



**HIT Standards Committee
Transport & Security Standards Workgroup
Final Transcript
October 22, 2014**

Presentation

Operator

All lines are bridged with the public.

Michelle Consolazio, MPH – FACA Lead/Policy Analyst – Office of the National Coordinator for Health Information Technology

Good afternoon everyone, this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the HIT Standards Committee's Transport & Security Standards Workgroup. This is a public call and there will be time for public comment at the end of the call. As a reminder, this meeting is being transcribed and recorded...and I just said that, I'm sorry. I'll now take roll. Dixie Baker?

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

I'm here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Lisa Gallagher?

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Lisa. Aaron Miri? Brian Freedman?

Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.

Hello, I'm here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Brian.

Brian Freedman, MS, CISSP, PMP, CHCO – Senior Information Assurance Analyst – Security Risk Solutions, Inc.

Hi.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Jason Taule? Jeff Brandt? John Hummel?

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

I'm here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, John. Lee Jones? Paul Clip?

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Peter Kaufman? I know Peter's on. Scott Rea? Sharon Terry? And Steven Lane?

Steven Lane, MD, MPH, FAAFP – EHR Ambulatory Physician Director – Sutter Health

Here.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Steven. Is there anyone from ONC on the line?

Mazen Yacoub, MBA – Healthcare Management Consultant

Hi, Mazen Yacoub, contract support is on the line.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Mazen.

Lucia C. Savage, JD – Chief Privacy Officer – Office of the National Coordinator for Health Information Technology

Hey Michelle, Lucia Savage is dialing in just to check it out.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Hi, Lucia. And just a reminder to everyone, if you aren't speaking if you could please mute your lines it would be appreciated and I will turn it over to you Dixie and Lisa.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Okay, thank you Michelle and thank you all for dialing in. I know we're very busy, especially this time of year, so we really appreciate you taking the time to participate in our workgroup. We really only have two primary items on the agenda for today. The first is that we are very close to finalizing our work plan for this year, very close means we've reached what we believe is a final work plan, but it hasn't been signed off by everyone yet, but we're fairly confident of it at this point, so we want to review it with you. And as we all know, work plans are subject to change along the way, but we did want to go over it with you so that you know the direction that we're heading and the kind of recommendations we'll be asked to give...we've been asked to give.

The second topic is a presentation by Paul Grassi about identity management. We've had several presentations around identity management and this one is a very good presentation, especially since its more of a...its very, very thought provoking and conversation provoking and we think it should be a very, very good discussion. So...and we want to thank Paul for being our guest speaker, today. Is he on the line? Oh, I think he said he may be dialing in a little late, actually.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Yes Dixie, we don't have him yet.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Okay. Lisa, do you want to add anything.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

No, I think you covered it, Dixie. Thank you.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Okay, then let's...let me bring...let's display the...I'm not sure we're going to show anything on the work plan. I believe...I know that the work plan was distributed, so we just wanted to point out...let me bring it up here, let's see, no, that's not it, there. We wanted to point out that a lot of what we've seen so far and the presentations that we've made, the discussions that we've had are around identity management and indeed identity management is one of the primary focus areas for us for this year's work plan at two levels. First is to make a recommendation, which we're currently anticipating to be presented in December, around identity management from a general perspective, authentication, authorization, identity proofing, etcetera.

The second aspect of it is as part of a broader topic of API security, electronic health record API security. There's another workgroup called the Architecture and Interop...is it Architecture and Interoperability, is that...or API...Architecture and API Workgroup, I think. Is that right Michelle, is that the official title of it?

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Architecture Services and APIs, yes.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Okay. And they are developing...they are defining an API that would allow query into an EHR. And we've been asked to look at that API from a perspective of security to include, but not limited it to the identity management. So that work will build on our work...our recommendation in identity management.

The third topic we'll be undertaking is consent management and there...the ONC has had for some time some work underway through the MITRE team to do a kind of a landscape survey of solutions that are available in identity management. So this topic will include a presentation of the results of that. And as you know, we've already had a presentation from...about the user managed access, which also relates to consent management.

Probably around end of year, beginning of 2015, ONC will be publishing a Notice of Proposed Rulemaking for the 2015 edition of the Certification...Standards and Certification Criteria for EHRs. So we will be asked to review that NPRM and we also will be asked to review the Interoperability Roadmap,

which is another activity that's underway at ONC now. It was, in fact, presented at the last Standards Committee.

So...and then the last thing on our list is data provenance, which will be toward the end of...probably around May or so and we're not sure at this point exactly how far we'll get into that topic. So, with that...I hope that that gives you some context for what we've been discussing and the recommendations that we've been asked to provide through this work here. Are there any questions? Okay, then I think...is Paul on the line yet? He's not. Lisa, could you at least start this off, I know that you've heard Paul give this presentation, would you feel comfortable getting the discussion started on it or...

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

I can give some background if that would be helpful.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Yeah, that would be very helpful, yeah.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So we, on this workgroup, we've had a number of discussions, as Dixie said, on the general topic of identity management. And we've also spent some time looking at some of the projects that are being done on the NSTIC, which is the National Strategy for Trusted Identities in Cyberspace. We have some folks participating on the Health Committee of the NSTIC, we have folks who are participating on a HIMSS Task Force on Identity Management, so there's a lot of activity.

With regard to the work that NIST has done, their guide...their special publication 800-...help me out Dixie, I can't remember...

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

63.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

...800-63-2 and there is an effort within NIST to take a look at that document and to take a look at the current state of technology around identity management as it pertains to the guidance they've given in that document. Paul Grassi is working at NIST and considered the subject matter expert on identity management or the portfolio owner; I'm not sure exactly what term they use. And I saw him give this briefing at an Identity Conference, a Global Identity Conference in Florida and what I found interesting was that NIST is doing a comprehensive inventory of all of their documents around identity management and the various components to see how much guidance they have, if there are holes in the guidance that they have, if there is any additional work that they need to do.

