

Privacy & Security Tiger Team Transcript July 16, 2012

Presentation

Operator

Ms. Robertson, all lines are bridged.

MacKenzie Robertson – Office of the National Coordinator

Thank you. Good afternoon everyone. This is MacKenzie Robertson in the Office of the National Coordinator. This is a meeting of the HIT Policy Committee's Privacy and Security Tiger Team. This is a public call and there will be time for public comment at the end. The call is also being transcribed, so please make sure you identify yourself before speaking. I'll now take roll. Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Deven. Paul Egerman? Dixie Baker?

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

I'm here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Dixie. Dan Callahan? Neil Calman? Judy Faulkner?

Judy Faulkner – EPIC Systems – Founder

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Judy. Leslie Francis?

Leslie Francis – National Committee on Vital and Health Statistics

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks Leslie. Gayle Harrell? John Houston?

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks John. David McCallie?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Here.

MacKenzie Robertson – Office of the National Coordinator

Thanks David. Wes Rishel? Micky Tripathi? Latanya Sweeney? Is there any staff on the line?

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Joy Pritts.

MacKenzie Robertson – Office of the National Coordinator

Thanks Joy. Okay, Deven, I'll turn it over to you.

Deven McGraw – Center for Democracy & Technology – Director

Okay, great. Thank you very much. What we have on our agenda today is, and Paul's not able to join us today. We are going to have a discussion about the hearing that we had last week on Trusted Identity of Providers in Cyberspace. Let's go to the next slide, let me see if I have the control here. Yup. We're going to discuss the next steps. All right, so here we are at the point of our first Tiger Team call post-hearing. We have one more call on the schedule; the one today is 90 minutes, the one on the schedule for July 24 is for a full 2 hours. Those are the only two calls that we have on the schedule to discuss the results of the hearing and decide what, if any, recommendations we're going to make to the Policy Committee at the August 1 meeting. So, that's really what we're going to do today is begin that discussion.

Just to be clear about where we think the focus ought to be for this discussion. It's really on the issue of identity proofing and authentication. As one of our testifiers put it, who's knocking at the door? The question of sort of what level of access you have to data once you've been properly identified and authenticated is really another issue and it's not one that we're going to take up in our recommendations. I think to try to sort of combine all of those issues at once would be quite complicated, I think it will be enough for us to get some...to make some headway on the issue of identity proofing and authentication, but, I think it's probably helpful for us to acknowledge that all that does is address the question of sort of...we can trust that we know who's at the door, but that doesn't necessarily translate automatically into data access, just because you've got those first two problems resolved.

Are folks comfortable with confining our discussion to those issues, since that's really what we covered in the hearing, although certainly a number of folks who testified as well as at least one of public commenters acknowledged that this is...it's not the whole ball of wax to just do identity proofing and authentication. The issue of access control and authorization to actually access data is another one, but not necessarily one that we can resolve with this discussion.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Hey Deven, you're planning on making note of the fact that authorization is there, we're just not going to address it, right?

Deven McGraw – Center for Democracy & Technology – Director

Yes, absolutely...

W

...I sent that email around, too.

Deven McGraw – Center for Democracy & Technology – Director

Yup, yup. And thank you for pinging me about that early, because that allowed me to introduce it and I think it's a great idea, that we acknowledge that again, there's a complicated set of issues around access to data and this is one slice of it, but not the whole enchilada. So...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Deven, the other point is that the conversation was confined to authenticating and identity proofing providers and not consumers.

Deven McGraw – Center for Democracy & Technology – Director

That's correct, thank you Dixie. We'll make note of that, too.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And Deven, this is David. I have one more suggestion.

Deven McGraw – Center for Democracy & Technology – Director

Sure.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

I think the...just completely in agreement with what you said, but the use of the word trust is one that we're going to have to be careful to restrict to the trust of identity, rather than trust that you belong here.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And I bring that up just because we stumbled on the fact and it took us a while to figure out what was going on when we were working on direct, that a lot of people in our conversation had a very different...many people in the conversation had different notions of what they were trusting, and we continually stubbed our toe on the fact that some people thought we were trusting at a different level than other people, and I think it breaks down into exactly what you specified here. But just if we start using a word like trust, we need to be sure that we're talking about trust of identity.

Deven McGraw – Center for Democracy & Technology – Director

Trusted identity, right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And then I have a question...

Deven McGraw – Center for Democracy & Technology – Director

Sure.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

...which I think we'll come back to maybe later, but I'll just register it. I was re-reading the NIST document that they were talking about, the re-release version of the 800-63 and it...I didn't really think this through the first time I read it, but they lump together identity proofing and authentication into levels of assurance and we tended to tease them apart. And I don't know which is the right way to do it, but it's an interesting question that we have to resolve. Do we speak in terms of the aggregate level of assurance or do we tease apart specific identity proofing levels from authentication levels.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Well, they don't...well, you're right, they don't at all. And I think that Phil Holt, I think is the name of the one who presented last week. He had a slide about level of assurance 3 that didn't mention identity proofing at all, and I think that that suggested that they could be teased apart, but in truth, they really...they're really not separate.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, I think that's a really good point that both of you have raised. Because I don't know that in any previous discussions that we've had on this topic, that we've sort of parsed...you know, made separate recommendations in other words, right down to the proofing and authentication and instead have tended to be...to more generally have lumped the two together, and in fact, pointed out as part of our comments on the NWHIN RFI, that in fact the RFI kind of lumped those two issues together at least in one or two places as well. So, I think it's worth sort of thinking about whether we need to make a distinction, in terms of our own recommendations between one functionality versus the other.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

I don't think we should, because the regulation doesn't.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

I think where it'll come to a head is if we try to reference back to the NIST levels, we may end up defining some mix of what we think is appropriate identity proofing and authentication that doesn't align exactly with an existing NIST level.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

In other words, we may be creating a level of assurance 2.75 or something like that, that's...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Right, and I think that's the danger if we try to tease them apart. I think it's important that we be consistent to exactly avoid that.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Well it would be ideal if we can be comfortable that one of the NIST levels fits what we think works in healthcare. I'm just not sure we're going to get there.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Right.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

David, this is Joy. I think that what we have found when we've been talking about this within the direct context is that it may be possible that the...you can match to the NIST for most of the requirements, but you may need to add additional requirements specifically for health.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, so start with a lower one and add a few to elevate it?

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Well, I don't mean it's to necessarily elevate it, it might further restrict it is the discussion...some of the things that I've heard discussed.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

I mean that's what the DEA did, right. I mean, they don't map exactly to one of the NIST levels, they put all sorts of additional constraints on there.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Well because...that comes not only to authorization, but it also comes a little bit to who can...well, it comes to...oh, it comes to authorization, authentication and authorization, I'm sorry, that's...

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

That's a good point that was a very good point.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

But, I think we need to remember that at the beginning of last week's meeting, Farzad said very clearly that he, based on every...all the advice he had been given and all what he had read, he believed that level of assurance 3, as defined in 800-63-1 was appropriate. And one of the purposes of the hearing, in his mind, one of the key purposes, was to determine whether that was indeed feasible. And he didn't say, my purpose is to figure out what we need to add on and take out and nuance, etcetera; he said we need to examine the feasibility of that recommendation.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Dixie, I would reiterate where I was stumbling just a few moments ago, is that we often lump in, and at times in the hearing too, the authorization piece of this, which does not necessarily have to be part and parcel to this discussion.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

It should not be, in fact.

Deven McGraw – Center for Democracy & Technology – Director

We've already agreed that it's not. So, John, did I hear you in the background?

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Yeah, I mean I just want to...so, is NIST, is that going to be sacrosanct or not. I mean, are we going to find ourselves at such odds in general if we decide to break up the level of assurances or rely incompletely on one level?

