

Privacy & Security Tiger Team
Draft Transcript
June 18, 2012

Presentation

Operator

All lines are bridged Ms. Robertson.

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 to 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 Egeman?

Deven McGraw – Center for Democracy & Technology – Director

Yeah, he told me he wasn't sure if he would be able to join us today.

MacKenzie Robertson – Office of the National Coordinator

Okay. 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? Carol Diamond? Judy Faulkner? Leslie Francis? Gayle Harrell? I know you're on, Gayle. 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? Might be on mute. Wes Rishel? Micky Tripathi? Latanya Sweeney? Is there any staff on the line?

Gayle Harrell – Florida House of Representatives

Gayle Harrell's on board, I got disconnected for a minute; I'm back.

MacKenzie Robertson – Office of the National Coordinator

Okay, thanks Gayle.

Kathryn Marchesini – Office of the National Coordinator

Kathryn Marchesini from ONC.

MacKenzie Robertson – Office of the National Coordinator

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

Deven McGraw – Center for Democracy & Technology – Director

All right, terrific, thank you very much. We did have our Policy Committee meeting on the NwHIN Governance Request for Information where we had discussion of our Tiger Team recommendations on the topics that we were able to cover and also the Governance working group and the Information Exchange working group weighed in. And it was a pretty long meeting and I've actually, much of what we had said in the way of recommendations was adopted by the full committee and sent along. The most amount of conversation that we related to the issue of the condition that precludes the use or sale of de-identified data for commercial purposes, not surprisingly. It was a very robust debate that did not actually reach consensus, sort of like our own debate on the topic. What's going to be sent to ONC is the set of concerns that were ... that the Policy Committee and its working groups had surfaced and it will ultimately be up to ONC to sort of make the decision about where they want to head for the proposed rule, and we'll have another opportunity to comment on that.

As well, I think the only place where the Policy Committee may have differed from where the Tiger Team came out was on the issue of patients' ability to access and seek amendments to unique data from an NVE, a Nationwide Health Information Network validated entity. The Policy Committee was more inclined to be supportive of the CTE, but understood the concerns that had been surfaced in our Tiger Team meeting; but I actually do want to take a look at the transcript and the write up of that meeting, because we covered so much and Gayle, you might agree with me on this, we covered so much that it's actually, I'm not 100% certain of where we exactly landed on some of these recommendations. It will be good to have an opportunity to take a look at the write up, when it's ready.

Gayle Harrell – Florida House of Representatives

I would totally agree with you Deven and I look forward to reading that myself and maybe the two of us or those of us who are on both entities could comment back on it.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, well, if there's ... I mean, I think we don't have an opportunity to do so from a Tiger Team perspective because as you'll see in a few minutes, we've been asked to move on to another important issue. But certainly I think it's important, for all the work that we put in, to putting some recommendations in front of the Policy Committee that everyone at least gets a sense of where the Committee landed. And again, particularly in this instance where it's a request for information rather than an actual rule making, we very well may get another bite at this apple. So..

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

Deven, it's David McCallie, I just wanted to let you know I joined late, I was muted when I first dialed in so, I redialed.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Thank you. Anybody else want to acknowledge that they're on, that might have missed roll call?

Joy Pritts – Office of the National Coordinator

Joy's on.

Deven McGraw – Center for Democracy & Technology – Director

Okay, great. All right, terrific. So what we have to do today is to take a look at a new question, can I have the next slide... oh, I do have control, here we go, to talk about a new charge for the Tiger Team. And it's not a redo of our entire charge, because our charge is pretty broad, but it is a particular task that we've been asked to look into, actually jointly with the Privacy and Security working group of the Health IT Standards Committee. And so, what we're going to do for the first couple of minutes of this call is to kind of lay some groundwork in terms of what the Tiger Team and the Policy Committee have recommended in the past that's related to this issue. And then we're going to be turning it over to folks to talk about in more detail what's been going on with the National Strategy for Trusted Identity in Cyberspace. So specifically we have been asked to consider identity management and perhaps how the National Strategy for Trusted Identities in Cyberspace, which is commonly referred to as NSTIC, can be leveraged to better enable physician authentication, particularly for communications and sharing of data across a network.