They are taking a look at whether we need yet another revision to that document, the 800-63 or if there is a need for an industry version of that document, and I put that in quotes because the question there would be, does NIST write it or does the IT industry or some sector-specific IT focus group put that together. They are looking at that as a topic. And interestingly, they're also revisiting the levels of assurance that are documented in 800-63 and I think it's...it's not just a caution of, do we have the LOAs right, but really as we go forward and technology continues to evolve, is that model going to serve us well?

And so when I saw this briefing I thought those are very intriguing questions. I think it's important for us to know that NIST has a point-person on this topic and that he is taking a comprehensive look at their entire portfolio of guidance documents. So, given where we were in the process and we've had several briefings and several discussions, I thought it would be very informative for us to take a look at what NIST is thinking about? What they're revisiting? What they're schedule is? How we can listen to what Paul says, give him some input perhaps from the health sector, have a dialogue, try to have some understanding of what's going to happen over the next year or two and how we can connect with him so that we stay up-to-date. So I thought a dialogue with this group and Paul, connecting him...connecting with the NIST function on identity management would be a good idea.

So that's a little bit of the background on it. I don't know Dixie if we...do you want to open it up to a discussion until we get Paul on the line or what should we do next?

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Well, are the people that are on the line, are you guys familiar with Special Publication 800-63 that's published by NIST? And Lisa mentioned the levels of assurance that are defined in that document. Are you familiar with those?

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

This is John Hummel, yes I am.

LeRoy E. Jones, MS – Chief Executive Officer – GSI Health

Yes, Lee Jones, I am also.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

This is Peter Kaufman, I am intimately familiar with it and we actually met with NIST and were responsible for 800-63-2 having some of the stuff about hospital and some of the other features of 800-63-2.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Yes, I remember you mentioning that.

Steven Lane, MD, MPH, FAAFP – EHR Ambulatory Physician Director – Sutter Health

And this Steven Lane and I am not familiar but I am going to print it out and read it.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Yeah.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, good.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Well the levels of assurance address sort of packages of identity proofing and authentication and management of encryption keys that together provide a certain level of assurance. In other words, depending on how sure you want to be that that person is who they claim to be. And when you were involved in the revision of it, is that what you said there?

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Peter...

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Oh yes.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yes, Peter Kaufman, maybe you can give us some background on your involvement with the revision.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Okay. Basically it's very difficult to, and not scalable, to identity proof every doctor in the country to a level 3 or 4. There are some online solutions, but the failure rate, even after a great deal of tweaking that was done with Experian was still, after three tries, almost 10%. And that doesn't seem that bad, 90% get through until you think that if you're identity proofing 500,000 doctors; that means that 50,000 doctors were unable to identity proof. So we needed a solution. Notaries don't want to be involved in this, although we were going to have in our pilot for the NSTIC IDESG pilot we were going to have notaries involved, but we didn't get funded for that.

So we needed another solution and since most doctors, not all these days, but most have privileges at a hospital and hospitals are doing more than a level 4 identity proofing, they're requiring things including your college diploma, not diploma, your college transcripts and your medical school transcripts and all your licensing information and face-to-face visits and an interview that it seemed reasonable to allow hospital medical staff offices that were going through that to do identity proofing.

So since DrFirst is literally right down the street from NIST, we went up and met with people at NIST to go over that that was me and Tom Sullivan and Michelle Soble-Lernor, who is our Chief Pharmacist. And they were very appreciative of our time and in agreement with what we said, but the person we met with immediately left and went to work for the Executive Branch of the federal government and the person who replaced him was pulled out of retirement to finish up a bunch of projects and this wasn't his highest priority, but he was a believer in it, he just needed to find time.

And they did finally kind of put it through and they put through very reasonable recommendations and we're about to start using hospitals for identity proofing here at DrFirst.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Well that's interesting.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Previously the ways to identity proof for a level 3 or 4, which is what's required for controlled drug ePrescribing involved either a face-to-face with the appropriate authority, and there were almost none of them around or online identity proofing with one of these companies like Experian that does it based on out-of-pocket data. But the out-of-pocket data for a level 3 or 4 involved financial information that most people didn't have ready on hand and also required a proof of address, which initially required an email...not an email, a snail mail letter, be sent to your house. So if you needed to use, for example, controlled drug ePrescribing, you'd have to wait at least a day if it was going to be FedEx'd or maybe several days to get that logged back in and put it in.

Then the other chair that NIST made was to allow a phone call or a text to a landline or to a cell phone that was billed to your home address. It couldn't be your business address; it had to be your home address. So if you had your phone billed to your home address, they could then immediately call and give you a code to put in and that would be proof that you had that address.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Um hmm.

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert

So this is Scott Rea over at DigiCert and we are a commercial certification authority. We are cross-certified with the Federal Bridge and we've actually been doing identity vetting in healthcare space under the Direct Project for quite some time now and Direct obviously requires LOA 3, but since we're issuing FBCA credentials, it's actually a little higher than LOA 3 because there's not an exact mapping between the NIST LOAs and the FBCA, the Federal Bridge Certification Authority, that is the FBCA, the Federal PKI LOAs.

So we've actually been issuing to a higher requirement of FBCA Medium for probably about 80% of the current Direct implementation. And we are generally, in that case, because we're doing Medium, we are doing the face-to-face aspect but we are leveraging, in a lot of cases, in most cases, a trusted agent at the healthcare facility, maybe in their HR Department, who have had to vet providers or workers who have privileges within the facility, etcetera, and we utilize them as a trusted agent. Or, worst case scenario, we are sending them to a notary, and we've done tens of thousands of these things and we don't seem to be having too much pushback from most folks in getting this done, in terms of issuing Direct credentials.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

That's the conclusion that the Privacy & Security Tiger Team reached that in most cases, providers do have face-to-face contact with the individuals, so that that could be done. And in those cases where it couldn't, there would be a notary or some sort...now, Scott, who are you talking about that's a commercial certification authority, when you say we? Who are you with?

