



**HIT Standards Committee
Transport & Security Standards Workgroup
Final Transcript
December 3, 2014**

Presentation

Operator

Thank you. All lines are now bridged.

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

Thank you. Good afternoon everyone, this is Michelle Consolazio with the Office of the National Coordinator. This is a meeting of the Health IT 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, please state your name before speaking as this meeting is being transcribed and recorded. 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

Hi, Dixie.

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

Hello.

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

I'm here.

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

Hi, Lisa.

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

Hi.

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

Aaron Miri?

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children’s Medical Center, Dallas

I’m here.

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

Hi, Aaron.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children’s Medical Center, Dallas

Hello.

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

Brian Freedman? I think Brian’s there.

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

I’m here.

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

Hi, Brian. Jason Taule? Jeff Brandt?

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

I’m here. This is Jeff.

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

Hi, Jeff. John Hummel?

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Hello.

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? Peter Kaufman?

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

Here.

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

Hi, Peter. Scott Rea? Sharon Terry? 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. And I don't believe...is there anyone on from ONC? I believe there are folks on from MITRE instead, so I know we have Chris Miller and a few other folks from MITRE on the line as well. So with that, I will turn it over to you Dixie and Lisa.

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

Yes. Thank you all for dialing in and yeah, I know that Julie is doing some training so, thank you Chris for covering for her, we appreciate it. Thank you all for dialing in, I know it's a really busy time of year so we particularly appreciate you giving us some of your time. Today's meeting we have two main items on the agenda. First is to finalize our identity management recommendations, which we'll be presenting to the Health Information Technology Standards Committee December meeting, which is next Wednesday. So we had a really productive discussion the last time so I think that we'll be able to finalize those fairly expeditiously.

And then we'll move on to the next item on our work plan which is to explore security issues, concerns and considerations around RESTful APIs, application programming interfaces. REST, of course, is a style of programming that simply uses the web standards, Hypertext Transfer Protocol to transfer information using simple URLs. And that is the direction that both the Policy Committee and the Standards Committee seem to be going for EHR application programming interfaces and as recommended by the JASON Task Force. So our work around RESTful APIs is really looking at security considerations that need to be considered when one is building an application programming interface using RESTful style.

Then after...so we have a guest speaker around RESTful APIs and that is Mark Russell, who has done considerable work in this area for the MITRE Corporation and has recently, he and his partner, Justin Richer, have published recently some VA work, and he'll be talking about that today. So, thank you Mark for joining us today. And then we'll finish with public comment and move on to the next meeting. Lisa, would you like to have anything to add?

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, with that, let's move on to the next slide. Okay, let me move to the right...here we go. You'll recall that this work was really motivated by some recommendations that came out of the Policy Committee, specifically the Privacy & Security Tiger Team of the Policy Committee, passed them over to the

Standards Committee and we got them in that way. And these are responsive and they really...they asked for recommendations around authentication in identity management.

So we had five recommendations that we discussed at our last meeting and four of them we accepted as they were and the first one was, we recommended to look at a little bit more and especially look at it from the perspective of FIPS 140-2, which is the NIST standard, a special publication...or NIST FIPS document that addresses cryptography and NXA is the Annex to FIPS 140-2 that lists the encryption and integrity algorithms that are deemed acceptable. The rest of 140-2 has to do with certification of encryption modules.

So, we recommended, this is the recommended changed wording of the first recommendation. The first recommendation, you'll recall, had to do with multifactor authentication. So, our suggestion is...and we also worked with Peter and Aaron on refining the wording to this, so our thanks to them for their help. Okay, our recommendation is to add a certification criterion that requires the EHR technology to demonstrate the capability to do two things, first to restrict access to the system or to one or more individual functions within the system, such as prescribing controlled substances, to only those individuals who have presented at least two of the three forms of authentication, knowledge of a secret, possession of a physical object and a biometric.

And then the second thing is to continuously protect the integrity and confidentiality of the information used to authenticate users using the standards that are already specified in the 2014 Edition of the EHR Standards and Certification Criteria. And that...the existing, so the existing certification criteria already says, use FIPS 140...use algorithms that are approved in Annex A of FIPS 140-2 for both encryption and integrity protection. So we're just simply referencing using those to protect authentication information.

And the first one, a) in this one is, we cited the...two of the three forms because multifactor authentication is not just presenting two things, like two passwords, but the idea is to present two types of things like a password plus a hard token, a secure ID token, for example or a smart card or a fingerprint. And the two factors really need to be two type...different types of authentication. So, let's open up discussion of this recommended rewording.

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

So, this is Steven Lane and I just have a couple of comments on a).

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

Um hmm.

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

We say, "who have presented at least two of the three forms of authentication;" there are other forms of authentication I could imagine. Would...do we need the word "the," two of three forms of authentication?

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

Well, actually those are the only three, authentication is either...is present...is defined as, presentation of either something you know, something you have or something you are. I mean, historically through the decades that's widely viewed as the three...those are it and some...but, within each of those three categories, there is a broad range of things that you might have. I mean, the typical something you know

is usually a password or...but it can also be a PIN number, for example, but is something you know. And something you have is a physical object, a physical thing such as a smart card or a hard token or something that you actually have. And the third is something you are. Now, the field of biometrics is huge, it could be a retina scan, it could be a fingerprint, it could be facial recognition, it could be voice recognition. But basically those are the only three forms of authentication that are ever recognized or talked about. So that's...

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

Well that's helpful clarification. My only other question was really one of grammar and that is, in the last line there, should it say "and" or should it say "or" a biometric, two of three forms?

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

Oh yeah, let me see, the way we worded it was two of the three forms of authentication, it should be "and," those are knowledge of a secret, possession of a secret and a biometric; those are the three.

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

We're just listing the three forms, very good. Okay.

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

Yeah.

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

Thanks.

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

This is Peter. To me it looks like "a" and "b" seem like Venus and Mars; "a" is very pedestrian and just kind of like very knowledgeable, anybody could understand it whereas "b" is extremely specific numbers and standards and everything. And I wonder if we couldn't make "a" a little bit more specific or, I don't know if I want to say make more pedantic, but make it seem a little closer in wording and terminology to "b" or make "b" a little more wording and terminology similar to "a." And also, I also thought it seemed funny about two of the three forms, and maybe it should read, two of the following. I know there were only three, but two of the following three forms or two of these three forms.

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

That's what we have, two of the three forms.

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

You have two of "the;" instead of "the" have "these."

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

Oh these, okay. Yeah, yeah. The following I think is good. Let me make that note.

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

This is John Hummel. For the knowledge of a secret, do we...should we put in there part of the NIST standard for strong authentication passwords?

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

Let me answer Peter's, because it really relates to your comment as well.

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

Okay.

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

Peter, where I thought you were going, which I think is a reasonable comment, actually, is “a” and “b” really are not that tightly related. “A” has to do with the...you could be certified, you could ask your product to be certified such that it supports multifactor authentication. That’s something new. “B” actually when I was looking this up, looking up the reference, I realized, and the existing 2014 certification standard doesn’t have a requirement for protecting authentication information. So, in truth, I think “b” should be applied to all authentication, in truth I think these probably should be two separate recommendations because “b” ...

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

Okay, that would solve it.