Deven McGraw – Center for Democracy & Technology – Director

Well, and I think we should talk about that as part of the substance of the recommendations, because certainly we heard a lot of testimony about creating some consistency in terms of trusted identity, so if there's sort of a level that's set that is a bar that everyone needs to come to, not only is it clear arguably in the healthcare context, than it's clear in other contexts where that identity credential might be able to be used as well, such as for exchanging information with the government where a specific level is required. I mean, those are sort of the considerations I think that you have to weigh when you're either choosing a level or if you're not going to...that may be different from where some of these other initiatives are headed, where you're choosing to sort of create your own level, that is not specific to the set of criteria that others are using, but it's different for healthcare. But again, it's something for us to talk about and not to necessarily take as a given.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

It also sounds like, to some degree, that if we choose not to, which I think we may end up doing from my perspective, we have to figure out a way to map to whatever level...NIST level we...I mean NIST level 3 so we can say where there are differences and what needs to be done if, in fact, somebody feels it wise to then have to map to a particular level for some other reason.

Deven McGraw – Center for Democracy & Technology – Director

Right. Well, let me, let me...I was struggling myself with how to sort of launch into a discussion about what we heard at the hearing and how that might translate into a set of recommendations, beyond the mere question of should we do level 3 or not, or something...or level 3 as a baseline, allowing people to go to level 4, or what should be the LOA for NIST guidance. In part because one of the things that was to me a persistent theme of the hearing that we may need to tease out is the question of, do you credential at the organizational level and require those organizations then to credential their individual users and do you set a level for that or do you just trust them to do the right thing, in the words of one of our panelists. And so, I've got this slide up now is a very brief summary of some previous recommendations that we've made on this topic. There are, of course, slides in the back-up portion of this deck that mimic the ones that we used at the hearing that are in more detail. But essentially, on the one hand we have previously said that on the digital certificate issue, those should be issued with a "high" degree of assurance issued at an entity level, with each entity then deciding to credential its individual users, which assures a sort of trusted machine-to-machine transfer of protected health information.

But we've also said previously that individual level credentials for accessing information across a network or remotely, should be issued at a level higher than just user name and password. And this is the place where we were reluctant previously to land on a specific level. And then our other recommendations, in terms of sort of the use case, the universe of exchange that we have tried to cover, we have tried to think about what is going to be needed to facilitate exchange among providers to meaningful use. And I posed as a question about whether this should continue to be our focus, meaning to sort of think about the universe of transactions for meaningful use, but I strongly encourage us to be thinking of those transactions so that we're not trying to solve for every possible exchange of data under the sun.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Well I, this is Dixie, one of the key take-homes that I gathered from the hearing was that virtually everybody was talking about individual level certificates. In fact, you'll recall that when I asked the CMS guy, Tony Trenkle...yeah, when I asked him about whether CMS was preparing itself to accept direct transactions that were based on organization level certificates, he goes, "you know yeah, we follow the direct project, blah, blah, blah"...but virtually nobody said that they were dealing with organization level certificates. Now, when we did talk about trusting organizations to distribute certificates to their people, that was not a conversation about issuing an organization level certificate, it was conversation about setting up an organization to provision individual level certificates, which is a different topic. And I came away thinking, you know, we probably should not be talking about organization level certificates, because none of these guys are.

Deven McGraw – Center for Democracy & Technology – Director

Except for Rick Rubin.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Except for Rick Rubin, but his came across as very loosey goosey to me. You know, they said, well, eh, you know, we do whatever our people tell us they want us to do...(indiscernible) exchanging with federal agencies I didn't hear that at all. And even he didn't talk about organization level certificates.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

But how...I don't see how you can do this without organization level certificates and have enough logic in the environments to make it really robust.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

So you can identify an organization in an individual certificate, you know, it's not like if you accept a certificate from Dixie Baker, it can't possibly say that this is an SAIC certificate, chances are it would, right, within the certificate. But, the certificate itself issues at the granularity of an individual.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

Yeah, but what happens though if I have a physician who has a private practice and has medical staff privileges at three or four hospitals, is it robust enough to handle that? Because I'm a little fearful that we end up having misalignment of who that physicians actually performing services for at any given time.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

So the certificate is aimed to authenticate your identity. So, you go in to hospital A and it goes, oh yes, this is John Houston. And then the hospital itself, this is exactly what Joy was talking about, don't get it confused with authorization. The hospital itself goes, oh, oh yeah, John Houston, here is what he's authorized to do at my hospital. But to just get in the door, it just identifies you as an individual. And you may have totally different authorizations at hospital A versus hospital B; in fact, hospital C you might even be a patient. But that is something that's not visible at the certificate level, the certificate just authenticates you as an individual and then figuring out what you're authorized to do remains a function of the hospital itself.

Deven McGraw – Center for Democracy & Technology – Director

So, we did actually Dixie, call for...this is Deven again, a digital seamless level at the entity level, I'm 100% sure.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Absolutely we did. What I'm saying is...that's why I asked that question to Tony Trenkle, because at the hearing, everybody was talking about individual level certificates.

Deven McGraw – Center for Democracy & Technology – Director

Right, that's clearly the case. Certainly, that's what the NSTIC effort is leaning towards; the FICAM credentials are all of this. And NIST 800-63-1, and its predecessor, all focused on individual level credentials. And so I guess what I was positing is whether in fact, this is...whether sort of organization-to-organization hand-off and authentication works for some use cases, but doesn't work for others. And is there a place to sort of make a distinction and maybe it's not a distinction that in the long run will be terribly meaningful, because one thing that you could ultimately require is if everybody...if individuals themselves should be credentialed at a certain level, it's to set that requirement on organizations with respect to the credentialing of their own individuals. But, I'm getting a little ahead of myself. I just was wondering whether there are some distinctions that could be made by use case, or is it more of a temporal issue, where it's going to take some time. If, in fact, we want to have individual level credentials at a certain level, do we need to acknowledge that it could take some time to get there.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah Deven, this is David. I think that it seems inevitable that at some point in the future, it will all be based on individual credentials. And the providers who write prescriptions will be forced into that via the DEA, regardless of what we say. And if NSTIC or its successor succeed, more and more of the populace will be comfortable with that approach. And it seems in healthcare, it's just inevitable that we'll eventually get there, in which case, our task might be to define a reasonable timetable, perhaps in terms of meaningful use stages, and to kind of lay out a stepping stone or road map that says, here's what is acceptable today, but here's where we're headed and here's what's going to be required circa 2014, maybe part of Stage 3, however we decide to do it. We're not going to avoid eventually landing up with individuals...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

I think we should look at whether...we have assumed, no question about it, we have assumed that organization level certificates were available and could be...you could go out and get one, and all that. After the hearing, I even questioned whether if we continue to say, well this is organization level certificate, I question whether we're even asking for them to step back, because right now it doesn't sound like anybody is issuing them.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Well I think Dixie, what happens today is people issue them through ordinary certificate authorities and then do joint, pair-wise, trust relationships. So, you know, hospital X could go get a certificate and then position it to others who they want to have commerce with and say, here's the certificate that I'm signing my direct messages with, will you add it to your trust chain. And people say yeah, we'll add it. And...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

So it's an individual level certificate, but the organization steps up and takes responsibility for its use.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Correct. And it's more what it's not. Each individual person who sends and receives messages does not have a PKI certificate; only the organization that has authenticated them and using internal best practice approaches to authentication. So, it's better defined in terms of what it isn't. It isn't a credential for each account; it is one credential for the organization that has provided you with an account.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

It's sort of the equivalent of allowing, by policy, not winkie, winkie, but by policy, you might have a small clinic that you have one password to log in to the system, and that's okay, my policy allows that. In this case, they're saying, okay, we have one certificate and we allow you know, Susie at the front desk and Dr. Jones to use it. Is that what you're saying?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

No, no. Each individual is robustly authenticated into the hospital's system, because that's required under HIPAA and...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Right, I know, but I mean, it's the moral equivalent of that. You're saying multiple people are using a single certificate.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

No. Well, multiple...the certificate is only guaranteeing the integrity and the organizational source.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

It's not guaranteeing anything about individual non-repudiation and the like. We've covered that ground.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Right, but it's issued to an individual.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

It's issued to...it's effectively to an organization; I don't know how they got it. It could even be self-signed. In fact, most of the ones today are self-signed.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

But we keep hearing that there's...nobody's issuing, even self-signing, organization certificate as defined in the PKI rule, right, a certificate that really is issued to an organization. We keep hearing that nobody is doing that...