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert

So, DigiCert.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Oh, DigiCert, okay.

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert

Yes. So DigiCert is a commercial certification authority. I'm also a Board Member for DirectTrust and so these are implementation of DirectTrust policies that I'm talking about here, but DigiCert is my employer and they are cross-certified with the Federal Bridge, more than a dozen LOAs and FBCA Medium is what we've targeted mostly for the Direct market and it doesn't seem to be too difficult to folks explaining what's needed. We capture the information, we can do the verification on the backend and as long as you utilize the process of a trusted agent and you have that relationship with that trusted agent, then that works pretty well.

And to be fair, in the Direct space, there may be a little bit of a difference than say for EPCS, because typically in the Direct space. If you're using a health information service provider, then you have basically a trusted introducer built in and...in not all cases. But that helps facilitate the process as well of

using a trusted agent. But like I said, we haven't seemed to have had too much issues with this; yes, we've had some folks who push back and you don't necessarily have to go to the financial data.

We've had folks push back who might not pass checks, etcetera, because we still validate...for FBCA Medium we still validate the credentials they present, even though it's done in person. And if they don't pass something, they might have to provide some additional data, you don't necessarily have to rely on financial data. We've had some push back on folks not wanting to provide that, but they're usually...enough to provide a utility bill or something along those lines. And so generally speaking, it's going pretty smoothly, I think.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Well that's really useful. Do you know whether there's any effort to do a mapping between the Federal Bridge and 800-63?

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert

Well so Kantara...well there is, if you like. So you can actually go to 800-63-2 and at the end of the document there is a mapping, it's really a one-way mapping if you like, but I heard earlier, and I apologize I got on a little bit late because the previous meeting ran over a little, but I heard earlier in the introduction that there was some talk about a revisit of identity proofing processes and I think that's a good thing to do and I really like what's been included in 800-63 in terms of, in the latest version -2, in terms of healthcare entities being utilized as trusted for the identity proofing process, as long as they have the appropriate controls in place. They have to demonstrate that.

I will point out that under the federal PKI policies, what...it does specify who is allowed to be that trusted agent. It is either somebody who is a state or federal entity that is approved for doing identity vetting processes. And as most folks will probably realize, under the eVerify Act...employers or somebody in the HR office fits that category and we've generally been leveraging that aspect and haven't had too many challenges with it.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

That's very useful, really useful insight. Okay, is Paul on the line yet?

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

I am here.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Oh, excellent. Excellent, we've just been talking about 800-63 and Peter Kaufman was involved in version 2 of it and Scott has been u...is very familiar with it, so we've gotten some background from our members while we were waiting for you. So we're glad that you were able to join us and we really appreciate your time.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

No problem, thanks for having me.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Okay, so with that, let me just turn it over to you.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

Great. Can I...do you want me to control this or just say next slide?

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Altarum, which is your...can you just turn it over to...

Lonnie Moore – Meetings Coordinator – Altarum Institute

Yeah, Paul, just say next slide and we will advance the slides for you.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Okay. All right.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

All right, there's some animation in here, I think, unless you converted it to PDF, so be aware of that. Well, good afternoon everyone, or good morning, I'm not sure where everybody's located. I'm Paul Grassi with NIST. I work in the National Strategy for Trusted Identities in Cyberspace, National Program Office. And I also have some responsibilities back at the NIST Information Technology Laboratory, working on the set of special publications that we have in the 800 series around identity and access management. Next slide, please.

So, I was brought on board to specifically look at the technology and standards landscape, which is quickly bleeding into some of the policy stuff as well, since documents like 800-63 is 100% backed by OMB Memorandum. So we can't really do a whole lot to that document, at least radical surgery to that document unless we get a policy update as well. So when I started I looked at, from an NSTIC and a federal identity perspective which includes providing services to the citizens or individuals that are looking for government benefits, I looked and said, we've got a good set of pilots that are working with diverse user sets and diverse relying parts, which is key to us.

Its one thing to talk amongst ourselves as identity SMEs, but it's a whole other thing if you're getting users and relying parties to adopt. We're starting to see commercialization of attributes. We're seeing...we've recognized a significant set of gaps in technology and policy that we need to address. F6, which is our version of kind of a third-party credentialing hub for citizens to get privacy-enhancing access to the government is going live, but we've still got a lot of serious gaps and so we get to the point where we've got this implemented, federated identity ecosystem working that's market-driven, user-centric, private, privacy enhancing, etcetera. Still too high to develop these systems, we still lack some level of consumer centricity, even with some of the better announcements today, in today's day around 2-factor auth, it's still not super easy and convenient, it costs users money.

We haven't figured out the liability model, we haven't completely figured out the business model. We might have some attribute providers, but they're community of interest focused, they're not ubiquitous, there are no standards around that. And then now a days Internet of Things is creating some great opportunity, but some significant identity challenges. And then one of my favorite kind of colloquialisms is Envision It, which was littered throughout the National Strategy of use cases we saw that could be possible with an identity ecosystem that was driven by the private sector. Next slide. And feel free to jump in at any time to ask questions.

So I won't read this to you, but this is an example of three of the Envision It's from the document that we have not achieved today. We might have achieved one of these bullets, we might have achieved one

of the three functions, but we really don't have interoperable credentials at large. We have secure credentials in the form of a lot of the social providers offering two-factor options with picking up on the end of the last conversation, with no identity proofing behind it, but they're not interoperable and they just kind of push the problem. Instead of having 10 passwords to manage, I now have 10 different tokens that I've got to manage, more secure but certainly not user-centric. Next slide, please.