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

...really, and the reason the reference is there in “b” is because the existing 2014 edition has authentication in it and it has FIPS 140-2, Annex A algorithms, but it doesn’t tie the two together. And what we were trying to do is say, this builds on something that’s already there, this isn’t something out of the blue. But I think it would be reasonable to make these two separate recommendations so that they wouldn’t be tightly tied because you need to protect authentication information. In other words, “b,” regardless of whether you have multifactor or not. So I think that that might be a reasonable thing to do, what do you think about that, Peter?

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

I think that would be fine, that would absolutely solve my problem. And in terms of the next question, I think that we don’t want to do too much about strong password authentication at this point because it’s such a moving target and there’s such an issue with what should be in a password. I’m very much in favor of not requiring any capitals or letters or numbers or anything, but I’d like to see it 15 characters or 20 characters instead of these ones you have to write down because there’s all this weird stuff in them.

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

Well I was just thinking, this is John again, that in the NIST standards, it calls for strong passwords that are 8 characters at a minimum, upper/lower case with a number and a special character. And so if I’m an EMR programmer and my current password field is 6 characters, then I’ve left this in the criteria for them to be certified that they’re going to have to change that field if it’s not adequate.

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

Well, you know again, I think that that’s a reasonable recommendation but I would say it shouldn’t just apply to...I think I would be...I would say that that’s another one that we should recommend that would be applied to all authentication that uses knowledge of a secret, not just multifactor. Do you know what I mean?

M

And I think that we’re really only talking about the demonstrating the capability to do this, we’re not saying that everyone has to satisfy that standard, they just have to be able to.

Amy Zimmerman, MPH – State HIT Coordinator – Rhode Island Department of Health & Human Services

Right.

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

That's right.

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

...EHR system has to have that capability.

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

Well, we're not even saying that, we're saying if the vendor, because remember that the way that products are certified now is an EHR vendor...there are no required certification standar...criteria. The vendor comes in and says I want my product certified against the following criteria.

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

Right, their modules.

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

Right, right, modules, exactly right, yeah.

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

Right.

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

So they pick which ones they're going to be certified against. So these would be criteria that they could choose to have their product certified against and then, if I were a provider and I purchased that product, I could further choose whether to use it or not.

M

Right, but I think that what we're saying, Dixie, is that we think there should be a "c" here and...

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

Well I think...

M

...that the third item would be that requiring the EHR technology to demonstrate the capability to require a strong password based on the established guideline.

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

Yeah, what's the NIST is it 800-63 is what you're talking about, or...

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

Yeah.

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

But we're also only talking about one component of multifactor, which is the knowledge of a secret...

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

Yeah.

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

...how do we distinguish that?

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

Well I would say we...

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

I don't think putting it as "c" is helpful because...

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

Yeah.

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

...it doesn't go at the same level in the outline.

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

Well that's what I said; I think that...I've already made this change...

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

Oh, okay.

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

I made "b" a bullet, not a "b," so there should be...

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

Right.

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

...bullet "a," "a" is bullet, "b" is a separate bullet; you know, they're not...they're separate criteria and I think what I'm hearing is a third major bullet which is, in cases where they use knowledge, and we need to look up the existing language in the 2014, because it already requires that, but somehow say that if they use a password, which is the knowledge one, it should follow the guidelines of NIST 800-63, and it would be helpful...Kris, can you write down that your team would look up in 800-63 the exact citation of where it has the password guidance?

Kris Miller, LLM, JD, MPA, CIPP/G, CIPP/E – Principal Privacy Strategist, Enterprise Strategy & Transformation Division – MITRE Corporation

We'll do that, yup, taking a note.

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

So couldn't it be "b..."

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

But again, I wanted to say that I'm very much against requiring special characters or caps and smalls in passwords. A longer password is more secure than a short password that's difficult to remember and easy to crack; a longer password is easier to remember and harder to crack.

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

So I would be strongly opposed to us making up our own criteria for strong passwords. We'll have Kris look up what...well, who was it that...who was the person...whenever you make a comment, would you please remember to announce your name. Who was it that suggested that, because I don't...and certainly the public doesn't know who's talking, but who suggested that we incorporate 800-63 password guidance?

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

That was me, John Hummel.

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

John, okay, John. Do you happen to know, does...I suspect 800-63 does mention capitals and lower case, but do you know what it includes?

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

...right now, I'll get back to you in a couple of minutes.

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

Okay. Yeah, that would be useful because, yeah, because I don't want us rewriting the password rules. If we have an existing standard we can cite, that's a good thing, but I don't think we should be making up, you know picking and choosing within the standard.

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

Well that wa...my point was, if the existing one is based on stuff that is becoming obsolete for passwords that we should not cite anything at all then.

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

I would agree.

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

Not to say...by the time that this is in use it will be something that's considered passé.

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

Well, passwords themselves are considered passé, but they still exist. But yeah, let's have John look that up and come back to us perhaps later in this meeting or afterwards, whichever works out. Okay.

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

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates
I've made my notes...

Lisa Gallagher, BSEE, CISM, CPHIMS - Vice President, Technology Solutions – Healthcare Information & Management Systems Society
That's good.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates
...Kris, I'm sure you have, too. So, where we are is, this is not going to be one recommendation with "a" and "b" as sub...we are going to have one recommendation that says add a certification criteria that requires the EHR technology to demonstrate the capability to restrict access, blah, blah, blah. We're going to have a second one that says, add a certification criteria that requires blah, blah, blah, continuously protect the integrity. Then we're going to have a third new one, perhaps, that addresses the strength of passwords, to be discussed later in this meeting or online following the meeting.

Aaron Miri, MBA, PMP, CHCIO – Chief Technology Officer – Children's Medical Center, Dallas
So Dixie, this is Aaron Miri; I think it's a great idea to have a separate one. I also do like following a NIST standard of complexity that's out there and proven, even if it does become sort of past tense by the time this is implemented, at least it's a step in the right direction, which is better than right now as it stands within the requirements for certification. So, I think it's a great idea.

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems
Hey guys, this is Jason Taule; I think we might be able to reconcile it by using the word entropy instead of complexity. The 800-63 standard does talk about how to calculate the amount of entropy and it does, for different levels, talk about the minimum number of bits of entropy. So, there are lots of ways of achieving that without coming into some of the problems that the other gentleman was talking about earlier. So we can still refer to the 800-63, but talk about satisfying the entropy requirements not complexity. Because I'm in full agreement, our standard here, for example, is it's got to be a minimum of 14 characters, because the bad guys have hash tables with every combination of the ASCII character set up through 12-13 already calculated.

Dixie Baker, MS, PhD – Senior Partner, Martin, Blanck & Associates
Okay, so do you...who's speaking now?

Jason B. Taule, MSB, CMC, CPCM, HCISPP, CCISO, CISM, CGEIT, CRISC, CHSIII, CDPS, NSA-IAM – Chief Security & Privacy Officer – FEi Systems
This was Jason Taule, again. So I think the reconciliation is to use the word entropy and refer to the 800-63 entropy requirements, not complexity requirements.

John Hummel – Director, IT and Systems and Innovation – Tahoe Forest Hospital District
This is John Hummel; I think that's a good suggestion.

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

I agree this is Lisa; I know that in that standard they do use the term entropy and...