And we've made some recommendations before on this issue of provider authentication and, in fact, we resurfaced some of them as part of our responses to the RFI. But the ONC has asked us to take another look because the environment has changed a bit since we first took up this issue and there have been some developments again that might be able to be leveraged in a way that will enable us to make further progress on this. And we did, in fact, leave room in previous recommendations, to reassess our policy for consistency with NSTIC as it develops. And again, a big part of the call that we're having today is to have a presentation on NSTIC so all of you to have a baseline understanding of what it is and how it might be quite relevant to physician authentication questions.

Patient consumer authentication, such as will certainly be necessary to enable patients to access data through portals, but also if the vision is for more active patient sharing of data with providers in the future, certainly identity proofing and authentication of the patient is also pretty critical, so, we are not at all ignoring that aspect, but you have to find something to focus on first, and we are going to focus first on providers. And my hope is that some of what recommendations that we come up with for providers, may be leveraged, at least to some extent, in what might be applicable to patients as well. So again, today we have a briefing by Jeremy Grant and another member of his staff. And then on July 11th, we're going to have a joint, in-person, public hearing, again co-chaired with Dixie and the other members of her, it should be the HITSC, it's the HITSC's Privacy and Security Workgroup to talk about again, sort of what are the challenges of physician identity in a clinical setting, particularly when you are talking about access across a network, but not necessarily limited to that particular use case. What is the current status of NSTIC, how might it be applicable in this setting and we'll definitely be hearing from...looking to hear from folks in the private sector as well as the Federal Government, about how they've been trying to address this question; all with the goal of coming up with some recommendations to our respective Federal Advisory Committees.

We will do the hearing jointly. And I'm also hoping that the hearing gives us a little bit of time to have some initial discussions together as a group about what some of the issues are that are appropriate to be tackled by the Policy Committee versus those that are appropriate to be tackled by the Standards Committee. But our deliberations on recommendations will not be done jointly, but will instead be done within our respective working groups, reporting up to our respective Federal Advisory Bodies. But we always try, at least in our workgroup, I think we've done a reasonably good job at it, to try to remain as in sync as possible, at least not putting conflicting recommendations up through the chain and we are able to do that, in part, because we have so many joint members. Our Tiger Team has a number of members from the Standards Privacy and Security working group on it.

And on this slide here is just a timeline of how we're going to get through this. We need to finalize our recommendations for the Health IT Policy Committee meeting that's on the very first day of August. So, we're really going to work to get through this in July. We have canceled out pre-scheduled meeting for July 2nd, because it's a bad day, coming a couple of days before a Federal Holiday, and also we are scheduling the joint hearing for July 11th, which is the day after the Health IT Policy Committee meeting that takes place in July. We're looking at a half day, there's a time on your slide of 9 a.m. to 1 p.m., but we're going to need to extend that a little bit, but, we're still hoping to end it at a time when folks can catch ... we're talking about only another hour or 90 minutes. We just had a discussion earlier today, suggesting that we would need a little bit more time for this hearing, but nevertheless, it will not be longer than a typical Policy Committee meeting, as the folks can use the time to return home if you are travelling. Then we already have a Tiger Team call scheduled for July 16th, it's an hour and a half call, for us to work on recommendations. We don't have another meeting scheduled on the calendar already before August 1, but we're trying to get one on there, because I just have a feeling that 90 minutes for one call is probably not going to be enough for us to get through what we need to get through.