But, we have great news coming out of at least the White House in an Executive Order that just was released a couple of weeks ago, I think it was October 17, there's the date, where we've recognized through a lot of the private sector breaches and frankly, some of our own that the way we are doing identity management and authentication today, even with the good work that NSTIC is doing and the good work that the private sector is doing and our movement towards a shared service around strong credentials, passwords still are the norm.

So the President signed an Executive Order to basically require two-factor authentication and effective identity proofing for all government services that have...make personal data accessible. This is something we're very happy about and we're looking forward to what this White House plan will look like in the middle of January that actually codifies how we're going to get there.

But from our perspective, and I think I say this in a later slide, this is our recognition that there's no such thing as a secure password. In essence, level 2 credentials for those who are familiar with 800-63 are dead and we're looking at a level 3 type paradigm, while retaining level 1 because we believe in anonymity, pseudo-anonymity and the benefits there. So we're not saying that everything, you know, passwords got to completely go, but when there is any amount of risk, especially when personal data is being released, that we step up our game. Next slide, please.

So this is my personal assessment, and I've run this through folks across government and in the private sector of where we're doing good and where we are not doing so good. And I use the royal we in this case, even though I've got it called out as NIST, because the whole of government is struggling with a lot of these items. And the reason I named it NIST is part of my job and the reason I was hired and my observation is that we could do a lot better in the guidance that we're putting out.

So, full coverage, the green items, those are sort of no-brainers. We've got a wonderful set of documents around the HSPD-PIV card, the FIPS 140-2, which is on cryptography. I don't see a whole lot of change going on there, other than the refinements as needed. In terms of where we need to start looking at things being refreshed, this is really kind of the "800-63 sweet spot." The proofing, all the authentication technologies that are out there, the innovation that the market has realized in the past, it's been almost 10 years since 63 was initially released, over 10 years since M04 was released. So, we're really going to start to take a hard look at that.

But that said, that's authentication only, authentication frankly should get you nothing so we have to look at the yellows and reds, because those are really where the rubber meets the road in terms of giving people the appropriate access to the right things and nothing more.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

What does linking/association mean?

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

Yeah, that's another thing going on, some of these are very...are not our favorite definition and we're actually going through a refresh of the FICAM at large, but that's essentially looking at the digital

identity that gets associated to a credential and linking that to your individual accounts in downstream applications.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

Oh I...okay, thanks.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

Typically, because we've got all these legacy applications out there and healthcare is no different, where you're given a username and password or something similar and then all of a sudden something like a PIV card comes along and the information on that PIV card has no association to the information in the system and you have to map that so that when I log in to an App with a PIV, it knows what account is actually mine.

So, there's a summary slide, but a lot of my time at least for the federally focused work, is going to be in really upping our game in terms of special publications, interagency reports around identity management. And where we can't do it in a special pub because it doesn't make sense to, we'll partner with the agencies that have the mandate and ability to take some of this on, GSA predominantly is the executive agent for identity in the government. Next slide, please.

So this is the summary I talked about in the next fiscal/calendar year, what we're looking at spending a lot of time on. We've been very focused on privacy, but we admit there are places we can do better and I have a slide near the end on what our specific problem is and what is our ask out to the private sector and in groups like yours, not only is there an ask but there are some things that we've been doing that we're looking forward to sharing. We've got to enhance our standards to establish confidence, trustworthiness and privacy preservation.

We've got to address the portability of preferred credentials and relying party accounts. This one is a little bit tricky, typically when you talk about federated identity you talk about portability of the federated credential. So, if I decide I want to use my Google account, it is "portable," because I can use that at multiple relying parties, multiple online service providers. But there's an issue with portability that hasn't really been addressed in the market or by government. I've done this, and it's almost like I told you to ask this question in advance, the linking and association process is very specific to the credential I show up with. Well, I've linked and associated my Google account with maybe 50 service providers, what if Google upsets me and I want to switch to something stronger or some other provider? Yeah who, Verizon, Facebook, whatever it may be, I've basically disassociated myself with the 50 accounts I've worked hard to build over time and how do I go to those relying parties in a standards-based way, in a secure way, in a private way to say, okay, this new credential that I prefer should really be linked and associated with the account that was prior associated with Google. That does not exist yet outside of proprietary and per relying party based ways.

Bring your own identity is another issue we're trying to tackle. Right now we're doing a lot of work in doing credential acquisitions, well what if you're acquiring a credential that I don't want to use, I'm using one that meets the security and privacy requirements of your federation, why can't I just show up with that and have it automatically accepted? And there is a lot of work going on in the identity ecosystem steering group that you may be familiar with that's looking at trust marks and automated kind of validation of the security and privacy requirements that you meet in a way that allows discovery and could realistically allow this bring your own identity capability.

In the other, under the key, we're looking at Internet of Things identity, non-intrusive security models, continuous monitoring and assessment. This is really kind of...outside of IoT, this is really looking at the

fact that the current state is pretty heavyweight audits and certifications and how do we make it easier? We've got an organization that has a military background that went through one of the FICAM processes and said, going through the FICAM to get our level 3 certification was worse than a tour in Iraq that cannot continue.

On the standards side, like I said, we're going to revisit and retool standards to potentially include 800-63 to address current market state and also be flexible for innovation. We're going to look at new standards that increase participation. We ourselves are going to increase our participation in open standards. And then again, looking at mobility, cloud and shared services.

And then for users and actual relying parties, we've got to figure out a way to make it easier, simpler, cheaper, faster to do full-blown identity and access management, not just the acceptance of the credential. It's ridiculous how much money is being spent to do basic identity management in government organizations. Focus beyond the PIV, establish toolkits and then identify and foster innovation from untapped resources. This is sort of a shameless plug for our pilot grants and trying to figure out ways to engage with communities that may not be associated with identity at all, but offer something that enhances our ecosystem and I would argue one of our most successful pilots is a company that would claim they're not an identity management firm. And that's great. Next slide, please.