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

I heard Rick Rubin say they're doing it.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, I did, too. I don't think it is the case that no one is doing it Dixie, it's not...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

(indiscernible).

Deven McGraw – Center for Democracy & Technology – Director

But it's what is very clear from our previous discussions is whether that can be sort of recognized under the Federal Bridge/FICAM framework, which...

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Right. And anyone who's using exchange is doing that today, by some means. They're getting a certificate from somewhere, those are not individual.

Judy Faulkner – EPIC Systems – Founder

This is Judy and...

Deven McGraw – Center for Democracy & Technology – Director

...Judy's trying to break in, go ahead Judy.

Judy Faulkner – EPIC Systems – Founder

Yeah, that's what we do here. We issue certificates using the exchange methodology and basically the organization that joins a group of organizations who all together honor and respect those certificates.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

So, are they server certificates Judy?

Judy Faulkner – EPIC Systems – Founder

Yes.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Okay. So we still...we know we have server certificates, so...

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

They may not be server certificates in the technical...

Judy Faulkner – EPIC Systems – Founder

They're server and client.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Machine certificates.

Judy Faulkner – EPIC Systems – Founder

They're servers and clients.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yeah, um hm.

Judy Faulkner – EPIC Systems – Founder

They're machine.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yeah, machine certificates is a better...good point, right.

Judy Faulkner – EPIC Systems – Founder

And also the other thing is, I think as we look at this, I don't think the system is broken yet, we haven't seen or heard of problems with it, and so I think as we figure out what to do, both from the point of view of the individual and the organization, especially for the individual, we should go slowly on what's coming up next, because our experience, and maybe yours is too David, that the individual physicians who have to log on one after another, after another time as they enter different places, as they leave and as they return, can't stand the loss of time if that becomes a complex procedure.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Judy Faulkner – EPIC Systems – Founder

That's why for some of them, what they do is they have one login for a certain period of time, and then they, if in fact they walk away; if they come back in a certain period of time a proximity sensor could say, "it's still you, you've only been gone for a very short period of time, it's still you." If it's a longer period of time, then it can evoke some more entries to make it multiple things that they have to do, but, the idea is to make it simple. I think if we go too fast, we may make it complex and then we'll get...produce a lot of problems.

Deven McGraw – Center for Democracy & Technology – Director

Right, which I hear Judy, and in that particular circumstance, and I think that's good to remember. But, the one thing that also occurred to me about individual level credentials is when you have providers with multiple affiliations, that if they had a credential that was recognizable by multiple systems, in fact, they would almost be better off from that timing perspective, unless I misunderstood what folks were saying. Because they wouldn't need separate credentials for each system that they tried to access; instead, their credentialed one time, through a recognized process, and then those credentials can be recognized in multiple locations.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, that's almost...this is David. That's almost a parallel or independent question, which is, who owns the certificate in a sense, and what's the scope of use of the certificate.

Judy Faulkner – EPIC Systems – Founder

That's right. And what happens if you've left one, they want to be able to take you off immediately.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Judy Faulkner – EPIC Systems – Founder

And you might still be on the others.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

That all goes back to my comment about organizational sort of certificate/how do you keep the logic in place to manage all that.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

I think what...one of the things that we heard pretty consistently, maybe I extrapolated but I think it fit what we heard, was that within a well-defined group of people, which might include multiple organizations that have good relationships with each other, it's possible to define rules that everyone trusts are adequate for that group of people.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

You only get into trouble when you start trying to bridge that trust to groups of organizations that you don't have such a close relationship with. And again, sometimes that's more about authorization than authentication, but, it'll eventually come back to authentication.

Judy Faulkner – EPIC Systems – Founder

I don't know if we found that to be accurate David. When we first started in with interoperability, we did find that people pushed back, I need the trust to know everybody. But after a while, it didn't become that at all, it was, as long as there's this central body saying everybody is okay, then it is the patient's right to go wherever that patient wants to go, and have the information follow. And it doesn't have to be that I just agree on those.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Judy, I...this is David again,...I agree. As long as there's that central organization that people can look to. We heard stories in Washington of the difficulties of building cross-HIE trust. It wasn't stated it would be impossible, but it was definitely harder and required a lot more work than it did within the existing HIE. And the point I'm getting at is, I think consistent with what you said a minute ago, which is that we should go slow because it's not really broken, we certainly aren't in an ideal state yet, but it's not broken. And, that's why I think in terms of a broad timeline that says, we know that eventually individuals will possess cryptographic credentials to prove that they are who they say they are, and in healthcare, this may happen a little bit ahead of the rest of the population, I'm not sure. Healthcare doesn't tend to be ahead, so maybe it won't, but whatever, and will eventually happen, and we should really be scheming about what's the right step-wise way to get there that doesn't put too much stress on a system that isn't already broken, and that accounts for external factors like the DEA e-Prescribing use case, which will, of course, drive a lot of behavior, since that's so critical to physician activity.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

I totally agree that we shouldn't push too hard, or we should get in step with how things are moving. My biggest question is whether we need to reword or re-couch recommendations we've made that specifically refer to organization level certificates. And maybe, specifically refer to machine certificates versus individual certificates, but I think that we need to get into good solid alignment with what exists today, instead of like forcing people perhaps to go into the organization certificates that don't currently exist. That's all I'm saying.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Well, I certainly think we can be...we can add some clarity to our previous recommendations, because I think we were talking about machine level certificates. But let's, I want us to focus on where this conversation seems to be going, in terms of sort of a timeframe or a set of recommendations to sort of step up to individual level certificates and what needs to be in place to have that trusted identity, because we either specify a timeframe or we state that we want the NSTIC process to specifically focus on this issue, or we ask for some other foundational elements to be...urge ONC to put some other foundational elements in place to make sure that it happens. We specify a level that we think that we ought to be aiming at if we're comfortable with that. And I think since Dr. Mostashari did raise it at the hearing, we should definitely have it on the table. So I want to move us into that discussion.

But I'm also sort of curious about something David, that you said and that was a central theme, or a bit of a theme of some of the last conversation, which was that there's some central organization to rely on, which allows the credentials issued by multiple different parties to sort of be trusted by the network as a whole and not just within a closed...not just within a community that has agreed to trust one another and to share data. What would that look like?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Well, I mean, I can give you the example of what a number of people who are working on direct are trying to do, it's to create kind of a not-for-profit directtrust.org was the working name, which would essentially define the rules of the road for good behavior, that if you followed, would assure others that you, since you have that sort of seal of approval, if you would, that you had implemented the proper practices so that you could be trusted at this identity level that is defined for direct. And that the rules of the road would be a combination of audit and self-assertion and to be determined, waiting in some measures on the NwHIN governance RFI to know exactly what that would look like. But, it would be essentially, just call it rules of the road or minimum standard behavior that you would adhere to. And we see this in commercial services such as the extended validation certificates that a lot of banks and other financial institutions use, which in order to obtain a certificate for your SSL service, you have to do additional proof that you are, in fact, the Bank of America and so forth. And if you do that, and if you pay your fee, you get a EV certificate, which makes the browser bar light up green. So, it's analogous to that. It could be a single vendor who does it across their client base. It could be a vendor coalition; it could be the NwHIN governance at some point.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Judy Faulkner – EPIC Systems – Founder

This is Judy and I can give you a little bit of our experience.