So, stay tuned for some further information on scheduling another meeting in July and then hopefully we'll have a little bit of breathing space in August, after that meeting. Does anybody have any questions about the schedule before I just have a few slides to go through again to remind us what were and where our previous stumbling blocks were in developing policies around provider authentication, particularly for access to patient data through NwHIN and then we're going to turn it over to the folks from the Commerce Department, who are going to lead us through a bigger ... a more in-depth explanation of what NSTIC actually is. Does anybody have any questions? All right, terrific.

So, I'm on slide 5, just again, a reminder of what we have previously said. Organizations that are seeking to exchange information as part of NwHIN, should be required to adopt baseline user authentication policies that require more than just the basic level of user name and password, when access is remote. We said at least two factors should be required in the context of remote access, which we defined, at least for the purposes of our initial recommendations, as access over a public network like the internet. And so, just to remind folks of our rationale and also some of the things that we struggled over in this recommendation.

We were not comfortable with recommending application of say NIST level 3 or the DEA requirements for EHR user authentication, even for remote access, because of the stringency of the second factor requirement was mostly what was holding us back there; in terms of reaching consensus. I think there were some who were perfectly fine with heading in that direction, but others who were not. We were particularly concerned about remote access versus access within an entities private, secure network, but we had a little bit of trouble defining what constituted remote access, beyond agreeing that certainly if it's an internet-like access, that would be remote. The other thing we said is that the Standards Committee should also be providing recommendations on appropriate factors for that second factor beyond the user name and password.

Moving on to slide 7 -- again we acknowledged that what we were trying to do was set a baseline, but certainly more stringent requirements could be adopted. Although that's something that we also might want to be thinking about, given that we're trying to facilitate access across a network and varying authentication policies used by different organizations might, in fact, make is a bit of a struggle to enable more streamlined access; again assuming the access is for the appropriate purpose. But, I'm throwing that out there, we have time to think about that as part of a number of things that we should be thinking about in terms of fleshing out these recommendations more. Further, we also did say that for more sensitive, higher risk transactions, an additional level of authentication of even greater strength, after the initial level of authentication, might be required as really is already recognized by the DEA policy regarding e-prescribing of controlled substances. And that we might have to do some additional work to identify use cases that might require greater authentication above the baseline. But, we didn't really have a lot of time to flesh out what that would look like. So, that's another area where we might be able to have some additional conversation during this month and July.

And then we finally said that these policies should ... NwHIN policies regarding authentication should be reassessed for consistency with other national identification efforts and technology developments such as NSTIC. We wanted to make sure that we continued to leverage innovation in this space and that's one of the reasons for the hearing. So, with that ... oh, no, there was more. We're always about as comprehensive as we can be with the information we have at the time. We also encouraged ONC to be developing and disseminating evidence about the efficacy of various authentication policies and then reassess the policies for NwHIN accordingly. Then of course, the last thing that we did say was that for writing of e-prescriptions for controlled substances; certainly, the certified EHR should have the capability to do the two factor authentication. And this is actually a topic that we reassessed as part of our Stage 2 meaningful use and certification recommendations, if you'll recall. So, all right, with that ... does anybody have any questions before we launch into the next phase of this?

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

Deven, I do. This is Dixie.

Deven McGraw – Center for Democracy & Technology – Director

Okay, go right ahead.

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

I should have brought this up earlier, actually, but it just occurred to me to ask it. What will be the end product here, will it be a Tiger Team recommendation, is it to fit in with the meaningful use, or is it just something, a recommended guidance that we sent to ONC, what's the ultimate product, if you will, that we're thinking about.

Deven McGraw – Center for Democracy & Technology – Director

Well, I'll let the folks from ONC chime in, if I'm not getting this right. But my understanding is that, consistent with our previous recommendations that urged ONC to keep track of developments on NSTIC and leverage it to the extent possible for policy on physician credentialing across the network. There have been some developments and a strong desire on the part of both ONC and the Department of Commerce to use NSTIC to develop some more detail about policies for physician credentialing across the network, that ultimately are going to be most useful probably for policy related to NwHIN. But, Joy and Kristen, do you want to add anything to that? We have Kristen Ratcliff who's also from ONC who has been...who works with Dr. Mostashari, who's been doing a lot of work on helping us pull this hearing together. Is there anything you all want to add to that necessarily?