So to the topic that was being discussed when I joined, on the right-hand side are some publications that are out there around identity proofing and on assurance, one of them being 800-63. What if we flip those on their heads, what if we did something else? And I won't necessarily read these to you, but there is a lot of conversation out in the industry, out in the private sector about componentizing the components that make up assurance rather than packaging them all in one draconian LOA and saying, you've got to do it this way or you're not compliant.

What if we completely got rid of LOA? What if we compressed LOA? Like I said earlier, level 2 really doesn't exist, there's no such thing as a secure password so why are we allowing level 2 to even continue on? And then level 4, I don't know of many applications, at least in government that need a citizen to carry a Smart Card. And if there is one, we'd like to know. And I should caveat, obviously getting rid of LOA would require M04 to get updated first, so we certainly need the policy function to be done before we can get into the technical weeds.

This private sector companion, it's not a role NIST typically plays, so we're just kind of seeing what type of reaction we get here. As NSTIC we participate in the non-profit IDESG, Identity Ecosystem Steering Group, and as part of that group we participate heavily in their committees, so what if something came out of there? What if we spent all of our time working in a private sector standards body as opposed to building our own 800-63 and pointed to that instead? And then what else, and this is an open question as we look at potentially modifying 63-2 before looking and responsive to the way the market is today. Next slide.

So this is just the discussion example of the vectors of trust. This is very, very preliminary, it's only to provide an example of one of the items that's out there that's gaining a little bit of momentum in competition, if you will, to scale or levels of assurance. No one's decided what are the components? No one's decided if each component has 1-4 levels or not even...but this is one way of looking at the problem, breaking it up into just identity proofing, credential strength, assertion presentation and binding as an example.

So this means, what if I have an application that I want to maintain a high level of security, but I don't really care if I know who the person is on the other line? I want to make sure it's the same person, but I don't care; well this allows us to have no proofing, but a strong credential. Assertion presentation is a highly technical component of it, but is important. Some protocols are very leaky, you have a strong

proofing and a strong credential, but as soon as you try to federate, it gets very leaky with the amount of data that can be accessed through the browser or through potential man in the middle. So, we want to make sure that we think about that.

Then a provider, an identity provider generically, I don't mean that term as a...to insinuate anything, could say look I can offer identity proofing levels 1-3, credential strengths 1 and 2, presentation 2 and 4 and provider 2 does something different. Provider 3 does something else and the relying party says, you know, my risk tolerance, yeah, it's not really level 1, 2, 3 or 4 from a level of assurance perspective, it's broken down in these components and I can go work with these modularized providers as I wish.

And in this model, the providers don't have to provide all of the components in this vector system, they can be just token managers, they can be just proofers. And you're seeing FICAM do that today in the way it's doing conformance and acquisition of identity services, though we still map them back to the levels of assurance. So, the business model supports breaking these up across different entities, but they still need to combine to form into something that's an LOA that's conformant with the relying party. And it also allows individuals to go out there and say, look, it's just really important for me to have a strong credential and pick/choose.

There's something not included here that I talked about earlier which is the trust mark scheme, which is a way for providers in an automated way with cryptography to essentially demonstrate to end users, hey, we meet these certain requirements, we meet the "seal of approval" and it also allows these relying parties to do discovery. So instead of having to do draconian contractual services and integration processes, they can actually search a trust frameworks registry, for example, and says hey, which providers meet the levels that I require among these components and out will come a result and poof, we can do discovery and linking. Next slide.

Sorry I'm rushing, I'm trying to make sure I get done in time for questions. These are some of the other components that are getting thrown around that could make up the vectors. What are some of the business processes? What are the...what's the maturity around...oh, and I'm sorry, I got things reversed. So on the business process side; it's really what are the backend processes around account management? We've seen that even something that's a two-factor credential could get taken over because the password recovery mechanism is an email address.

Organizational maturity is what are my security policies? What's my operational security posture? How do I manage incidents? There are legal components that could be there. And then there's a whole bucket of other things, reputational-based services, additional claims, heuristic compensating controls which is just a fancy way of saying, are you doing contextual adaptive based authentication like banks do today. Are you looking at where the IP...the IP address of the person? What time of day? Does it fit their typical profile? And that's really interesting, but I don't even claim to know how we would begin to measure that to say you're doing it in a way that's low, medium, high.

And then end-point security is interesting in the sense that if I'm offering a high-risk service, what is the security posture of the user's agent...user agent that's trying to access it? And do I need to do more because they're coming from Windows Millennium versus the latest patched version of a Mac? Next slide, please.

I think you can hit the button one more time and something will fly in. Nope, I'm sorry, all right. So, I'll quickly go over this. There's a lot of conversation around attributes and do we need to build a standard on it. And really with attributes it's the same type of conversation, is there a way on a per attribute level to calculate a level of assurance or level of confidence? And if there...if that is needed, who does it? And we're getting feedback on both sides of the coin and everything in between from don't do anything it's completely up to the relying party and the contracts they get into with attribute providers to let's attach

50 pieces of meta-data and calculate the level of confidence and assert that to the attribute providers so they can do something with it.

And in the middle are some additional thoughts, do we do attributes in 800-63 as well as just identity assurance? Do we, as I said, let RPs decide and do nothing? Address root causes is somewhat of a federal perspective, we're doing things on attributes because our business processes stink and I'm not sorry to say that, it's a little bit silly to me that we have to attach a level of confidence as to whether I'm a federal employee or not. I would say let's look at our HR process, not the attribute that says I'm a fed. Next slide.