Deven McGraw – Center for Democracy & Technology – Director

Okay, yes Judy, please do.

Judy Faulkner – EPIC Systems – Founder

I was just talking, I think we've had maybe 65 million people covered right now for interoperability and those signed up are probably over 100 million, and we so far transmit about 1.2 million records every month via interoperability. Our customers all sign the same rules of the road, and they know everybody else signs those same rules of the road, and then we give them authentication certificates so that they can...which we do through the exchange, as you were talking about. And then they allow each of their staff to get a...to get authorized, because they've hired the person, they see the person, the person comes in, they know who the person is, and that person then gets a password. So, it is just password based for some, I think for most actually. And so far, we have not heard of it being broken. Actually, the password concept has been used now for thirty some years and we have not heard of it being broken.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, I think...this is David. That's consistent with our experience.

Judy Faulkner – EPIC Systems – Founder

And I think the idea of the vendor coalition is a great one, where the vendors get together, share rules of the road, and then we're all...then the sending back and forth can go much easier. Or the government has rules for the road for everyone...

Deven McGraw – Center for Democracy & Technology – Director

Right.

Judy Faulkner – EPIC Systems – Founder

...that's fine, too. I don't think it's particularly good if you do it individual HIE by HIE.

Deven McGraw – Center for Democracy & Technology – Director

Well yeah, I...that seems to not create a sense of trust across an entire network.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

No, and it's incredibly expensive, just takes forever.

Judy Faulkner – EPIC Systems – Founder

Yeah, but you can send to us David, we can send to you and that would work easily.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

I think we actually have a team talking about it as we speak.

Deven McGraw – Center for Democracy & Technology – Director

Really. And as part of...what, your participation in NSTIC or as a separate effort.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

No, no, just there's a working conversation going between Cerner and EPIC about our implementation of exchange connecting with their implementation of exchange. And I'm not on that team, but I know it's...the conversations are underway.

Judy Faulkner – EPIC Systems – Founder

And I think if you took the major vendors, you'd cover huge amounts of the U.S. fairly quickly.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Some of it is technical and some of it is the trust issues.

Judy Faulkner – EPIC Systems – Founder

Yeah, we don't try and look for the technical, as long as everyone's following the standards, we think it's pretty simple that way.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, the problem with exchange is there's more than one definition of what the standard is. But yeah, those are the minor problems...

Judy Faulkner – EPIC Systems – Founder

Yeah.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

...the trust issues are much more of the thing that people focus on, I agree.

Judy Faulkner – EPIC Systems – Founder

That's right, and they can be overcome.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, yeah.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Is there any way...this is Dixie...would it be appropriate Deven for the Tiger Team to make a statement that we would encourage coalitions among vendors to agree upon rules of the road type policy. I think that that is a way to achieve interoperability and trust...and trusted operability much more quickly than from the top down sort of approach.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And, this is David, I think that's what our feedback Dixie, the conversation that you led at the Standards Committee meeting, was to the NwHIN governance RFI, was that...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Um hm, yeah.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

...some very high level standards would be defined as certificates for interoperability or whatever the term they used, but that at the practical level, it would be private entities that just got together and created, I forget all the technical words that we used...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Conditions for trusted exchange, CTE...

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, the conditions of trusted exchange would be very high level, broad-based things.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Like saying LOA 3 that might be one of those broad-based...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yeah, yeah, that's right.

Deven McGraw – Center for Democracy & Technology – Director

Well that's...I mean, I think that's really interesting. I think the only thing that makes me...I mean; I actually think that if a private sector solution among the vendors helps to resolve this issue, I think that would be terrific. Are we fairly certain that that can occur without some government intervention, or is this...or is there a role that the NWHIN CTEs, for example, could play, not that we're trying to comment on an RFI that's closed, of course, but just speaking generally.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

So this is David. I mean, I think of course anything is possible with the right judges and incentives, but, it's...with direct anyway, which this is my first experience with trying to do something like this, it proves to be a lot trickier than anyone had expected. And there were, I don't think any problems that weren't overcomeable, but we just ran into a million reasons why we should do something different than what seemed like the simplest way to do it. Everything from, there are large companies out there that already do this for healthcare and they didn't want to be disenfranchised, so they thought they should do it. And they thought anybody who did anything less than what they do would be untrustworthy. And you get into arguments about, well is trustworthy enough, and then...it was...we had hundreds of conversations. So, I think guidance is going to be required more than just at the level of "go out there and do something."

Deven McGraw – Center for Democracy & Technology – Director

Right.

Judy Faulkner – EPIC Systems – Founder

Although I do think that, we had some of those same discussions in the very beginning...

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah.

Judy Faulkner – EPIC Systems – Founder

...but we've been probably doing this for six years now or something. We've had some of those and they just fade into the distance. I'd hate to see us go down a path that was wrong without taking into account what you folks have learned and what we have learned in the doing, because we might go down a wrong way. It took...the reason it took a lot of discussions was to find the right path. And one of those big things was creating the rules of the road and who should be able to get the data. The biggest argument we had, which was an interesting one, was that organizations wanted to pick and choose who they would interoperate with. And we said, "no, it's with everybody, because it's the patient's choice," and they would say, "no, it isn't the patient's choice, it's their choice." That's where the biggest problem came.

Deven McGraw – Center for Democracy & Technology – Director

Oh boy. Well, and that seems to be more to the actual authorization question of what data do we actually access versus rules of the road for identity purposes, right.

Judy Faulkner – EPIC Systems – Founder

Well, it wasn't even what data, it was fear of losing my patient to another organization and the fear of paying another organization the ED funds when they wanted to the patient to go to their own EDs, stuff like that.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

But you know, that's a perfect example of something that really you don't want legislated. And I think David's right that the concept that we're expressing here is consistent with our RFI recommendation. But I also think that we could express support for the same concept without referring to the RFI, and that is, that regulation...federal regulation should establish the rules for the road at a very high...basic high trust level and that the details about how those rules are interpreted with specific exchanges, really are ideally established by the community and vendors, vendor communities and HIEs.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

This is David. Agree with all of the above. Judy, our equivalent in direct was in that same thing, it's that some people said, we want to decide who our doctors can talk to, and the direct leadership said basically no, this is universal, we'll set minimum standards of identity assurance and then everybody can talk to everybody, and you'll make the decision based on patient care and patient wishes. So, I totally agree that it shouldn't be that you can pick and choose. But, I want to remind ourselves that we got this to this state with even comfort and then ran into the federal issue, what's the...

Deven McGraw – Center for Democracy & Technology – Director

The bridge, the FICAM issue...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yeah.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Bridge, the Federal Bridge. Right.

Deven McGraw – Center for Democracy & Technology – Director

Well right, although that was because we were looking for a way to cross-certify to the Federal Bridge a machine-level certificate.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yup.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

But if we...if we set up...if we say to private industry, go figure this out with the rules of the road, make it work, which I think would happen, could be done, and CMS says, yeah, but we can't talk to you because your certificates don't come from the Federal Bridge...

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

...then we've got a problem because that's 50% of healthcare.

Deven McGraw – Center for Democracy & Technology – Director

Well, but maybe that's maybe a rule...does that constitute a rule of the road that says, it's a baseline of level of authorization 3, and it's done through a provider who's been certified or cross certified.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

That gets us back into the conundrum of the Federal Bridge doesn't really know how to issue those kind of organizational certificates and if institutions do their own password management, that really is an LOA 3 by NIST rules.

Deven McGraw – Center for Democracy & Technology – Director

Well right, although I thought that we were talking about a timeline of sorts, maybe unspecified timeline, for moving the industry to individual level credentials.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, yeah, yeah. So, I...

Deven McGraw – Center for Democracy & Technology – Director

Well, we cannot solve the issue of...and maybe will not be able to solve the issue of machine level certificates that are cross-certified to the Federal Bridge, but certainly if what we're aiming at is individual level credentials anyway, couldn't rules of the road that allow for exchange of data with federal agencies be part of what we would recommend?