Joy Pritts – Office of the National Coordinator

No Deven, I think that you're right, this is being thought of in a probably beyond guidance in a larger policy context.

Deven McGraw – Center for Democracy & Technology – Director

Okay.

Kristen Ratcliff – Office of the National Coordinator

Deven, I agree.

Deven McGraw – Center for Democracy & Technology – Director

So, in many respects it's ... we're trying to make the hearing as sort of getting us as much information on sort of where NSTIC is to date, what the issues are from the physicians side, where the private sector might have some good answers that are consistent with NSTIC, to develop a...to inform our recommendations. It kind of allows us really to go back and look at what we've done before and given that we're trying to create a space where there is trust across a network versus just with respect to accessing data within your own institution or your own physician practice, to see whether there's more that we can say. And I suspect that there will be, but it's kind of hard to know the parameters of what that will be until we get through the hearing. Does that make sense?

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

Yes it does, actually.

Deven McGraw – Center for Democracy & Technology – Director

Okay. Good. Anybody else have a question? All right, then I am going to turn it over to Jeremy Grant and his colleague, Naomi Lefkowitz, to talk us through some slides on NSTIC.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Right, thanks, and we really appreciate the invitation to address the Tiger Team today. This is Jeremy, obviously, Naomi is sitting here with me. Can everybody hear me okay, I'm on speakerphone but I can pick up if need be.

Deven McGraw – Center for Democracy & Technology – Director

I can hear you just fine. Everybody's fine.

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

Fine, yeah.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

If there are any sound quality issues, we have very thin windows in the Commerce Department basement, 14th Street, so when trucks go by or what not, if it gets noisy just give a holler and we'll pick up the earpiece. Really appreciate the invitation. Just a little bit of background. I think the work of the Tiger Team was well under way when President Obama signed the National Strategy for Trusted Identities in Cyberspace, just a little over a year ago, last April. I've told the story a few times, some of you may have heard, it was my second day of work when I got an email from Aneesh Chopra that was addressed to me and Farzad, that basically introduced the two of us to each other and basically pointed out Farzad...as you know, it can be very hard to achieve many of the benefits of Health IT without actually adequately addressing the identification and authentication conundrum, introduced me talking about a new White House strategy that was focused on crafting the solution for the country, in partnership with the private sector, and basically pointed out it would be really silly if what we did in Health IT didn't align with the National strategy and asked if we'd be kind enough to work together. And we have been actually for well over a year now, both the two of us and our teams have been collaborating and looking for areas where we can help them, and likewise, where we can learn from a lot of the work that's been going on within the Health IT space. So I wanted to talk a little bit more about the strategy and what we've been up to today, and I think we should also have plenty of time for questions.

Next slide. Three objectives to hit; one, obviously we just wanted to be able to have everybody have a chance to learn today about NSTIC. Second, to discuss how it is that a government led initiative can help to improve online trust, to reduce fraud and to create new efficiencies in health care and then third, I think to discuss the role both the organizations that you represent as well as each of you as a Tiger Team member, can play in advancing the use of trusted identities in cyberspace, as well as the ways that it can help IT realize some of its potential.

On the next slide I just wanted to give a high level overview of NSTIC, how this strategy actually came about. Some background, it was originally called for in President Obama's cyberspace policy review that was published in May, 2009, where there were ten near term action items that were called for in the strategy. The tenth was the creation of a cybersecurity focused identity management vision and strategy that looked not just at the intersection between cybersecurity and identity, because that's something I think a lot of people focus on quite a bit, but that would also make sure to address privacy and civil liberties interests and look for ways to leverage privacy enhancing technologies for the nation. From that, a White House team that had participation from a lot of different agencies, was stood up to start actually drafting that strategy. A draft was released in the summer of 2010 for comment; a lot of different private sector stakeholders and public had a chance to provide comment and then the draft was further refined until it was finally signed by the President in April of 2011 at a big event hosted by the U.S. Chamber of Commerce.