Okay, so this gets in our privacy request. Our credential, Federal Cloud Credential Exchange soon to be known as Connect.gov is our citizen, individual facing credential broker, if you will, for...oops, my screen went blank, sorry...for allowing citizens to choose the credentials of their choice and do the business that they would like to do online with the government. It's primary privacy characteristics is allow...or enabling anonymity, unlinkability, unobservability, and that goes in both directions. So if I'm using Google to do business at the VA, Google has no idea that I'm going to the VA, they know I'm going to the government, because their through FCCX, but they don't know I'm going to the VA. And the VA doesn't know that I came from Google, nor does the VA know where else I've gone with that credential or any other one that I've had or that I've used. However, due to limitations in cryptography and the identity standards, attributes still flow freely, so FCCX is in a significant position of power. And the answer right now today is, we'll let the RP figure it out and we're not relying party and we think that's unacceptable.

So what we're starting to prototype, which is the next slide and which is our task is is there a way to profile some of the existing standards to get what we want. And a key point here is, by maintaining this blinding from the identity provider, i.e. Google and the relying party, VA, PKI doesn't work because you'd have to exchange keys, and if I wanted my attributes to be hidden from the broker, then Google would need to know to encrypt it with my public key and poof, the gig is up and they know who they're doing it with, so basic PKI doesn't work.

So they can't know the RP, we don't want the broker to see the attributes. The relying party can't know the CSP. We may soften that requirement. We want to do it in a standards-based and protocol agnostic way. And we want to do it with minimal changes to our infrastructure so that backward compatibility exists for those early adopters of this solution. We're making progress, we're playing around with some exotic cryptography as well as some key...inline key exchange that isn't today supported by SAML, but it still puts the broker in a somewhat position of power to be a man in the middle. We want to completely eradicate that and we're not all the way there yet. And I think that might be it, next slide.

Okay, so in summary, we NIST, we NSTIC and NSTIC really gives us an ability to be very...much mo...as private sector centric, if not more than NIST already is. But if you look at what we do in the 800 series, those are purely government only, so we're rebooting and reinvigorating our commitment to identity and we're looking at it, no bets are off, everything is on the table. It's not just about PIV and it's really about reacting to the market and allowing innovation and realizing that the private sector's doing a lot of really cool things that should be allowed in government.

We're not special, I think that kind of goes hand in hand with what I just said, but it also talks to what I said earlier around, why is this so hard? Why is it taking so long and so much money to build identity? I honestly think it's because we think we're special when we're really not.

We need to adopt private sector innovation. We all need to stop talking amongst ourselves, that's...I mentioned that earlier, this is really about user uptake and relying party uptake, not the identity providers and attribute providers and identity SMEs talking to each other, thinking they've got the best solution, which means our relying parties and users rule. And in keeping with NISTs transparent and

highly successful ways of interacting with the public and private sector, we're going to certainly be engaging in a range of ways on what we can best do with these special publications and other efforts to better serve the community at large. That's it; I think I went a little bit over, any questions for me?

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

This is Peter. You talked about, there's a lot of the stuff that was a little over my head and I'm clearly going to need to do a little more of my research on this. But I think that having a chance to get maybe an hour for those of us who don't understand all this with a question and answer might be really great, just to go through your slides and ask questions on each slide. But the one thing I did kind of understand that I couldn't see a way through was where you said having the relying party not know who the CSP is, how could they possibly accept a credential without knowing who the credential is coming from unless there's a government agency that'll just act as an intermediary or some other agency to act as an intermediary between the relying parties and the CSP. That sounds like a big and difficult way to do this, are there other things I'm not thinking of, of ways around that?

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

Nope, you've actually answered it. We do have a broker that's managing that for us, so...

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

They could do it for the whole world?

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

Well, right now it's doing it just for the access to government services.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Um hmm.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

We're not trying to do anything for the whole world; we're looking for an interoperable federation. It's probable that you could see models like this in communities of interest and we kind of have that already in things like InCommon and we're starting to see now the mobile operators are coming together to think about a way to broker identities so that smartphone holders can access relying party services in an interoperable way and the relying parties don't have to integrate with each operator independently.

But you're right, we...you're absolutely right, we have to have that broker in the middle that is essentially, beyond just doing the technical things, is the trust broker, that's maybe a better term. It's got the relationship with the CSP doing the validation that it's legitimate and then it repackages that information back to the relying party. The relying party trusts the broker and through that, implicitly trusts the CSP.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Is the next step going to be that there will be multiple brokers and then we'll say, well we don't want to know who the broker is either, don't want the relying party to know who the broker is either so we'll need a broker of brokers to separate out the brokers?

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

I don't know if we'll get that far, no, I think at least in our world, in the government space for FCCX, we're going to stick with the one. We may end up, to achieve some of our privacy goals, have to add an element here or there, but it's too early to tell and certainly, when it comes to more...we're looking for more identity services to connect to this, we're not interested in just CSPs that can give me a level 3 or level 4 credential, we're interested in attribute providers as well that can assert entitlements or other types of credentials about me, without necessarily being tied to issuing a credential as well.

M

Hey Paul, this is...

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates

This is Dixie, I need to check out now, I had told Lisa before I have a meeting that was called at the last minute that I need to get to. But I do want to thank you and Lisa will take over now coordinating with the question and answer, but thank you so much, I appreciate it.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

Thank you.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thanks Dixie. So, any other questions for Paul?

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

Yes. Hi, this is Paul Clip, Paul that was an interesting presentation, thank you. I guess I'm...I follow along with the previous comment and it seems like we're trying to build something very complicated and I wonder what the use cases are for this. If I go back to the we...the privacy profile slide, why do we need a broker at all? I mean, if I'm...my identity is with Google and I need to talk to the VA, why do I have to go through a complicated broker and then I'm still not sure when I look at those comments that the CSP can't know about me and I can't know about the CSP, but that may be requi...I mean, if I know I need to go talk to the VA, why do all of this?