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Well one of the things I heard pretty clearly last week is that cross-certification of this Federal Bridge is not going to be a requirement, but consistency with the FICAM framework is.

Deven McGraw – Center for Democracy & Technology – Director

Yes, you're right Dixie I'm mixing...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

So, I feel more comfortable with that.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

But, so, this is Joy. FICAM, I think, this is confusing in general and it's taken me a while to get...so, Federal Bridge is associated with FICAM. The Federal Bridge piece is PKI, but FICAM also accommodates non-PKI solutions.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Um hm, right.

Deven McGraw – Center for Democracy & Technology – Director

But I guess if I'm hearing Dixie correctly, there's a comfort level with referencing FICAM because it doesn't box you into a PKI solution.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And, somebody...I think, on the panel, suggested that FICAM could build out a process that would allow for non-PKI organization level approaches, but they don't have one because no one's ever asked for one.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, I did hear that, too.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

The only non-PKI things they have approved so far, the one from Verizon and from SAFE, are for individuals.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

And SAFE BioPharma...there are four of them, OIX, Verizon...

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yes, that's right, there's a couple that have been added, that's right. But they're all still individual.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Yeah, they're all individual.

Deven McGraw – Center for Democracy & Technology – Director

They're all individual.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

This is Joy. So, I just want to clarify what the prior conversation was about, which is, when we were talking about Federal Bridge and...when you were talking about Federal Bridge, we were talking about it in the context of the direct project, which it's my understanding required PKI solution, which is why we were focusing on the Federal Bridge in that specific context. But you are absolutely right that FICAM is broader than PKI solutions. So, you'll...FICAM is broad enough to accommodate a PKI solution using Federal Bridge, but also non-PKI. If you're referencing just the direct project, then you are limited to PKI. David, isn't that right?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yes Joy, that is correct for the organization certificate that signs the messages before they go out on the email wire. So, the individual user who logs into his HISP and composes a message does not need a certificate, a personal certificate. So, only the organization needs one, and that is PKI-based. And even the so-called non-PKI things are actually PKI under the covers, but that's a different point.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

But that whole...the whole direct project is based on trust anchors that maybe more like a web of trust than a strict PKI, hierarchical PKI.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Well, not necessarily. If...you could do it that way with every...with pair-wise agreements of whose certificates you trust, that's what we were trying to avoid for the reasons that Judy listed earlier is people want to pick and choose and we don't think that's good in the long run for the organizations or for healthcare.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

So, what we were going to do is to say, if you meet the minimum standard of behavior, you can go get a certificate from one of the approved certificate authorities, which would use a CPS policy to validate that you had, in fact, behaved properly, you get the certificate. And then everyone would trust you, because you got a certificate under a valid certificate policy. Just like my SSL browser pack lets me trust thousands or millions of websites, because they all got their certificates under a certain GPS.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Um hm.

Judy Faulkner – EPIC Systems – Founder

And then they...

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

So direct is going to work exactly the same way.

Judy Faulkner – EPIC Systems – Founder

This is Judy. And, continuing on from what David just said, in the rules of the road themselves, there are policies for what if someone misuses that, they can be thrown out.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah.

Judy Faulkner – EPIC Systems – Founder

Then we have a team of customers who have representatives who are the guidance team for if there is something that goes wrong. Now, there never has been anything that has gone wrong, but they are there in case. Now that's a very interesting thing, because if someone misuses the security and something is wrong, and the next patient comes in, and you're going to go have a major operation there and you want your data over, it's a very interesting situation, can your data no longer go over because somewhere within there, there was a breach of security. Very interesting things, because I, as a patient is going to want my data over. But that's why we have a group of physician customers and others on top of this, rather than us, and we don't have to be in the middle of that.

Deven McGraw – Center for Democracy & Technology – Director

That's a...Judy, that's an issue that Neil, I recall Neil Calman bringing up in some previous Policy Committee meetings where, there is a desire to sort of punish the entity that sort of doesn't play by the rules of the road from a trust and security standpoint. But at the end of the day, if the patient needs the data to flow, that's...

Judy Faulkner – EPIC Systems – Founder

The data has to flow, right. Yeah, it's very interesting.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And, this is David, I want to...I know we agreed we were not talking about authorization, but one of the problems that we...one of the sticky points that you run into when you have rules defined about your proofing and level of assurance is you can have some of the authorization starts to bleed into the authentication. So for example, our own Tiger Team has recommended that certificates for direct only be issued to healthcare organizations. So, what's happened there is you bleed a little bit of authorization, i.e., you're a healthcare organization, into the authentication step, and I think that's what would run into in larger scale if you tried to do this, is you say, universal connectivity, somebody's going to say, "but I don't want to connect unless they're doctors," and then somebody else might say, "I don't want to connect unless they're good doctors," and then somebody else may want to say, "I don't want to connect unless they're good doctors who have never had a HIPAA violation."

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And all of a sudden, you've now really drifted into authorization, you're not worried about identity anymore, you're worried about who has rights to do things.

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And that's why it's just so dicey, because in the real world, people don't always keep really clean lines between these things.

Deven McGraw – Center for Democracy & Technology – Director

No, I get that. But, I think a part of our job should be to try to keep those lines clean.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Oh, absolutely. We need to be rigid about it. In fact, I kind of regret that we made the decision to say you have to be a healthcare organization, because that just opens the door to sort of saying, well, you have to be a healthcare organization in good standing...you're state regulators and...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

That isn't authorization. Authorization says what you can do and what you can't do, your privileges. That's just part of constraining the rules of who gets a certificate...

Deven McGraw – Center for Democracy & Technology – Director

Yeah, but it's not true identity Dixie. I can see David's point, it's much more about sort of whether there's a comfort level with sharing data with an entity that goes beyond just are they who they say they are.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

It is...you're right, it's to the level of yes can you play or can you not. Yeah.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

And all candidates who...it's one of the issues we're dealing with in the state of Pennsylvania is, who can participate in some of these exchanges, and there's a pair community out there that absolutely considers itself to be providing treatment services and wants to participate.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, the ability to land an email in my inbox is, in a sense, an authorization. If the system will let you send me something, then you have crossed into an activity.

Deven McGraw – Center for Democracy & Technology – Director

Right. Right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Again, I don't want to go back and revisit that, by no means am I suggesting that. I'm just saying that that's what makes this stuff so difficult.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

David, it might make you feel better, but you didn't limit yourselves to healthcare organizations, you said healthcare related, which is a much broader area.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

That's true, we were worried about excluding I think Wes used astronauts as the example, but...I mean NASA is a healthcare organization in some broad sense. No, I agree Joy. And we, I'm glad we did it that way because it was too difficult to say, if you're covered under HIPAA, well that excludes a bunch of people that are legitimate healthcare providers, like dentists and other things. So, anyway, it's just a tricky problem, the fact that it hasn't been solved is more a reflection that it's hard than that no one wants to solve it.

Deven McGraw – Center for Democracy & Technology – Director

Right. Well, so what would be the rules of the road that we would...we could recommend, just sticking to identity and authentication for...that would be sort of the measure to ensure trusted identity, even if you have sort of multiple organizations, like vendors, doing the credentialing. What would we recommend? Is this where we have the discussion about level of assurance?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

What if we took an approach that said something that we believe NIST level 3, level of assurance 3, is an appropriate minimum, you obviously can go higher, but it's an appropriate minimum that healthcare should target by the year X. Whatever we pick for X, maybe we say it's by the end of meaningful use Stage 3 or something, and that en route to getting there, we recognize the need for a stepwise progression around both the proofing requirement and the management of certificates. And then define a series of steps that start with kind of what current best practice is, in other words, what we're all comfortable with today. Rick Rubin maybe his testimony kind of being an example of...