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

And it's separate...it can be separated from a complexity.

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

Yes, it actually is the measure that they use for...

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

Okay.

Aaron Miri, MBA, PMP – Chief Technology Officer, Information Services – Children's Medical Center

Yeah, that definition out of it's a measure of the amount of uncertainty that an attacker faces to determine a value of secret. Entropy is usually stated in bits. This is Aaron.

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

Yup.

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

Okay. So we can...

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

I found it right as you started reading it...

Aaron Miri, MBA, PMP – Chief Technology Officer, Information Services – Children's Medical Center

I'm reading your mind.

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

No, I'm reading yours.

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

Yeah, so, we'll get...Kris, if you can, let's see, John...work with John and make sure that we get the right reference...well, do you have it open there, John?

Kris Miller, LLM, JD, MPA, CIPP/G, CIPP/E – Principal Privacy Strategist, Enterprise Strategy & Transformation Division – MITRE Corporation

This is Kris; I'm looking at paragraph 8.2.2.4. It discusses password strength, mentions 10-bit entropy, minimum entropy and there's an appendix as well. So, I'll work with John offline and we can hash that out.

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

That would be great. That would be great, thank you, that's perfect. Thank you very much, both of you. Okay, making myself a note here. All right, then I think we're ready to go to the next slide, and thank you guys for your...those are excellent suggestions. Now these are the other three recommendations we

had, I think...the first is to support the NIST effort to revamp 800-63, and these haven't been changed from the last time you saw them and approved them.

The second is to consider the Data Segmentation for Privacy for authorizing access to behavioral data and we will address this later in our work plan. And the last is to track the development and piloting of the...we probably should have Kantara...that's a Kantara work, so probably should say, Kantara User Managed Access profile of OAuth 2.0.

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

That's right.

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

Okay. You still okay with those? All right.

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

It's Lisa, I am.

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

Dixie, this is John Hummel again. I think the wording that we're looking for for the entropy is on page 104 of the dash 63-2.

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

Dash 63, right?

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

Yeah, dash 63, release 2.

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

Yeah, yeah, yeah, release 2.

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

Under randomly selected passwords a.1. I was just looking at it in terms of the entropy, so yeah, the randomly selected passwords, yes.

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

Yeah.

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

Okay. Okay.

Kris Miller, LLM, JD, MPA, CIPP/G, CIPP/E – Principal Privacy Strategist, Enterprise Strategy & Transformation Division – MITRE Corporation

This is Kris, thank you for that.

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

Thank you all. Great. Good coordination. All right with that, we'll write these up and we'll put them in a presentation and they'll be presented at the Standards Committee next week. All right, next slide, please. I think we're ready to move on. Thank you.

As we mentioned, we're starting a new task here and that is to explore security issues around RESTful Application Programming Interfaces and we have a guest speaker, Mark Russell, from the MITRE Corporation. And Mark, thank you very, very much for joining us today and with that, I'll turn it over to you.

Mark Russell – Cybersecurity Subject Matter Expert - MITRE Corporation

Okay, thanks a lot, thanks for having us. Great, there's my slide. If you go ahead to the next slide. So today we're going to talk about OAuth and OpenID Connect, risks and vulnerabilities. I know the subject was generally REST API risks and vulnerabilities, I'll talk a little bit about why this presentation is scoped down the way it is. We're going to talk a bit about some work that MITRE did for the VA on the subject of RESTFUL interface security and it's a wide topic so I'm going to just give you a lot of pointers to further information and just try to give you a flavor for it here. Could you go to the next slide, please?

So this is some background on the task that we did for the VA. Mary Pulvermacher and Justin Richer from MITRE are also here on the line with me today, who also worked on this task. But essentially the VA Office of Information Technology Architecture, Strategy and Design Division is tasked with sort of looking at the future of technology and where the VA wants to go creating design patterns to guide people who are building systems and integrating software into the environment.

So they had tasked us to look at the security of RESTful interfaces. They're looking to go to REST for a number of reasons; one is simply just the need to be increasingly connected to a large number of both organizations and individuals. There are a lot of individual patients who want to use their own mobile Apps and web applications to interact with their medical data. There are small medical providers who increasingly want to be connected and be able to exchange data with the VA. And then, of course, there are sort of the big organizations like the DoD, which VA has always interacted with, but would like some additional options for streamlining how they do that.

So all these things are pushing REST, the question is, with VA, their use case is involving largely medical data of America's veterans. They have a large responsibility to protect the data and also they have a long history of using SOAP interfaces and we're interested in finding out how they could get similar security assurances out of REST. SOAP is a big set of protocols and standards that define pretty much everything about how messages are interchanged and secured. REST removes...one of the appeals of REST is that it's a much more lightweight system, but the question is, how can we still assure the security of the data and the APIs when we move to this new kind of style of application development.

So we were asked to develop a profile for sharing information over REST using open standards, because that will make it easier for others to integrate with them, in a way that's secure and compliant with VAs requirements; of course as a government agency, of encyclopedia sized security requirements to comply with. Must be able to support lightweight web clients and mobile devices; people increasingly want to use their own Apps to do things and so it's...you can no longer assume that you're going to control the client side of the equation.

And so we actually delivered profiles earlier this year and currently are working on a pilot deployment to demonstrate that the profiles can be implemented and that they work and that they deliver the security that we're looking for. So the pilot deployments currently underway, we're going to be releasing all that source code as Open Source, but we currently have a website you can go to to get the profiles and some other documents and the VA has graciously approved all this for public release, so, we're hoping to get the word out on this work and hoping that other people can use it as a foundation to do things like what it sounds like you're looking to do. Next slide, please.

So this is just some contact information for the team; if you go ahead to the next slide. So this slide just introduces a slew of standards that can be used for securing REST. So this graphic is laid out with standards, standards on the bottom are sort of foundational and the standards above them depend on them. So at the bottom we won't talk too much about TLS, which is what you use whenever you use HTTPS, but basically that's sort of going to just work as long as someone is keeping these patched.

OAuth we'll spend a good bit of time talking about, it's an authorization protocol for RESTful APIs. On the bottom right you have JOSE, which is a set of standards related to JavaScript Object Notation or JSON, which is a lightweight data exchange format, somewhat analogous to XML, but aimed at being much more lightweight. So JOSE is aimed at providing encryption and signature for JSON objects. And built on top of JOSE is JWT or some folks call it "jot" for short, I usually say JWT, but this provides signed and encrypted tokens. And then OpenID Connect, we'll also talk a bit about.

User Managed Access, I already heard Dixie mention that earlier. We looked at User Managed Access and it definitely has a lot of potential for a lot of medical use cases and things we're interested in. We felt at the time we started this work that it was still maturing to the point where it didn't make sense to profile it at the time we were starting off this project, but definitely something we're interested in looking at in the future. So, I apologize for that alphabet soup, but that's just some context to give you an idea of the set of standards we looked at. For the most part we focused on OAuth and OpenID Connect because basically they have a lot of impact on how the API and interface is designed and they're relatively complex standards, so, we wanted to look at profiling them and basically making them meet the VA's requirements for securing REST. If you go on to the next slide; next slide, please. Thanks

Okay, so what you see here, this is the OAuth authorization code flow. So I understand Justin has already talked to you a bit about OAuth in general; I won't cover the basics. But essentially the goal of OAuth is you have a resource owner who wants to use a client of their choice to interact with a resource that they have access to. And so in looking at risks and vulnerabilities, it's really helpful to separate out these four different parties. In many cases they're going to have the same motivations and some of the same risks will apply to all of them, but it helps to remember that they may all be affiliated with the same organization or truthfully, they may all be completely unaffiliated.