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

So you as an individual, this is completely transparent to. You don't know that the broker's there at all, other than the fact that we are asserting and in our outreach and marketing campaign asserting certain privacy and security elements of this type of solution. It's the relying party, the VA that we are keeping from...we're blinding, if you will, from knowing CSPs users are going to and same with the CSPs.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

What is the privacy issue with that? What is the privacy issue of relying parties knowing what CSP it is?

Paul Clip, MBA, MSIN – Vice President, Platform Services – RelayHealth/McKesson

Yeah.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

It's the trackability side, we want to keep this completely unlinkable and not allow either side of the coin to know where users are going online. They should feel safe to go anywhere they want without necessarily being tracked.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

But the broker knows where they're going.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

Well the broker does, which is why it's in a position of power and the mechanics of the broker...internals of the broker is everything's done with meaningless but unique numbers, so there's no PII, no identifiable information in there. So if you were a bad actor and got access to their database, you would see just a bunch of gobbledygook and not really know what that's associated with. The broker doesn't know the individual that's doing these types of accesses. That's why we're looking to enhance some of the privacy, because they could, at this point theoretically peer into the assertion that's coming from the CSP and say, oh, this is Paul, maybe we want to be a bad actor and we're looking, in our next phase, to take that capability away.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

In the days of Edward Snowden, I would think that it would be a lot easier to figure out a way to get this data from the gobbledygook and decrypt it through the broker than it would be through a lot of individual CSPs. And I wonder if there are going to be people worried about not just privacy but security of their data, having a broker like that who would be such an easy target, or possibly the broker may be the, not the target, but the actual bad actor or somebody at the broker would be the bad actor.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

Which is exactly why we're looking beyond what's there today in terms of security and privacy, to make sure that to our best ability, that's not capable; but there's nothing stored in the broker that could be decrypted and breached. It's all meaningless numbers. My personal information that is ultimately coming from a CSP and going to an agency, that, of course the user has consented to provide, is never written inside the broker.

And the other...to the other question about why are we doing this, there is an economic motivation here beyond security and privacy. By creating a centralized service where all agencies can go, we can significantly reduce the cost of these credentials and also simplify the integration and we also have user choice. If a user wants to use a credential like Verizon, they can use that at every agency rather than every agency saying well, I'll do Verizon, this one will do something else and this one will do something else. This meets all four of our NSTIC guiding principles.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, this is Lisa G...oh Paul, this is Lisa Gallagher, I have a question for you just related to the relationship of this work to what we're doing in the health sector. We have some folks who are looking at what level of assurance we need in healthcare to meet certain use cases and looking at your briefing slides and the work that you're doing in reconsidering the 800-63 document, you talk about things like

thinking about instead of LOA componentizing trust and assembling vectors of trust and things like that. What can we do, right now as we're trying to make our way through this in terms of what we're dealing with now and then we've got a glimpse of what NIST is thinking about and the federal government thinking about now, are there questions we can answer or things we can work on together with NIST at this moment in time that we could think about? Do you have any things you want us to think about? That's kind of my question, because we're sort of in this, this is really interesting to think about, but we have some near-term projects that I think maybe we can have a more longer term view of it and think about it for the health sector.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

Yeah, it's our intent and we're meeting about this tomorrow, as a matter of fact, to actually start engaging the private sector soon on what exactly those questions are that we're looking for answers on. So that's one. For those that are familiar with OpenID Connect as another ubiquitous identity standard, there is some healthcare related work going on there from a security and privacy perspective. They're profiling out three standards OAuth, OpenID and UMA and we're participating pretty heavily there because we think can...we're hoping we can adopt most of that work, if you will, for a next set of profiles that we would accept.

I think it's not really a great answer to your question, but I think our Executive Order is kind of laid...drawn a line in the sand in terms of what we think anything regarding personal data should be, it should be multi-factor credential with appropriate identity proofing. And what's interesting about that is it doesn't necessarily mean you always have to have high identity proofing. If I have a site that's tracking my blood pressure, I might want to log into that with a two-factor credential, but maybe the site doesn't really care that it's me, it's just the same person showing up. So, and that would be low proofing with a high credential. But those are right now probably the three best things I could answer that and certainly can come back to you with more ideas as I get them.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, thank you. Does anyone else have questions for Paul? I'm sure there are more.

Steven Lane, MD, MPH, FAAFP – HER Ambulatory Physician Director – Sutter Health

Well, there was the earlier comment that I think there would be benefit from going back through this again in a little bit more of a real-time Q&A format and I...this is Steven Lane, I would certainly welcome that opportunity as well. There's a lot here.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

As do I, I would love that.

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

This is John Hummel...

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert

Yeah and this is Scott...

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

...I would think that's a really good idea, too.

Scott Rea, MS – Senior PKI Architect & Vice President of Government/Education Relations – DigiCert

Yeah, Scott wants to plus one then as well.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. Well Michelle, I guess that's something that we can talk about offline, what would be a mechanism to do that, have a more in depth discussion.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

I think that...Lisa.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. I'm trying to think if I have any more questions. I guess Paul, do you have any...you have this inventory you did of your coverage of identity services, how you cover that with your guidance documents. Is there anything new coming out that we should look for? What's the schedule for 800-63, if there is one? And what can we...

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NIST – National Institute of Standards and Technology

The...probably the most important thing coming out is our derived credential. Keep in mind it's based on the PIV and how do I take that PIV and basically generate certificates off of it that work in mobile platform. That certainly may not be relevant as it relates to the PIV form factor, but in terms of how we're getting strong identity into the phone may have some value.

We are working hard on a privacy engineering discipline, and I'm certainly not the right person to talk about that; the folks in my office are. There is material up on the NIST web site; you can look at to decide if that's something you'd want to take a look at.

And then in terms of 800-63 and anything really identity related around assurance and trust, the Executive Order and what the White House is doing. They've got a plan that they're building right now that in mid-January will be our marching orders, we expect. We think the EO and its read between the line saying LOA 2 is dead is basically going to direct us to do something. So we're excited for that and expect calendar year 2015 to be very busy and in preparation for that and maybe we might hold back because we don't know what the White House is going to say, but maybe before or certainly right after, we'll be engaging, most likely, in a series of RFIs and workshops.