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

...current best practice, and then sort of say by such and such a date or by such and such a Stage of meaningful use, if we want to keep referencing back to that, you should have implemented these...you should have reached these levels of compliance with NIST level of assurance 3.

Judy Faulkner – EPIC Systems – Founder

If I could comment on that. I could see that if in fact we do...we need it, but if we watch what's going on, get feedback and people feel that where it is comfortable, I don't think we should keep adding more locks to the door, to lock the...doors currently working well.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, I'm sympathetic to that from the point of view of moving forward with just getting people using these systems; I think the federal government's needs may be the determining factor...

Deven McGraw – Center for Democracy & Technology – Director

Right.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

...of what we...CMS is bound by a different set of constraints than we vendors.

Judy Faulkner – EPIC Systems – Founder

Yeah, but I still think that we're going to get horrendous pushback if we make people go through a lot of effort when we can't show any cause for having to do that.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, and I'm...Judy, I'm certainly saying that the status quo is good for where we are now. So for example, on identity proofing, I would say that a hospitals existing credentialing operations are perfectly adequate for identity proofing, at the level of healthcare transactions. And if we want to say something like in the future, physicians may achieve independent possession of certificates, as part of an NSTIC effort, because they want to have one fob that will work at all of the places of care and also works at their bank and also lets them authenticate to their website or whatever, then those would be...as long as that level of assurance met a certain NIST standard, it would be acceptable, in lieu of or in place of the hospital's credentialing.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

I also would like to remind everybody about some...I'm looking at the...you know, Farzad's talking points from last week, and he made the point that, well, let me read it. "If there's one thing I'd like to stress today, it's that the status quo is not good enough. Too many doctors have to use twenty or more user names and passwords each day. Too many doctors have their online identity stolen, as we'll hear, it can be a career ender. We should be aiming to develop policies that allow for high level assurance for trusted identity for providers, without cycling innovative technology solutions, and I believe it's possible for us to do that together." I think he made a really important couple of points there, but the password issue; doctors have to remember all these different passwords, etcetera. Having a digital certificate is a really important enabler for single sign-on and for making the workflow easier for doctors. So, passwords are not a panacea by any means. I mean, later on in the testimony it was also pointed out that all the...how many breaches in the past year were related to passwords. But, a digital certificate is not an additional barrier for doctors, it really is a way to make the workflow easier for them.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

It is Dixie, but it comes at great cost to go and retrofit across an organization that many of whom are using single sign-on technologies that are not certificate-based.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Right, that's right, but, it's a direction that I think it was very clear that...if we heard one message, it was that one, that the status quo is not good enough.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Well, we were hearing.

Judy Faulkner – EPIC Systems – Founder

But I do think...let me give you a rule of thumb we have observed with users in solving software. Seventy percent of the changes they make before they go live are wrong, seventy percent of the changes they make after they go live are right. And that's why I think it's better to see how each step goes before putting them into concrete.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Sure, absolutely. Totally agree.

Deven McGraw – Center for Democracy & Technology – Director

Well, yeah. I mean, I think that's a really good...it's an excellent point. You know, level 3 credentialing at the individual level, the handwriting seems to be on the wall, both because of the concerns that many people have about mere username and password from a security standpoint, but also because where the federal government is headed and where DEA is, it just may be, in the long term, untenable to think that you can't go there. But, number one, we need a near term...we need to make sure that this is resolved for the near term, because Stage 2 does require much more robust exchange, or it will if the final rule comes out looking anything like the proposed rule did. And so, there's got to be something that works in the interim. And it sounds like that there are...there certainly is a pathway that we're already headed down or that the vendors are willing to head down with some sort of minimal rules of the road, that we could get a solution in place that would work, while there's some transition going on overall, not just in healthcare, towards trusted individual level identities, that could be used in multiple places...ideally for multiple reasons. It's a much more scalable option in the long term.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And I think Dixie, to your point about Farzad's notion that things are not good enough today, I mean, I think we would want to say what the minimums are for today, which hopefully would address many of the shared password problems that I think he was referring to, you know, where the password is doctor doctor or something like that.

Deven McGraw – Center for Democracy & Technology – Director

Or a, b, c, d, e, f, g.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

I think he was more referring to the fact that when people do, we all know this, when people do have to have multiple passwords, they write them down.

Deven McGraw – Center for Democracy & Technology – Director

They write them down or they just use the same one.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Or, yeah. There are just so many...yeah.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And, most large institutions that we work at have a single sign on service, so there is only one password for all of the systems at that institution. Now if the doctor practices...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Even more important that that first authentication is strong.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And they can...they typically are. I mean, usually, in our case, it's actually two-factor, it's a security card plus a PIN. So, I don't think we're...well run implementations are in pretty good shape, as Judy suggested. We don't hear about a lot of problems.

Deven McGraw – Center for Democracy & Technology – Director

We don't, but on the other hand, we want to make sure that this is sort of network wide trust, right. So, what are...

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

That's a harder barrier, yes.

Deven McGraw – Center for Democracy & Technology – Director

...but, what are those best practices that maybe we ought to highlight as being sort of again, this sort of lightweight set of identity and authentication rules of the road that would be sort of the benchmark, that would be imposed by either a central organization or maybe through the NwHIN accreditation process.

Judy Faulkner – EPIC Systems – Founder

Deven, as you're asking...

Leslie Francis – National Committee on Vital and Health Statistics

So, this is Leslie. Just to chime in to say that also, what's been worked out now has been worked out among the more sophisticated players.

Deven McGraw – Center for Democracy & Technology – Director

Well right, although I think that the less sophisticated players, I mean again, if we specify what those practices are, then ideally everyone, everybody can play.

Leslie Francis – National Committee on Vital and Health Statistics

Right. No, that's right. But...

Deven McGraw – Center for Democracy & Technology – Director

Let me let Leslie finish Judy, and then...

Judy Faulkner – EPIC Systems – Founder

I'm sorry, yes.

Leslie Francis – National Committee on Vital and Health Statistics

The fact that it's worked with more sophisticated players, doesn't necessarily say we shouldn't attain to having quite high levels for less sophisticated...

Deven McGraw – Center for Democracy & Technology – Director

So Judy, what...

Judy Faulkner – EPIC Systems – Founder

Oh, you had talked about rules of the road earlier and I think we're talking about them at two levels; one is technically and the other is what do they sign. I didn't know whether earlier when you were asking about rules of the road you were asking me about what the rules are that they sign for, I could read them to you if you want.

Deven McGraw – Center for Democracy & Technology – Director

Oh, the ones that you use?

Judy Faulkner – EPIC Systems – Founder

Yeah.

Deven McGraw – Center for Democracy & Technology – Director

I would definitely be interested in hearing that, in part because of Leslie's comment, like it's either something that we're going impose across the board, I think we ought to know what they are, either that or we could, give direction to ONC to work with vendors to establish those policies. But, I like the idea, if we have time, of being as specific as we can be in recommendations. Does that...Leslie, because then I think you do pick up...you do address, Leslie, what I think I heard you say, which is that there ought to be a standard that is achievable by the smaller players, but also sets the bar at the level that we want for everyone.

Leslie Francis – National Committee on Vital and Health Statistics

Exactly. But, my worry is that the players who are playing now, have lots of experiences here. So, they have lots of controls in place, and what you see might be the tip of the iceberg in terms of what they're actually using for identity proofing and authorization, because they're using all sorts of other things, too.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Is your concern that the standards in use by less sophisticated players are not adequate, am I following?

Leslie Francis – National Committee on Vital and Health Statistics

No, no. My question is that, I'm probably not putting it exactly right, but my question is that the folks that you all have been talking about, the exchanges that exist now, are folks who have a pretty good reason to have a high level of trust in one another from the get go. Because they know that each of them is a well-run organization. And, so, even if they have level 2 for identity proofing and authorization, they have good reason to think all that is done extremely carefully. But then if you move over into a different organization, where we don't know that there's all that level of background good administrative practices, unless you have really quite a high level, it's more concerning to me.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

So Leslie, this is Joy. So are you talking about you're concerned about smaller practices where they might hire the kid down the street to do their...