At its core NSTIC calls for the creation of an identity ecosystem, essentially an online environment where individuals and organizations will be able to better trust each other because they're following agreed upon standards to obtain and authenticate their digital identities. What this means at its core is NSTIC is really trying to catalyze a marketplace where each of us will be able to choose from really a variety of different accredited credentials that are out there that we can use everywhere that we go online. And there are four guiding principles that are pervasive throughout the strategy which is that the solutions that emerge in the marketplace that we all use must be privacy-enhancing and voluntary, they must be secure and resilient, they must be interoperable and they have to be cost-effective and easy to use. There are really three problems that NSTIC is trying to solve, and if you slide to the next slide, I'll start to talk to those.

The first is that user names and passwords are fundamentally broken. I think most of us today are managing twenty-five or thirty different passwords, each with an increasing array of requirements. I know certainly here at NIST we're being asked to support 12 characters, letters, numbers, upper case and lower case including some symbols, but in some apps you can use one symbol and not another and in another app it's completely opposite. The reality is that most of us, or most Americans in general, I think, are using the same one or two passwords over and over again. In fact, if you start to talk to a lot of security experts in the space, they think anecdotally about 40% of people have a single password that they use for all of their email accounts and every place else they go. Furthermore, we found that even if you're using these strong 12 character passwords, they're quite vulnerable. The criminals and the bad guys have a lot of paths to easily capture the passwords that with password reuse, tend to be considered the key to the kingdom to get different elements of data and take over accounts, whether it's brute force attacks to crack a password, or fishing attacks which are a great way to go around even the strongest password, the ability to easily inject malware into computers that can put say key log-in software on. There's really not much utilities the password offers anymore, aside from a lot of inconvenience and a lot of insecurity.

With this we've seen rising cost of identity theft and data-breaches; there was an estimated 11.6 million US victims last year, were victims of identity theft at 13% up year over year, at a cost of 37 billion dollars. Javelin estimate, there was a 67% increase in the number of Americans impacted by data breaches last year and according to a separate report from Symantec, the health sector is the number one target, 43% of all US data breaches in 2011 were concentrated in the health sector. So clearly there are some problems today. And in attack after attack, when people come in and do the analysis of how they actually executed the attack, almost all the high profile ones in one way or another have been tied to passwords.

In fact, if you look at the next slide, it talks about...it quotes from a study that the US Secret Service does every year, in partnership with Verizon and several other law enforcement agencies around the world, and it looks at the top vectors of attack that were used in data breaches in 2011. It's a pretty stunning number. In 2010, passwords were certainly used quite a bit, but it was 4 of the top 10 vectors of attack. In 2011, 5 of the top 6 attack vectors were tied with passwords and 7 of the top 10, in fact, you can sort of go through the list and see just how prevalent our reliance on passwords was, as a method of breaking into different systems and the numbers that are circled on the right, the 35%, the 82% show what percentage of the records were actually tied to that particular method of attack. So, we have a lot of different statistics that show why passwords aren't exactly the most elegant or secure system for us to be using to secure any information these days. We'll talk shortly about what we're doing to get around that and improve upon that.

The second issue we're trying to deal with, if you move to the next slide, is we're coming up in a couple of weeks on 19 years since the New Yorker published their famous cartoon where the dog on the computer talks to its friend the dog and says, "The great thing about the Internet is nobody knows you're a dog." And while the cartoon has evolved a couple of times, here's the blog version, which you can see, where the dog says to his friend the dog, for those of you who don't have the benefit of PowerPoint, "I had my own blog for a while, but then decided to go back to just pointless, incessant barking." And the next was the Facebook version where the dog says to his friend the dog, we can advance one more click, yes, "On Facebook 273 people know I'm a dog, the rest can only see my limited profile." So while the dog cartoon has actually evolved a couple of times, the basic issue with dogs on the internet is still the same today. Now we always try to point out, I particularly do when Naomi who's our Senior Privacy Advisor is sitting next to me.