Steven Lane, MD, MPH, FAAFP – HER Ambulatory Physician Director – Sutter Health

Can you say a little more about what you...how you see the Executive Order impacting the world?

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NIST – National Institute of Standards and Technology

Well the Executive Order is applicable only to the federal government, it does not have any applicability anywhere else, given the nature that it's not law, it's not regulation, it's scope of an EO is federal only. But we expect certainly it to start to...or if...to catalyze the market even more in terms of the fact that we're not looking to issue our own credentials to individuals working with personal data on government sites, we're looking to the private sector to offer those services.

It's also got a lot of language in there about chip and PIN, which is not necessarily our domain but again, it's government adoption of that which has private sector impacts. And we hope from leading by example we'll see this type of approach, not just the adoption of two-factor, but the adoption of interoperable two-factor will gain traction in private sector as well, not just government services.

Especially if you look at the fact that a citizen, and again this is market driven and this is why getting to users and relying parties is so important to us. If a user decides to do business with the government using a Verizon credential, why should they do business with Amazon with a different credential? They might demand to use that Verizon credential there as well. So, it's hard to predict what the market is going to do, but that's the area that we see the EO hopefully having positive impact on in the private sector.

Steven Lane, MD, MPH, FAAFP – EHR Ambulatory Physician Director – Sutter Health

Well, I'll certainly share, as a practicing physician where we have recently gone down the path to doing electronic prescribing of controlled substances and getting all of the thousands of providers in our organization up with multifactor authentication both with biometrics as well as with soft tokens on smartphones, there's no question that there is a shift occurring out in society. And so it's interesting to hear that this government change is coming simultaneous with what we're...the clinicians are having to go through.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

Yeah and when, just as a little aside, we...there was an announcement a couple of weeks ago that Google the browser was going to start to support some new technologies for two-factor and when you dug into that announcement, you find out that the tokens are \$20 to \$50 a pop and we're sitting here saying, well we really want there to be market driven, but user convenient and we're hoping consumers don't have to pay, it will be really interesting to see who's going to buy this thing. And we found out that it's...those keys are trending, number one, on Amazon electronics. So, there's much more of a demand than we thought, which is great.

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District

This is John Hummel, I can tell you that we're installing DrFirst in for our key system, which is used in our ER and we're charged by each token that key system sends to us for each one of our providers. So, I think there's a willingness to pay for the tokens and the security so that they get the ePrescribing for their scheduled drugs.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

Absolutely, we were just surprised as to the fact that the shift of the price went right to the consumer and they're snatching them up. It's one thing for my agency to pay \$110 for my card, but if they said, if you want this job, you've got to pay \$110, I probably still would have done it, but that would be an interesting paradigm and we're seeing that consumers are interested for higher security and more interoperability, right? That key...the announcement that Google is accepting it, it's that the Chrome Browser is, which means any web site now can accept this. So I buy the key for \$18 and I could presumably use it everywhere in a much more secure manner than 20 different passwords.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, any other questions for Paul? Okay, Paul, on behalf of the workgroup, I want to say thank you for giving us this presentation and for the question and answer period. I think clearly this group has a lot of interest in the work you're doing and interest in engaging with you going forward. So, happy to have started this relationship and we will be in touch to see how we can facilitate that further discussion.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

Great.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

So thank you very, very much, Paul.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

Thank you and you have my contact info as well if there's any...conversations.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Yes, we do. Thank you very much.

Paul Grassi, CISSP – Senior Standards & Technology Advisor, NSTIC – National Institute of Standards and Technology

All right, thanks guys.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Thank you.

Peter N. Kaufman, MD – Chief Medical Officer and Vice President, Physician IT Services – DrFirst

Thank you.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, so going back to our agenda, that was the last topic discussion. We just wanted to give you a summary of the next steps for the group. We have, in November, we have a meeting of the HIT Standards Committee, which is on November 18 and at that meeting, occasionally we have presentations to give or recommendations that we owe to the Standards Committee at a particular meeting, but we don't have any recommendations that we're going to be presenting at that next meeting. So, we'll be just attending and participating in the dialogue for the other topics.

And then we have a meeting of this workgroup on November 19 and at that meeting we are going to start discussing our own recommendations on the topic of identity management in healthcare that we will provide later to the Standards Committee. So that's our agenda for the remainder of November is Standards Committee on November 18 and a meeting of this workgroup on November 19. We will be in touch with you all to give you information about how we're going to brainstorm and create the list of recommendations and we'll fill you in on that as the process develops.

Michelle, I don't know if there was anything else you wanted me to cover before we go to public comment.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

No, I think we're good, Lisa. So if you're ready, we'll open up the lines.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay. Can we please open up the lines for public comment, operator?

Public Comment

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Lonnie or Caitlin, we can't hear you if you're speaking.

Lonnie Moore – Meetings Coordinator – Altarum Institute

Oh, if you are listening via your computer speakers, you may dial 1-877-705-2976 and press *1 to be placed in the comment queue. If you are on the phone and would like to make a public comment, please press *1 at this time. We have no public comments at this time.

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

Okay, thank you. So Michelle, I'll turn it back over to you.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Okay, well thank you everyone. As Lisa mentioned, we have a Standards Committee meeting on November 18 and then, I forget the date but there is another workgroup meeting coming up for this group as well and we'll be in touch...

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society

That's November 19.

Michelle Consolazio, MPA – Federal Advisory Committee Program Lead – Office of the National Coordinator for Health Information Technology

Thank you. Thank you everyone, have a great day.

Public Comment Received During the Meeting

1. What happens to the information the Broker holds? I'm concerned because of the ethical implications for the nefarious use of user.