Typically the authorization server and protected resource would be both hosted by the same organization, but the protocol allows for them to not be. So, when we looked at security risks, it was important to look at what each party sort of has to lose in this OAuth flow and what's important to them; if you go to the next slide.

So, thinking first about the resource owner. If you've been working IT security for a long time, this may be a little bit confusing. It's helpful to think of the resource owner basically as someone who has access to something, it's not necessarily a data owner or system owner; it's someone who has some access to a resource and through the use of OAuth, they're able to delegate that access to a software client; so

when I think owner, I usually think the person who's in charge of the system, but really, it could just be an ordinary user of the system.

The resource owner has credentials, you just spent a good bit of time talking about this, but could be a password and it could be a private key that's registered with the authorization server. They have access to a protected resource and the resource owner has decided that they want to use a particular software client to interact with the resource. One example would be maybe I have a g-mail account and I've downloaded an email App on my Android for when I want to use this email App to go and fetch my email for me.

So what risks are facing the resource owner? Obviously, if their credentials are stolen, they can be impersonated. Those credentials might be usable on a number of different sites and resources. And through the OAuth delegation process, the resource owner might be tricked or might simply not know what they're doing, they might grant more access than they wanted to; maybe they grant access to parts of the medical record that they weren't intending to do some kind of blood pressure tracking App. And lastly, the resource owner...the protected resource, especially in medical use cases, is typically going to be sensitive data about the user. So, fundamentally what they want to do is enable this use of the client that they've decided is beneficial to them, but without excessive risk to their data going elsewhere. So that's really the main motivation of the resource owner; if you go to the next slide.

So the client is going to be a piece of software. There are many different types of clients, native clients such as mobile Apps; they could be desktop Apps for that matter. There are embedded clients, which would be an App that runs directly in the browser, either in JavaScript or a plugin. And then there are web clients. So really a client could be...it could be something that one person uses or it could be something that thousands of people use.

And so the client registers with the authorization server, to get a client ID. Most clients have their own credentials so the client is actually authenticating itself when it tries to access resources and interact with the authorization server. And the client is responsible for orchestrating this authorization flow between the resource owner and the authorization server. It's the component that will redirect the resource owner over to the server to authorize the request.

And so the client often really has nothing to lose from this. Frequently the client will be written by some third party and maybe even a small developer who has a few Apps in the Android store or the Apple store. So, there are sort of reputational controls around a lot of these Apps. If word gets out that there's a bad App, the will start to get dinged on ratings, will eventually maybe get kicked out of the App store or if there's website people will stop using it. But of course that model depends on a few people experiencing the bad behavior in order for it to be reported. But really, the only real currency that a client has is the willingness of people to use it. So, that is sort of the control that exists. You could contemplate a model where the organization would vet individual clients, but that's a hard problem to begin with and it's very difficult to keep up with the rate of new clients coming out and updates to them.

So if you think in terms of risks to the client, if the client's credentials are stolen, other pieces of software might go out and do bad things, causing the client to get booted out of the App store or to have its client credentials revoked. The data within the client could be stolen or manipulated, authorization codes or tokens can be manipulated. There are some interesting variations on attacks that do that sort of thing; either they cause an access token to be sent to the wrong place or, in some cases,

they may cause a resource owner to interact with a different resource than they thought they were interacting with.

If you think about the resource as...it could be something that's already sensitive or it could be something like an application for benefits that the owner is going to then enter sensitive data into. If I can get you to use my protected resource, then I can go then and get all the data you've uploaded into it. And then abuse of unsafe redirects; there was some news about this a couple of months ago. But one of the larger social networks had an integration with ESPN and there was an issue where tokens were being redirected to third party sites that can be a problem. But in that case, what was ultimately determined was that there were a number of issues with how it had been implemented. The minimum requirements of the spec hadn't actually been followed so, it was sort of predictable what happened but it is something the client needs to be careful of and implement properly; if you go to the next slide.

The authorization server is kind of the hub that manages this whole process of OAuth authorization. It controls the policies...the authorization server is sort of the gatekeeper that will determine which clients can get registered. And it determines the scopes of access that can be requested by clients. Scopes in OAuth are basically ways of giving out pieces of access, so in a medical use case, scopes might be a certain set of FHIR resources that a client could access. It also handles the process of authenticating the resource owner. One of the most critical things it does is it will show the resource owner the details of an authorization request. So it may say this application which is published by such and such software company, wants to access these pieces of information of yours, do you approve or reject this?

So that's a critical function, it's very important to the user interface elements right and to allow people to make informed decisions when they're clicking approve or deny on that. Once again it's typically going to be hosted by the same organization as the protected resource, there's a pretty tight integration between the authorization server and the protected resource, in order to enable the resource server to figure out whether the token is good and what it's good for, what resources it should give access to.

So, risks to the authorization server include interception of credentials, tokens or codes. So this is basic kind of make sure all connections are encrypted stuff will go a long way towards remediating a lot of that. There could be brute force attacks on credentials, tokens or codes; we'll talk a bit about how that can be remediated. You have the same sort of issues with redirect URIs; there's a lot of redirection that's used in the OAuth protocol, there are a couple of different redirects and if there are issues, if they are manipulated, they can cause authorization codes or tokens to go to the wrong place. Cross-site request forgery I won't delve too much into. And then, of course, the basic denial or degradation of service; anytime you put up a web service, that's a risk or any other kind of service, for that matter; if you go to the next slide, please?

The protected resource is...this is sort of the end goal is to connect the client up with the protected resource. The considerations here are really going to depend entirely upon what the API does, but one of the main functions or security jobs of the protected resource server is to get the token and figure out whether it implies that the request should be granted or not. If you remember from the basics of OAuth, the token represents the fact that the resource owner has authorized the client to do something, it's up to the protected resource to figure out what that something is and there is some back-channel communications that can deal with the authorization server to help figure that out.

One thing that the OAuth spec itself does not specify is what a token should look like. So, you can...there's some leeway there to better define what a token should be to make some of these things

easier. But, essentially the protected resource has to defend against clients intercepting tokens intended for other people or other clients; clients using tokens issued for different resources which may not be an issue in a lot of cases, but if you use the same scopes across multiple resources, there needs to be a way to figure out where that token was meant to go. Replay of authorized requests, request for resources out of the granted scope and brute force guessing of tokens.

Let me pause there. I know that was a lot of information and I will just say also that there's a lot more information about this in some of the documents on our site, but if anybody has any questions right now, please go ahead. Okay, let's...

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

Well...

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Sorry, go ahead.

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

This is Lisa Gallagher, I was going to ask about countermeasures, but looking ahead, you have some discussion of that on the next slide.

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Yup.

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

And I think when you get to that, my question would be, how does that map to each of the potential risks on each of your previous slides, you know, is it complete coverage or are there other sort of countermeasures for the risk that you list for each of the actors? So I'll let you wait until the next slide for that question.

