up to digitally signing email. Eventually we'll be using it for S/MIME and an encryption of the email. And the bottom line is the technology exists. We've just not implemented the policies and enforced those to move this thing forward. So when we look at HS – Homeland Security Presidential Directive Number 12 and how it's languished for years, that's been accelerated and something we need to continue to deal with. And we will make sure that the expertise is there to help departments and agencies move this thing forward.

So in conclusion, I just want to – few comments, the things that we’re looking at is knowing what is in our network, all the devices, how the devices interact, the mechanism for those to interact securely; know what is coming in and out of that network – if it’s not signed, if it’s not digitally certified, I don’t want to see it hitting my network, or I want to have some mechanism to sandbox; I want to have some mechanism to make sure that we’re not introducing risk into the network that we shouldn’t be – and of course, knowing who’s on the network to the level required for the business that we’re going to transact. And that goes for – (inaudible) – anonymous access, just somebody to finding out what government service are available all the way up to and including something that’s more robust that says: This is really me. I’ve done in proof – proofing somewhere, and I can actually go out and say: This is me, and I need my VA records.

So with that, I thank all of you for coming together. I think this is a really good forum to discuss the things. And I know Jeremy’s here. And I’m sure Jeremy would love, as the rest of us would – (laughter) – to hear your ideas on things that we can move to accelerate this, because we’ve got a window to make this happen. And we don’t want to be discussing this again in 11 years from now. So thank you very much for the opportunity to discuss this with you. Thank you. (Applause.)

MR. NELSON: Well, thank you for those very candid and open remarks, Howard. It’s actually quite refreshing – an open forum like this – to get that kind of discussion. So we thank you for that. We have time for about five to seven minutes of questions. We’ll go ahead in standard CSIS format. We have microphones. Please state your name and your affiliation. And due to time, please limit to a question. So go ahead. We’ll start right here in the middle.

Q: Sorry. Jim Carney (sp) with Deloitte and Touche. What do you see as the fundamental stumbling block for why this hasn’t gone further faster? And what do you see as the White House role in trying to alleviate that stumbling block?

MR. SCHMIDT: Yeah, I think the biggest thing is we’ve not articulated a good business case for doing it. That – as I mentioned in my opening comments, things continue to work. You know, everything from a liability issue from a credit card fraud, identify theft – excuse me – financial fraud, the liability cap – is it \$50? So there has – it’s been sort of viewed as, yeah, I’m willing to absorb the losses and not do anything with it. But I think there is a bigger picture now. People that have recognized through the efforts that the White House and many of you in this room have said, it’s not just about the money. It’s the trust in the system. It’s the ability to build the system. And I think that’s what’s really got people thinking about this more than just, oh gee, there was a little loss that I can write off.

Venues like this are things that the White House is doing. We’ve got – we meet with Congress regularly. We meet with CEOs, the VCs – Jeremy’s office over there – I don’t know you’ve had, what, four or five workshops to date – continuously saying, here’s what we need, and asking private sector to build it. So I think there’s a whole different discussion today than what we had 11 years ago or even 3 years ago.

MR. NELSON: All right. Thank you for that.

That gentleman in the orange.

Q: Good morning. David McWhorter, Catalyst Partners. What is the mechanism for a company or, you know, maybe a client of mine or a company that I know that has something that we'd like to get in front of, you know, the entire group? I've been to the workshops. They're great. But you know, what's the mechanism for demonstrating to you the ideas of the company?

MR. SCHMIDT: Jeremy, stand up. You can demonstrate to Jeremy. (Laughter.) No, but seriously – and that's the one of the challenges we have. In – I think at the one meeting I was at, there were probably 30 or 40 different – I use the term start-ups, but they were in various stages. They had great technology; that they had put some effort into it, and weren't quite sure where they'd get the footing.

And that's one of the things we're working with Jeremy is, how does that become more public. Without endorsing any particular technology or endorsing any particular company, how do we get those that want to build the stuff, sort of a portal, if you would, that says: Here's the 50 options that are out there. Here's the status of fundings, whether they're just a founder and some angel investment or even a single investment or this is something that's done around B. And we have some customers out there, so people can see and make decisions on their own. That's the part we're lacking. And I think that's the next part. We need somebody to help us build – whether it's done through universities, whether it's done through Jeremy's office or NISC – a mechanism to sort of sift through these and figure out what's going to work best.

The downside, of course, like any of these things, we may miss something that's – that is the most rocking, greatest technology we've ever seen because somebody's just a small voice out there. And we want to put an equalizing platform in there through some sort of a portal.

MR. NELSON: Great. In the back.

MR. SCHMIDT: Oh, wait. I think it's a brown shirt, not an orange one. (Laughter.)

Q: Andrew Howell, Monument Policy Group.

MR. NELSON (?): Hey. How you doing?

Q: How are you?

MR. SCHMIDT: Good to see you.

Q: So, Howard, I want to pick up on a couple of things that you mentioned on HSPD-12 implementation and the fact that you just talked about business case. HSPD-12 is a good example of a program that, you know, departments and agencies have struggled to make the business case for investment. And in the tight budget environment where we are now, if you've turned the corner – can you talk a little bit about how you've turned the corner, in a tight budget

environment, on convincing departments and agencies to spend that money to increase assurance in identity?

MR. SCHMIDT: Yeah. Very simply stated is, it's not an option. It's not as, gee, you can do this if you want to. (Laughter.) I think that was the biggest thing we did last year, when Vivek and I put out the memo that said, no, this is not an option. This is a presidential directive. You come in with the plans. We've had tremendous success with senior leadership. And for those of you who'd have been in this environment for a while, it used to be this was a technology problem. It wasn't a business problem. And now we have the deputy secretaries across all the departments and agencies, basically they now have ownership of this. We have a – the President's Management Council. We bring them together. We go through their metrics. And they're held accountable for it.

In instances where they may be an issue of funding, that's where we look to do some reallocation of budget. In this austere time, said, yeah, this needs to be done. We may pull something from over here that can wait and make sure they've got it.

MR. NELSON: (Great ?). Last question. We'll go in – right there.

Q: Hi, Howard. Brian Benson (sp) with CA Technologies. You know, there's a big ROI associated with identity management. And in the commercial space, a lot of those companies have made their decision and their investments on that ROI. But I haven't seen a whole lot of that within the government, within the agencies. Are there any plans to use, whether it be an ROI calculator or showing the agencies that they can actually save money by going to – whether it be NSTIC or HSP-12 or FICAM or OMB 11-11?

MR. SCHMIDT: Yeah. And I think that we're probably way past that, because now that we've mandated it, it's kind of tough to go in and say, you have to do this, and here's the value you get. In the early days, they did some rough metrics, just in password help desk costs and those sort of things. But we've just got beyond that. Now there's a true value, and as we – as NSTIC expands, for private sector to say, gee, if we sell, you know, a hundred thousand credentials at a dollar a piece but it costs us 200,000 (dollars), you know, it's not a good return on that. How's that scale? How do we want – getting the costs down? That is what we're looking for in the private sector, because the government's going to be the consumer of that – not building our own. We want to get out of that business.

MR. NELSON: Well, great. These are awesome questions and great remarks, and I look forward to the rest of the day. I – again, I'd like to thank, you know, Brian Seagrave, Adam Isles from Raytheon for their sponsorship for this. And then, obviously, Howard, thank you for taking time out of your day for your candid remarks. (Applause.) We'll reconvene at 10:45.

(END)