Leslie Francis – National Committee on Vital and Health Statistics

Sure.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Okay.

Leslie Francis – National Committee on Vital and Health Statistics

I mean, that's all a question about who really gets authorized.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, and remember that access is a function of authorization, not authentication.

Leslie Francis – National Committee on Vital and Health Statistics

Exactly. We're talking about authentication, but it keeps bleeding back and forth.

Deven McGraw – Center for Democracy & Technology – Director

I know, but again, we should continue to try not to do that, because all we're trying to do is set the policies for knowing that we know who's on the other side of the door.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Right.

Deven McGraw – Center for Democracy & Technology – Director

That's it.

Leslie Francis – National Committee on Vital and Health Statistics

Right, and what I'm saying actually is that the policies at good places might be able to be less, ironically, because they've got great background backup.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

But, it's a different...

Joy Pritts – Office of the National Coordinator for Health Information Technology – Chief Privacy Officer

Can I help here? I think...

Leslie Francis – National Committee on Vital and Health Statistics

Yes.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Leslie, I think Leslie is focusing on the ID proofing aspect here, I think.

Leslie Francis – National Committee on Vital and Health Statistics

Sure...

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

And I think what she is saying is that it's one thing when you're dealing with a sophisticated hospital or organizations that...some of the established HIE organizations, because they're major businesses and their sophisticated. She's concerned about all the new entrants who are not sophisticated, and may not have all of these practices policies in place that would boost the potential level 2 to something that's really quite a bit higher.

Leslie Francis – National Committee on Vital and Health Statistics

Thank you.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And are you worried about potential attacks on the system, in other words, somebody masquerading as Dr. Smith when in fact they're the neighbor kid who's a hacker?

Leslie Francis – National Committee on Vital and Health Statistics

Sure.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

And a damn good physician too.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, maybe, maybe better than some (laughter).

Deven McGraw – Center for Democracy & Technology – Director

The neighbor kid?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

So that is true...that's an authentication...you're worried about spoofing, the risk of spoofing from less sophisticated organizations that aren't really watching carefully.

Leslie Francis – National Committee on Vital and Health Statistics

No, I'm worried about concerns that they could get hacked and this could go over.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

But the risk of failed authentication is someone is masquerading as someone else.

Leslie Francis – National Committee on Vital and Health Statistics

Right. Right, I understand that.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

That's a real risk that every system has to worry about, and it obviously is...increases as you allow connectivity from the outside.

Leslie Francis – National Committee on Vital and Health Statistics

Sure. But, for example, as sophisticated system that has a single sign-on, is going to have very strong password control, typically for that sign-on, for the robust...you know, the robust...password. Some of the other systems may not.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, but Leslie, I'm struggling with where your points drive us from a policy recommendation...

Leslie Francis – National Committee on Vital and Health Statistics

I meant them to drive us to say, you can't rely on the experience of the currently existing networks to say we could just get by with username and password, because it's been working there.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, and I think the...no, excuse me, never mind. I think that one of the things that we touched on in our previous recommendations was trying to make a distinction about internal access and remote access and, it makes sense that if we were to craft a roadmap, that we have different twin lanes, if you would, for those two use cases. And I agree that for remote access, where you are essentially trusting that the remote system has done appropriate proofing of identity, which is different than trusting that your own system has done proofing of identity. Because in the case of your own system, you know what is being done; in the remote system, you don't know what's being done. That we would have different levels on our roadmap for those two uses...

Leslie Francis – National Committee on Vital and Health Statistics

Yeah, that's another way to make the same point. I was concerned that there was a slip-back to letting the organizations do it as they do it internally.

Deven McGraw – Center for Democracy & Technology – Director

Right. Well, I think we do want...we have always, at least historically said, that it is the sort of remote access, you know, the ability to access data from an entity that's not part of your internal system or your integrated delivery network with entities that are related to one another or that know each other. But, given that the experience of the vendors that we have on the call, isn't trying to connect disparate systems. What additional requirements are we looking for there?

Judy Faulkner – EPIC Systems – Founder

This is Judy; I can explain a little bit, is that okay?

Deven McGraw – Center for Democracy & Technology – Director

Yeah, oh, absolutely.

Judy Faulkner – EPIC Systems – Founder

Okay, one of our first rules of the road is, by making a request for patient's information, you want to represent that you are making a request for the patient's information, you are providing treatment to that patient...

Deven McGraw – Center for Democracy & Technology – Director

Right, although that's really more to the authorization standpoint.

Judy Faulkner – EPIC Systems – Founder

Right. And then the thing is though, that they do go hand-in-hand together. Because when you do that, the system itself can be checking, is this the patient, you just can't go fishing. I think those two together are important.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

But, Leslie's worried that someone who is willfully trying to hack a system has no qualms about asserting that they're caring for the patient, if, in fact their goal is to steal data. So...

Judy Faulkner – EPIC Systems – Founder

Yeah, but that patient better be coming in, because what the system can and should be doing, is checking that there is a bona fide scheduled appointment, the patient is in the ED, the patient is an inpatient, etcetera.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, those are good safeguards...

Judy Faulkner – EPIC Systems – Founder

Exactly.

Deven McGraw – Center for Democracy & Technology – Director

But how's the remote location going to be able to check that?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Right. And it wouldn't be caught by...it wouldn't catch impersonation by someone who is knowledgeable about the patient's activity, like a family member or something.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

So with the remote authentication, to reiterate prior discussions, I thought that the concern was somebody has their health information on the cell phone or has access through the cell phone or a laptop or something, and they lose it, and you just have a...the only way of authenticating is to password it, but that might not be secure. And I thought that's why you were looking at a higher degree of authentication for those kinds of remote access.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, they think the thought is a higher-level minimum standard that we would specify as opposed to just endorsing current practice.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yeah.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Judy Faulkner – EPIC Systems – Founder

Right.

Deven McGraw – Center for Democracy & Technology – Director

Right, and I would think Joy, the other thing that's in play, at least for me, is that you can't count on sort of other...of trust, whether they're directly related to identity or authentication or not, to sort of bolster the...your comfort level with knowing that the person is who they are. So, if it's certainly within your own entity, there's really a kind of a penumbra of policies as well as an ability to sort of know exactly which computer the query is being initiated from. Like, in the same way that when I use my bank with the computer that I always access my bank records from, it's quite comfortable with flashing me right through with a password and if I happen to log on from another computer, they're going to ask me all kinds of other knowledge questions to get me in, right.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yeah.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, questions either about you or maybe your mother, like in my case.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

What's a penumbra?

Deven McGraw – Center for Democracy & Technology – Director

Penumbra?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

That was a great word.

Deven McGraw – Center for Democracy & Technology – Director

It's a nice legal word that I pulled out of my...you ought to know John.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

I don't, I'm too simple for those things.

Deven McGraw – Center for Democracy & Technology – Director

A collection of indicators, right, collection of policies that kind of together create...

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

A plethora of policies. It's a plethora of policies.

Deven McGraw – Center for Democracy & Technology – Director

Plethora, right.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

I'm a man of simple words.