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Okay sure, let's go ahead.

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

See if there are any other questions first, though.

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

I do have a question, this is Dixie. On the second one, the clients using tokens issued for different resources. If a client requests multiple resources, then there's one token issued for each resource, right?

Justin Richer, MS – Principle Technologist – MITRE Corporation

This is Justin; let me jump in on that. In an ideal deployment, yes; but this is known in the field as the confused client problem. And so this is what would happen if a client basically it gets one token and it thinks it's good for more resources than it's actually good for. And so that's how you can have poorly written software sending an OAuth token to a place where it doesn't actually belong.

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

Ah.

Justin Richer, MS – Principle Technologist – MITRE Corporation

And there are legitimate deployments where you could have multiple resources that would be protected by the same token that has multiple sets of rights bundled into it. So, say for example take something from the more social web space, you get somebody's account information using something like OpenID Connect, you might also want to be able to get at say their calendar information or their social graph or other things, you don't necessarily want to have to get a different token for each of those, you'd rather, as a client software developer, be able to get one token that has each of those different rights tied into it.

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

Hmm. So is there a concept for a virtual resource that combines resources?

Justin Richer, MS – Principle Technologist – MITRE Corporation

Not really because in the RESTful world, you don't really need that so much as a concept because it's just another endpoint. What a RESTful endpoint does behind the scenes in order to fulfill a given request is of no concern to the client.

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

Yeah...

Justin Richer, MS – Principle Technologist – MITRE Corporation

But along those lines, I will make a quick note that there is some work in the IETF, that's the Internet Engineering Task Force, the standards body that defines OAuth and JOSE and a lot of these other things, for how you can actually exchange one token for another of lesser scope.

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

Hmm.

Justin Richer, MS – Principle Technologist – MITRE Corporation

So that you could request a token that has all of those rights, but a well-behaved client would be able to, using this token chaining re-delegation mechanism, be able to request sort of mini-tokens to say, oh, I'm calling this service and I'm only calling it once so give me this one-scope for the next like 60 seconds and give me this sort of very limited access token that allows you to do limited rights and other things like that a little bit more cleanly.

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

Okay. Thank you.

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Okay, if there are no other questions, do you want to move on to the next slide? Thanks, Justin. Right, so this is a greatly summarized version of a longer table that's in one of the papers up on our site, but basically...so, in the previous slide we talked about risks, which are really, what are the bad things that can happen to each of the players? This slide really talks about what are the potential weaknesses in an implementation of OAuth that would allow those things to happen.

So, if an attacker is able to extract things out of a secret set of traffic like tokens or credentials, obviously they could play those back against the resource or impersonate the resource owner. TLS encryption goes a long way to mitigating that. There are some other countermeasures you can use as well. But basically, impersonating servers is also a big problem through either phishing or to...DNS caches, that sort of thing. So TLS server authentication is a good mitigation for that.

One of the things we did in our profile, on the next one, manufacturing and modifying tokens. So if you look at a lot of the OAuth libraries that are out there, they issue tokens as basically...random values, which are essentially passwords when you comes down it which means potentially someone could sit there all day long and try to guess a valid token. There are other controls we could have around that like rate-limiting the rate which you can guess token values or revoking clients that try to do this too many times. But one thing we did is instead of sort of static secrets as tokens, in our profile we said tokens should be assigned JWT. So, basically the signature makes it very difficult to brute force guess it, it makes it easy to validate as a valid token and so that goes a long way towards mitigating that vulnerability.

On the issue of redirection, I talked a bit about that...

M

What is JWTs again, I forgot?

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

I'm sorry, that's JSON Web Token. You can think of it basically as...it's a find and optionally encrypted JSON object, so it would have the signature of the authorization server and it would assert certain things about the token.

Justin Richer, MS – Principle Technologist – MITRE Corporation

This is Justin. So if you've heard of SAML assertions or similar security constructs, security token constructs like that a JWT is analogous to those. It carries claims in it such as who issued the token, when it expires, who it's talking about, what rights does it have all inside of a JSON object that is then protected by the mechanisms of the JOSE suite of specifications, which allow you to do the signing, the encryption and all of those other things.

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

"Jot" is how you pronounce JWT

Justin Richer, MS – Principle Technologist – MITRE Corporation

Yes. I've heard "jwt" and a few others, but "jot" is...that's what they say at the JOSE meetings is "jot."

M

Okay.

Justin Richer, MS – Principle Technologist – MITRE Corporation

So that's what I go by.

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Okay. So on the question of redirection, the main mitigation for that is when clients register, they should have to register what redirects they're going to use. Basically this tells the authorization server, after the user has clicked okay and said yes, I authorize this access, it needs to send either a token or a code back to the client. So the client should know in advance which redirect URLs they're going to use, by locking that down at the time of client registration, it eliminates a number of attacks where somebody might want to change the redirect URI and have it point to a server they control.

So the next one, guessing or interception of client credentials; once again we use signed JWTs for client authentication. There's a mechanism, it's actually defined in the OpenID Connect spec, but can be used with OAuth as well, that basically involves the client registers a private key using JWKS, JSON Web Key Set, and basically can then issue signed JWTs to authenticate to the authorization server and potentially the resource server also. But what that does basically is that instead of sending a static password over the network, the client is sending a signed message that can be validated on the other end. It can include claims about the client, but essentially it's a stronger authentication mechanism if the JWT is intercepted, it has a limited lifetime, you're not exposing long term secrets over the network.

And then client session hijacking or fixation, this is an issue where the user has...if you assume the user is using a web client, they have one session with that client and then they're going to establish a different session with the authorization server. So, if an attacker can take over the user session or if they can force the user into a session that they actually control with the client, they may get access to tokens or codes or they may simply be able to take over and interact with the resource. So there's a specific mitigation of this defined in the spec, there's a parameter called State which basically the client specifies up front and then can validate when it comes back from the authorization server that there's been one continuous session throughout the OAuth flow and that there hasn't been a break in that session or things haven't been manipulated, essentially.

So getting to the question earlier, do the countermeasures cover 100% of the issues we've talked about? I think that the short answer is yes, provided that certain precautions are followed. We get to a lot of that in our profile, but essentially, if you look at the OAuth spec itself, it's a very sort of loose specification, and that's intentional, because it's meant to cover a wide range of different use cases.

But, if you implement just the bare minimum security that's in the OAuth spec, there are a number of issues. Some of these attacks would be possible against a spec that...excuse me, an implementation that did just the bare minimum security that's in the spec. I think we've...if you look at the, there's a paper that's linked on my last slide that has a longer list that this was boiled down to of specific attacks and countermeasures and that may help you look at...for each specific example, what are the countermeasures and what are potential gaps in them? But, following the profiles we've defined, we believe things are fairly solid.

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

Could I...this is Dixie, I want to note that the spec itself is pretty good at identifying what you need to not do or what you...the spec itself points out a lot of these vulnerabilities.

M

Yes.

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

My question is that the first two are true, the TLS and countermeasures, they're true, but only if TLS is implemented such that its endpoints are secured. Is that covered in your profile of the implementation of TLS to make sure that when the endpoint, when it actually gets decrypted, it's in a safe space, behind the firewall or in a protected area? Is that covered in the profile itself or is the implementation of TLS considered out of scope?