The government does not have any problems with dogs on the internet, in fact, the ability to be anonymous or operate under a pseudonym online for a lot of applications is something not only that we don't think is a problem, but that everybody would acknowledge, and we certainly do, has actually helped to make the internet the vibrant place that it is today for discussion, for free association, for expression of different ideas. The flip side is there's a lot of very interesting transaction that we would like to conduct online, both in the private sector as well as in the public sector, where the risk model was such that they're not online today because we can't actually answer with any real authority whether somebody is a dog or not. And certainly we look at electronic health records as one of the key examples of this, where we could save billions and enable new efficiencies in care, but if we can't solve the authentication challenge for providers and individuals, it's going to be tough to actually realize the benefits. Now there are ways, as we detail in the next slide, to actually do some sort of identity proofing today. A lot of what we tend to do remotely tends to rely on a lot of smart questions, but, it's not always particularly easy and we need to find some better ways to do it.

On the next slide we really talk about the third leg of NSTIC which is privacy. As I mentioned before, the solution's be privacy enhancing and voluntary is one of the guiding principles. The NSTIC is very closely aligned with the Administration's Consumer Privacy Bill of Rights, particularly looking at ways, when we go online that we can try and change what the default behavior is, so individuals don't have to provide pages and pages of their personally identifiable information just to engage in a simple transaction. We've got an image of a driver's license and a movie ticket really to illustrate that. When I go to the movies, if I get carded, which doesn't happen much these days, but let's say it used to, it doesn't really matter what my name is, what state I live in, what my height or my weight is, in fact, they don't even need to know when my birthday is; all they need to know is a particular attribute about me, which is that I'm older than 17, and thus they can sell me a movie ticket.

But we don't really see much of that online, instead we're being asked to provide all sorts of information about ourselves, rather than those particular key attributes that are actually necessary to complete a transaction. And with it, individuals don't have a lot of means to control use of their information. Part of what we're trying to do with NSTIC is allow people to get a better handle on that and get some more attribute-based transactions rather than one that involves everything about the self. And just in case you guys haven't focused on in your group, but I'm sure you have, the amount of information that is actually out there on us. The next slide details a diagram that was actually part of the World Economic Forum's recent report on rethinking personal data and strengthening trust. This came out last month and we thought it was a pretty interesting read for a number of reasons. But this chart here, and I won't read every element on it obviously, but it talks about all the different types of data that is actually out there on us today, and actually being collected and often bought and sold and traded and swapped, whether it's information relating to our government identity, our sex, our address, different kinds of assets that we have, the digital exhaust that we leave on line in terms of whoever it is you're acting with and social networks and different ecommerce sites; different elements about our health data, discussions about who we're communicating with through different means, whether it's texting or IM or other activities that are out there.

If you start to look at all the different categories and look at the different data elements that are out there, it's a pretty stellar amount of information and it's one that continues to grow each year. A lot of what NSTIC is really trying to focus on is as this number continues to grow and in many cases people start to get concerned about just how much data is out there and their lack of control over it. How can we actually create an environment, an ecosystem as you will, where we can enable individuals to have more control over their information and essentially regain a little bit of control over that part of their lives.

So the next slide details how trusted identities can provide a foundation to address all three of these issues. We can enhance security by moving people to multifactor authentication, helping to fight cybercrime and identity theft and increase consumer confidence. We can improve privacy standards to give individuals more control over when and how data is revealed and allows them to share less information. And we think the economic benefits will be significant by enabling these types of transactions online, reducing costs for sensitive transactions and helping to improve customer experiences.