Deven McGraw – Center for Democracy & Technology – Director

It's an odd place for me to be using that term, that's for sure. All right, well we are creeping to the end of our ninety minutes and I thought we were making some progress. But then it seemed like we started to circle the same set of questions that vexed us from the very beginning, beyond some forward-looking statements about getting to individual level credentials at level 3 by sometime in the future, consistent with where industry appears to be going, but keeping an eye on where...how trusted exchange is occurring using methodologies that we customarily use along the way, to keep from wholesale disrupting things. I still feel like we've got some work to do to sort of figure out the remote questions that we tried to land on before, but didn't really get terribly specific. And also setting what the rules of the road might look like, I think more from a policy standpoint, trying to focus on identity and authentication and not authorization to the extent we can, and then if we think there are technical issues to resolve, obviously that's...I think we would give direction to the Standards Committee to develop that. Or perhaps the S&I framework, I don't know, we can get to that. But, I feel like there are some places where we circled around, but still ideally would need to drill down farther. And I...is that sort of what our folks think we generally are? Of course, it would be far better if you were to see some sort of summary recommendations that you could pick at, which we will do. But where else do folks think we still need to do some drill-down, and what questions would you ideally want to have answered in the interim, between now and our next call.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

All of the above.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Well, I can offer that I'm supposed to...that's probably not appropriate. I'm going to be presenting to the Standards Committee some observations from the hearing last week, and I'd be happy to summarize any feedback we get just during that discussion, might be of value.

W

Yeah, of course.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

I wonder if it's worth just coming back to the notion of if we know where our endgame is, that we really then have two variables. One is when do we get the endgame and two, how do we get there on each of these paths that we think may deserve appropriately different treatment, local access versus remote access, push versus pull and so forth. Is it worth, without specifying exactly the dates, could we just try to say what are the cells in the spreadsheet if you would, that end up with level 3 assurance in individual certificates...into individual credentials I should say, not certificates.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

That goes back to my comment at the end of the meeting about use cases and where do we find the overlap of...

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah. What are the broad use cases and what are the steps.

W

Yup.

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

And where do certain things apply such as level 3 more or less.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Right. I mean, I think we could take a whack at just the spreadsheet without filling in any content, and then sort of step back and say, now, do we think there's enough differentiation between these cells to say, this is a meaningful step up that we would expect could be associated with level 3...or Stage 3 of Meaningful Use, which is really the only lever arm that we as a workgroup have, I believe.

Deven McGraw – Center for Democracy & Technology – Director

Yeah. I think that's a really...I think that's a great idea...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Me too.

Deven McGraw – Center for Democracy & Technology – Director

And it's actually, it's sort of where, when I was first pulling some thoughts together about this, was sort of where my head was, which is that, certainly internal transactions we'd have to define what that was, and push transactions where the two endpoints are known, and you just want to make sure you're sending it to the right address. Like, those seem like much simpler use cases to resolve, not simple, but simpler, versus when you're talking about query and response where somebody's reaching out to get data, it maybe raises up some other concerns. I'm absolutely amenable to sort of parsing it that way, and any suggestions that folks may want to give me for what that matrix or grid would look like, broadly, and then we might be able to fill it in. I think it seems like a great way to proceed.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

When would level 3...Stage 3 start, according to the current...

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

2014...no, that's not...

Deven McGraw – Center for Democracy & Technology – Director

No, 2014 is when Stage 2 starts, earliest, so, we're talking about 16 I think, but we can check. I feel like I've seen that chart a million times, but apparently I still haven't memorized it.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, I haven't memorized it either.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

I know it started out 16, but you know, they've kind of dabbled with the dates.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

It's still...it's pretty far out is what my point kind of was going to be, that there's...if we said, here are some targets that should be achieved by the start of Stage 3 for the earliest adopters, and that's 2016, that's a pretty long runway.

Deven McGraw – Center for Democracy & Technology – Director

Yeah.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Particularly since I suspect that many of the organizations are already there.

Deven McGraw – Center for Democracy & Technology – Director

Right.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

And we'd be getting this parallel push from the NSTIC at the same time, too.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

And from the DEA.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

And from the DEA, yup.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Maybe in our use case list, the DEA use case should be there just so we have it as reference.

Deven McGraw – Center for Democracy & Technology – Director

Right, agreed.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Because the doctors that prescribe are going to be following that one, whether we like it or not.

Deven McGraw – Center for Democracy & Technology – Director

Well, exactly.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

It sure would have been nice to have a DEA testimony to talk about where they are.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Yeah, that would have been good.

Joy Pritts – Office of the National Coordinator – Chief Privacy Officer

Yeah, it sure would have been.

Deven McGraw – Center for Democracy & Technology – Director

All right folks. We really do need to move into public comment. So certainly send additional thoughts, please, by email, but in the meantime, I'll work with the folks from MITRE and ONC to try to pull together a draft chart. What did you refer to it as David, I liked your term?

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Oh, I said...I think I said the word roadmap at one point, but also I was just talking about spreadsheet.

Deven McGraw – Center for Democracy & Technology – Director

Spreadsheet, yes, spreadsheet, matrix...

John Houston – University of Pittsburgh Medical Center; National Committee on Vital & Health Statistics

That's a viable term.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Maybe swim lanes, use cases and swim lanes or...all these various things that allow you to gridify something.

Deven McGraw – Center for Democracy & Technology – Director

I'll be working on that on my end, so, send suggestions. But, I'll give you something to react to this week.

David McCallie, Jr. – Cerner Corporation – Vice President of Medical Informatics

Good.

Deven McGraw – Center for Democracy & Technology – Director

All right, MacKenzie, you want to open up the lines since I'm late.

MacKenzie Robertson – Office of the National Coordinator

Sure. Operator, could you please open the lines for public comment?

Public Comment

Caitlin Collins – Altarum Institute

Yes. If you are on the phone and would like to make a public comment please press *1 at this time. 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. I have a public comment.

Operator

Steve Kirsch, your line is live.

Steve Kirsch – OneID – Founder and Chief Technology Officer

Oh hi. A couple of things. I was on the phone with the President of CertiPath this morning and they're doing some very interesting work that will happen over the next probably sixty days or so, with respect to 800-63-1 and certification and providing alternatives to the current methods, so that might be of interest to people. The second thing is, I was at the hearing on the 11th, and spoke there, and I had suggested that the government had to issue some sort of identifier, and I'd like to modify that. Because, it's perhaps a better solution, is to have identifiers that are provisioned by identity providers that are accredited, and then a physician, for example, can then take that identity, a unique number that's provided by that identity provider, and then have a set of self-asserted attributes that met standards. Such as the standards that Accenture is using for biometrics in India, because they're handling the provisioning of billions of people in India and they've already gone through the work of setting up what those biometric standards are. And so, as far as identity-proofing for this particular effort, you might want to consider what is sufficient in terms of in-person biometrics, for instance, is face sufficient, is fingerprint sufficient, do you need iris as well; sort of, what level is acceptable. Or are any of those acceptable?

And then finally, probably establishing some vision for what you want to have the system look like at the end. Because I think there are some vendors who can do this now; you know, for example, my company is one of them, but I'm sure there are other vendors as well. And that if you had some standards and visions and say hey, it's going to be this universally usable identity that's not just what's in the hospital; that it has to support two-factor remote authentication and authorization, that it has to be an identity provider that can't have a possibility of a mass breach like LinkedIn recently did, that allows people to treat and identifier, but then have self-asserted attributes so you can go to anywhere to have your fingerprints scanned, as long as they meet the standards, for example. And then you can use that identifier and then verify your fingerprints. And that would be a pretty practical way to do it that would open it up to lots of players and kind of solve the conundrum that you're in right now. And then all you have to do, really, is specify what attributes are sufficient for level 3 and level 4, and then you're done, you can let the market take it from there. So, those are my suggestions.

Deven McGraw – Center for Democracy & Technology – Director

Thanks a lot Steve we appreciate your feedback. Do we have any more comments?

Operator

No more public comments.

Deven McGraw – Center for Democracy & Technology – Director

For a minute, I thought I was the only one left on the line. All right, thanks everybody for your time today. Keep an eye on your email; send me some if you want to put your thoughts down on virtual paper.

Dixie Baker – Science Applications International Corporation – CTO, Health & Life Sciences

Thanks.

MacKenzie Robertson – Office of the National Coordinator

Thanks everyone.