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Yeah, we generally consider that out of scope. I mean, you're right; there are a number of issues you have to make sure the right ciphers are being used, you have to make sure there isn't some intermediary decrypting the traffic and then passing it in the clear, all that kind of stuff. But, our take on that is that there's no specific TLS implementation considerations that are specific to REST APIs, it's sort of the same concerns you would have with any web application.

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

Um hmm, yeah.

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

The same TLS guidance there will help you here.

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

Yup.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Hey Dixie, this is Jeff Brandt, that's a good point. Usually most of the attacks happen at the edge so if we don't have a section on that, we definitely should bring...at least put that up as a marker to look into that, because that's, SSL is pretty safe and you're running OAuth 2, you're running SSL, it's at the edge where the problems become an issue.

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

Yeah, that's where the credit card numbers are captured.

M

Right.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Oh yeah, well hopefully they...

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

Yeah.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

(Indiscernible)

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

I'd say if there's one area of lingering concern, it's in terms of the client. It's really the resource owner's decision to trust a given client to interact with their data and there are bad clients out there, obviously malware is a difficult problem in any scope. So, sort of the best you can do is active monitoring and rapidly shutting down clients if there's a problem.

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

Um hmm.

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

But that's sort of inherent to the world we live in today, if you want to support users ability to choose which Apps they want to use, that's a problem you're going to have deal with. Okay, if there's nothing else, do you want to move on to the next one?

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

Yeah I think go ahead Mark.

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Okay, thanks. So just a few words about the profile; I've already talked about some of this, so I won't belabor the point, but basically our goal was to sort of raise the minimum bar on what OAuth requires in the specs. So a lot of the "shoulds" turned into "musts" in our profiles. And we specified, like I said, the token format assigned JWTs, they're easy to validate, can't be brute forced, stronger client authentication, the redirect URI registration; those three things together really address a large swath of the problems that have been seen with OAuth.

And another area VA wanted us to look at was if...for use cases where security is really paramount, what are some advanced techniques we can use that may impact the usability or ease of implementation. But, for those times when you really want to go the advanced measures, what can you do? So, TLS plan authentication is an option we're mainly looking at the JWT mechanisms for authentication, but there's no reason why an OAuth client couldn't use a TLS credential to authenticate. And then there are a new set of standards on proof of possession tokens which essentially provides stronger authentication. It's a similar notion to holder of key in the SAML world, but basically it's demonstrating proof of a cryptographic key. So those are some...and proof of possession is in early draft stage, but it's something to look forward to for some of these higher assurance use cases.

Justin Richer, MS – Principle Technologist – MITRE Corporation

And this is Justin, I just want to note that the work that we've done, sort of the rest of the recommendations that we've done, actually would slot in very nicely alongside either mutual TLS or proof or possession tokens or both, in cases that warranted. We've tried to build things so that it's very composable.

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Okay, next slide, please. Once again, I know I'm a little behind time, maybe we'll skip over some of these. There are some examples in the slides there you can see of what specifically choose to profile. This is about URI registration. Next slide. And this is about the specific language on JWTs must support RSA 256 signature method. So, as I said, this sort of just raises the bar on what OAuth requires to make these a bit more suitable for these medical use cases. If you go to the next slide, please.

So, we'll talk very briefly about OpenID Connect. So OAuth is all about authorization, the user allowing a client to access things that they have access to. OpenID Connect is more analogous to SAML; it's an authentication protocol that is actually built on OAuth. So everything we just said about OAuth still basically applies, the players have slightly different roles. Instead of a resource owner we have an end user who's looking to authenticate. The client acts as a relying party, if you're familiar with SAML terms; the OpenID provider is like the identity provider.

And so the goal of doing this essentially is, as with SAML, when users here are using a number of different web sites, they don't necessarily want to register an account for each site, it's more convenient and more secure for them to have one or two identity providers that they can use to log into a number of sites. You've probably seen login with Facebook everywhere, log in with Google Plus; they're using OpenID Connect for that functionality. So, the idea is that rather than establishing an account at your website, I'd like to use this existing account I have so your application will essentially trust information from my identity provider that says I'm who I say I am, that I've authenticated to them. And optionally it could say other things about me like what my email address is all the way down to it could say something like I am a licensed medical practitioner, depending on who the ID provider is.

OpenID Connect introduces, on the bottom right, the UserInfo Endpoint, which is an OAuth protected resource which basically just has identity information about the user so the relying party can go to the UserInfo Endpoint and request claims about the user, which would essentially be user attributes that would come back in a signed JWT. OpenID Connect also introduces an ID token, so in addition to your traditional OAuth authorization token, an OpenID provider can return an ID token, which is essentially just a signed JWT, it's got claims about the user, in the same lines of what you would get back from the UserInfo Endpoint. And there are just a couple of different flows you can use, depending on whether you want to make separate calls to UserInfo or you want to just get an ID token directly back from the OpenID provider. Next slide, please.

So just very briefly, security considerations here, we had a lot less to say about OpenID Connect because it's a much more thoroughly specified, if I can say that, protocol. It locks things down quite a bit. The ID tokens are encrypted...excuse me, signed and optionally encrypted JWTs. The...there's a set of...there's a defined OAuth scope that's used for OpenID Connect requests, which is actually called OpenID and then additional scopes can be specified to ask for additional attributes about their user. So, it really builds directly on the OAuth model.

So the main concern when it comes to federated authentication like this is that if someone can get their hands on a token of a valid user, they can impersonate that user to other web sites. And the spec has a number of features to help mitigate that risk; the JWTs are signed, there's something called c_hash that helps ensure the continuity of the whole OpenID Connect flow from start to finish to make sure no one's manipulating things in the middle. There are some other mitigations there. But the main thing to think about here is that the relying party really is placing a large degree of trust in the OpenID provider, so, especially if the information that comes back is being used for access control decisions. So, it's very similar to the use case...to the case with SAML, although unlike with SAML, the user's in control of granting you access to their attributes. Can we go on to the next slide?

So whenever you hear about the risks and vulnerabilities of anything you think, my gosh, this is terrible, I better not come anywhere near it, but, you always have to keep things in perspective. What is really the alternative? How much better or worse is this than what we do today or other options that are out

there? So if you think about what do people do today to give their software clients access to their information? Typically they will enter a password into something like an email client or another kind of software client to get it access to their resources. And that's really ceding all of the user's authorizations over to those clients to do whatever it wants with them.

There's no way to scope down the access. There's no way to revoke that access without changing your password. It just violates all kinds of security guidance and is, in general, not a good situation. OAuth tokenizes, you could say, that authorization and therefore makes it easy to manage and control. And really OAuth and OpenID Connect have a different mindset than we have historically had in the security world by bringing the user into the access control decision, to some degree. And that's frightening in many ways, but it also reflects the fact that we are enabling the users to interact with their data in the ways that they want to do it. So, users...it's up to the user to decide what client software, if they want to have a health tracker App on their iPhone, if they want to have a web site that's going to get their blood pressure and give them graphs and things like that, it's a very appealing use case for the users. It's outside of the realm of what we typically think of in IT security but, it's simply a change in mindset.

And then as I mentioned with OpenID Connect, where with SAML there's a decision that...the IDP is going to provide data to all the relying parties when they ask for it, now the user gets to say, well, what information is this website asking for? Do I want to approve or deny this? So, in many ways this is empowering the users while it may keep us security folks up at night a bit more. Can you go to the next slide?

And here are a slew of links. Our public site is there, it's got some other slides and documents, and it has the profiles themselves there. The second link is to an OpenID Foundation working group called HEART, which Justin is involved with, but they're actually looking at developing some specifications specifically for RESTful health APIs. And they're using our profiles as a starting point; they're also looking at UMA. So, that's interesting work there. The third link, a lot of my material is actually derived from the information that's in the OAuth 2.0 Threat Model and Security Considerations, a very good document. And there's another link there for OpenID Connect security. And then that final link is our main sort of security paper that has all the details that have been distilled down into this deck. And with that, I think that's my last slide.

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

Thank you, Mark. You know, you kind of skipped over your slides that have to do with registering clients. I know you were concerned with time, but I think that registering clients with the authorization server is a pretty important aspect of this, right? Did you recommend methods for authentication servers or authorization servers to actually register clients?

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

No, thank you. Actually I didn't mean to skip over that, it definitely is critical. So we talk a bit about that in the paper, but basically there are different ways you can go about it. There is actually a specification for dynamic client registration where it could happen totally automatically. It could be a manual process; it could involve some kind of review of the client.

This really depends on the relationship the organization wants to have with software clients. It could be as controlled a process as you want or it could be completely dynamic and I think the question is, how much control do you want over who gets to connect and how much resources are you really willing to dedicate to reviewing these clients as they're developed by developers who potentially have nothing to

do with your organization? And the ability to keep up with user demand as people come to you continuously with new clients.

We didn't have a specific recommendation we sort of outlined the options and the considerations there. I think a lot of us feel that an overly rigorous client review process is probably not going to keep up with demand and that sort of the only option is to go with, once a client has reached a certain threshold of let's say downloads in the App market and a certain reputation score, that it's probably acceptable until there's a problem. But obviously, some organizations may decide that that's not acceptable at all and they want to do a full review of the client before they let it in, and that's something that the organization can decide.

One other aspect of this that I didn't talk about because it's not really...not strictly security focused is that there's a good amount of interaction with client developers that needs to happen if you want to be an OAuth authorization server. So, you would basically need a website or some way for client developers to find out what they need to do to get registered, sort of what the rules of the road are, if you have policies about what they can and can't do, how often they can pull your backend services, all that kind of thing. And so, a lot of those day in, day out maintenance activities, there's a lot to think about there and I think a lot of organizations are still just figuring this out; so yeah, a lot of considerations on the client side.

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

Well do you see...do you think that any healthcare organizations will just simple develop...begin by; stick their toe in the water, by simply developing their own mobile Apps and using OAuth 2 to authorize them? So you register them because you developed them yourself, you think that they're very safe so they would feel comfortable using this new paradigm before they really allow other Apps. I sort of envisioned that that's the way things would happen as opposed to just always logging in through your webpage, they would say, okay, we've got this nice App you can download and use that and then use OAuth 2 to authorize it.

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Yeah, absolutely, I think...sorry, go ahead.

Justin Richer, MS – Principle Technologist – MITRE Corporation

I was just going to jump in if I may, this is Justin again. Yeah, I agree, I think that that's one way for a lot of more conservative and hesitant organizations to definitely get involved with this and I think that it may very well be the gateway towards a more open environment, because I agree with Mark, I don't think that the whole, we will build all of the Apps that you want to use, is scalable. It's not going to keep up with demand.

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

Yeah, I agree.

Justin Richer, MS – Principle Technologist – MITRE Corporation

And so one thing that we did inherit from the Blue Button Plus work is this notion of that there different kinds of clients and so there's a difference between a native client and a client in the browser and what not. And there's also a difference between a client that you've never heard of before, a client that 100 other users are using and nobody's complained about and a client that you developed in-house and had somebody go and manually register. And I think that there's ultimately room for all of these, and this is

something we haven't fully fleshed out, we touch on it very briefly in the profiles and related documents. But, where I think that we need to go with this is have guidance and guidelines on not only what these classes of applications are, but what it means to be able to deal with each of these.

So to give a concrete example, one implementation of the OAuth 2 authorization server, it allows dynamic client registration but, if you are the first user coming through with a dynamically registered client, you get a big red warning box on the authorization page saying, hey, this client just showed up, I've never heard of it before, it was registered seconds ago. So if you really want to be the first one through the door, okay, I'll let you scroll down and click okay. But just so you know, this is something new that just showed up. Over time as more users use it, as the registration kind of gets older without complaints and sys admins coming into the loop here, that warning gets more and more muted until eventually you just get the authorization page.

And so I think we'll see implementations of heuristics like that in order to deal with this spectrum of applications but what I think that we can do with work like what we're trying to do with the HEART working group is provide guidance for implementers of these specifications, so implementers of the authorization server, for example, to say, yeah, take dynamically registered clients, but warn people in these circumstances, have it...have that decision auditable in the following way and so forth.

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

Hmm, yeah, that's useful. Thank you. Do others have comments, questions? Are you guys out there? Do you have other questions for Mark or Justin?

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

Hi Dixie, this is Lisa. This question is almost for you, I'm wondering...I'm looking at the sources of additional information, the last slide and wondering if we might want to talk to the folks working on the HEART Project? Or if I'm...I'm trying to understand, is that different than...what are those specifications that they're developing?

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

Yeah, I thought that that was just being launched. I know that Eve Maler and Debbie Bucci are involved, is that fairly far along, Justin?

Justin Richer, MS – Principle Technologist – MITRE Corporation

That is just getting launched. It is now an official OpenID Foundation working group. The charter has been accepted and posted on the website, I actually just got the email from Eve earlier today saying, okay, the site's up, you can go sign the contributor agreements and get rolling here. So, it is just getting started. But that said they are looking to formally take the profiles of OAuth and OpenID Connect that we've developed...that we at MITRE have developed for the VA, the ones that we've been talking about today, as inputs into the HEART Working Group. So, those will actually be sort of revision 0, if you will, of the HEART Working Group documents. That's their intent at this time.

HEART is also going to be working on, as part of their charter, a profile for UMA, which as Mark mentioned at the head, we decided was a little bit much of a reach for our effort, but definitely something worthwhile. And also if necessary, a HEART profile for FHIR and specifically the places that FHIR overlaps with OAuth and these other technologies. So in other words, you have a particular kind of

FHIR resource, which scope do you ask for to be able to get that? It's not enough to be able to say, go get a token, you need a little bit more information than that and somebody needs to specify that.

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

So Dixie, maybe we do need to hear from them, just so we can...

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

I don't think they're...

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

No?

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

...I don't think they're that...

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

...that far along?

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

Well, let me...just ask you that just right out. Would it benefit us to...Justin, would it benefit us to hear from them at this point or if not, at what...how far along do you think we should...by the way, we've already heard from...had a presentation by Eve about UMA, so this group just heard from her a couple of weeks ago. When do you think it would be worthwhile to hear from Debbie and...I think Debbie and Eve are leading it, right?

Justin Richer, MS – Principle Technologist – MITRE Corporation

Yeah, Debbie and Eve and the Co-Chairs of the group, I'm probably going to be involved in some level of technical editing and implementation management. But, I would say...I would actually recommend sometime in the near future, because even though the concrete work is really just getting started, the charter itself and sort of the vision and goal is there...

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

Okay.

Justin Richer, MS – Principle Technologist – MITRE Corporation

...and that's something that's worth knowing about in detail and having a conversation about, in my opinion.

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

Okay, I certainly respect your opinion. That sounds like a good idea then, Lisa. Let's...Kris, why don't we make a note of that and maybe you could talk to or Julie, whatever, could talk to Debbie would be the easiest, just talk to her about scheduling them for one of our sessions in the near future.

Justin Richer, MS – Principle Technologist – MITRE Corporation

Sure, Kris, go ahead and work with me, I have all those contacts and we can get that worked out.

Kris Miller, LLM, JD, MPA, CIPP/G, CIPP/E – Principal Privacy Strategist, Enterprise Strategy & Transformation Division – MITRE Corporation

Sounds good, I'll reach out to you offline.

Justin Richer, MS – Principle Technologist – MITRE Corporation

Awesome.

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

Thank you once again, Justin.

Justin Richer, MS – Principle Technologist – MITRE Corporation

Yup. Oh, and I would...I think, I'll have to look up the exact date, but Eve has announced there is a public webinar that she's doing that's going to include Jeremy Grant from NSTIC and NIST that is actually going to also be touching on HEART and that's going to be one of the first kind of public forums, if you will, for HEART.

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

Oh yeah, we'd be interested...

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

Well do you know when that is?

Justin Richer, MS – Principle Technologist – MITRE Corporation

I would...she just tweeted it yesterday, so I would have to check. Let me look that up right now, if it's one of her top tweets, it should be easy...December 18.

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

Okay.

Justin Richer, MS – Principle Technologist – MITRE Corporation

So yeah, the...and it is an ONC sponsored hangout apparently. So, there you have it and that's on December 18.

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

Thank you.

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

Okay, thank you. Yeah, Kris, maybe you could get this group more information about that and just have it sent to everybody.

Kris Miller, LLM, JD, MPA, CIPP/G, CIPP/E – Principal Privacy Strategist, Enterprise Strategy & Transformation Division – MITRE Corporation

Will do.

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

Okay, are there other comments and questions?

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Hey Dixie, this is Jeff Brandt, excuse me.

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

Yeah hi...uh huh.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Hey, something I wanted to bring up just as a general for your information. I'm on the HL7 workgroup for mobile and we are now looking into doing a minimum data set, or at least doing the preliminary work for looking for a minimum data set for FHIR for mobile, exclusively for mobile and that would probably be more around we're looking at somebody to figure out how to refactor it to lower the overhead pri...something around OIDs, since there's so much repetition in the messaging for LMIC and rural solutions. So, I just wanted to put that out if anybody's interested, the workgroup is on Friday, would be, I think it's 8 o'clock Pacific Time and we could use some help if anybody's interested.

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

So that's like a subset of the meaningful use...common meaningful use data sets?

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

No, it's not...it has nothing to do with Meaningful Use.

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

Oh, it's not that, yeah, that really didn't either, that's a certification list, that's just what it's called. It's called the common...data set.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Yeah, what we're trying to do is be able to send the C-CDA is just...

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

Too big, yeah.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

...too verbose to run on anything lower than 4G, 3G probably fine, but...and again, we're just started looking into this, started working on it so I just wanted to bring it up if anybody was interested, we could definitely use some assistance.

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

Well you might want to look at the 2014 EHR Certification Standard defines a common Meaningful Use data set as a set of data elements that should be viewable, downloadable and transmittable by patients.

So, it's a patient subset, that's what it's intended to be and I would assume that a mobile set would sort of be aimed at consumers as well, right?

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture- Accenture

No, not exactly.

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

No?

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

It's a...I would definitely take a look at it, I appreciate the information. What we're really trying to do is facilitate a way to move data across mobile devices and this came from my push from the LMIC and rural committees, where if you drive 10 miles in any direction away from a metropolitan area, you will hit an LMIC or rural type environment as data throughput is concerned.

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

Oh, I see. Okay, great. Great to know, thank you.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

You bet.

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

Are there other comments? Questions?

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

Yeah, every time I see a presentation on OAuth and RESTful I pick up a little more. I think in another year I'll have it.

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

Yeah, good.

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

I feel the same way, Peter.

M

But you'll be a year ahead of me, Peter.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture - Accenture

This is Jeff again. That was an interesting...Jeff Brandt, sorry. I'm actually...just to let you know, I'm a manager at Accenture now of the RESTful API section, so it's apropos. One of the reasons there's such a push for REST is a) it's very easy, it's about as easy as you can do for protocol moving and one of the things that's interesting, and you brought it up is that the resource or EHR or whatever it is, is actually build system that other people can use to do what they need to do without really knowing about each

other. So it's very simple, once you start looking at it, it's even...it'll move big data elements usually like C-CDA...

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

Yeah.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

You say, get med list or give me "X" and so it's very, very simple and so, I'm glad to see that we're all moving that way.

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

Me, too. As I...throughout my career in security and Lisa as well, it's...people don't fully appreciate how important simplicity is to security.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Oh, exactly.

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

Complexity just creates vulnerabilities and simplicity is key to securing anything. So, I'm happy about it from that perspective as well.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Did you...I missed a little bit of this, I got cut off a couple of times, did you hear anything about the suggestion where they send the...to XML or...JSON or the weaving it into that?

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

They didn't get into that, today you mean? Yeah, didn't get into that. Yeah.

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Yeah, because that's one thing we should talk about, too and it really doesn't matter except for in a mobile environment, if you can go JSON instead of XML, you save a lot of overhead because XML is just heavier, it's more...it was developed for SOAP, as I heard him talk about that. And so, that's something that we should consider maybe in a recommendation on it, because there's plenty backing it, not just me saying it.

Justin Richer, MS – Principle Technologist – MITRE Corporation

Yeah...this is Justin; speaking as a developer and a tech lead that works with lots of developers, the answer is JSON.

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

Yeah, yeah...

Jeffrey Brandt – mHealth & Security Consultant – Brandt Professional Services, LLC; Manager, Technical Architecture – Accenture

Thank you.

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

...about that, yeah. I think it's...we're running up into our...we've run across our public comment time, so why don't we...why don't I once again thank Jason...thank Justin and Mark for being with us today, it was an excellent presentation and we sincerely appreciate it. Okay, Michelle?

Mark Russell – Cybersecurity Subject Matter Expert – MITRE Corporation

Thank you.

Justin Richer, MS – Principle Technologist – MITRE Corporation

Thank you.

Public Comment

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

Operator, can you please open the lines?

Lonnie Moore – Meetings Coordinator – Altarum Institute

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.

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

We have no public comment.

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

Great. Thank you again and thanks to all of you for dialing in. This has been a very productive and interesting discussion; so thank you.

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

Dixie, this is John Hummel. I'll get the suggested revisions that Kris is looking into by the end of today.

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

Great. Thank you very much, we appreciate your help. Bye, bye.

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

Thanks everyone.