I have got to say in particular one of the areas we're getting a lot of interest from online retailers who are sort of looking at their abandonment rates right now. Think about how many times each of you might be asked to create a new account at an online site and say, "I don't even want to bother, it's just a hassle," and those rates tend to be 45-50% a lot of times. Retailers have been really excited about the notion of, what if in a few years we've created this ecosystem, this marketplace where 75% or 80% of their visitors are coming to their sites with a strong trusted credential that they know that they can trust and rely upon to frankly get people past that initial account management phase and get them right to the kinds of services that they're looking to deliver online. Likewise we think the benefit to health care could be pretty significant if in a few years, particularly on the patient's side, a significant percentage of the population has a strong credential that could then be used to provide access to a lot of different health information that should be online.

So the next slide actually lays out the long term vision of NSTIC, and I always, when we're giving these presentations, like to point out that the January 1, 2016 date is a little arbitrary and we actually think we're going to deliver some real benefits much sooner, but there will be an identity ecosystem where individuals can choose from multiple identity providers and different types of digital credentials for more convenient, secure and privacy enhanced transactions, anywhere at any time. The next slide, people often ask, well this all sounds great, but how do you know that this matters? And if people aren't convinced enough by some of the slides on passwords and data breaches that we put up earlier, it's really worth noting what other organizations have found when they basically banned use of passwords.

Defense Department led the way, about six years ago, when after issuing common access cards, these were essentially strong smartcards that had several PKI certificates on them. And frankly using them for not a whole lot. The DOD CIO put out a mandate that said, you can no longer use user name and passwords to log onto DOD networks or computers, you must use the cryptographic functions that are part of those common access cards. A remarkable thing happened when they did that, their network intrusions fell about 46% virtually overnight as all of the stolen and spoofed user name and passwords that different folks were using to get into the systems basically became worthless. That's a pretty stunning number if you've spent any time looking at cybersecurity issues, because I don't know of any program that has actually resulted in a near instant 46% reduction in attacks. Now, it's also very clear to talk about the fact that there was still that other 54%, and there is no...there really is no silver bullet when it comes to cybersecurity, and I don't want to argue that this is one here. What it did do was it forced all the bad guys and folks who were trying to get into the systems to find other ways in. But it is worth noting that as we're trying to shut down a lot of the most commonly used vectors of attack, particularly in the private sector, in the consumer space, which is where NSTIC's heavily focused. You need to really start on what are people actually using today to get into these systems and how can we increase the layers of security in order to force fraudsters and criminals and others to have to expend a lot more resources than they do today to actually get access to an account and to get into information.

It's also worth talking about, a lot of times we get asked the question, if DOD had this experience where 46% of their intrusions went away, why aren't we using this everywhere in the rest of the world? And the answer is, we're using it a few places today, but we haven't really found the technology to be ubiquitous, because there are a lot of barriers that are out there. Generally speaking to date, higher assurance credentials have come with higher costs and burdens. They've been very impractical for a lot of organizations to implement, both because of the cost as well as some of the challenges that they introduce, and so a lot of what we've seen outside of government has been that when you have seen some sort of strong multifactor authentication, it's been for a single use application. So a classic example, my online brokerage gives me an RSA secure ID token, which is a one-time password generator, that gives me a new password every 60 seconds and that's actually one of the reasons I keep my money there is I really appreciate the added layer of security they give me on top of a user name and password. But I can't use that any place else I go because there aren't any standards that are out there for interoperability, there's really no way to use that token any place else I might go.

Now we think it's an area that if you had standards for interoperability and these kinds of tokens could be trusted across the economy, Metcalfe's law would apply, we would generate a network effect. But until we overcome these barriers, like interoperability standard or some policy questions like, what are the privacy rules when you use this kind of credential? What happens if something goes wrong, who gets sued and who's liable for what? Are there form factors that are more usable for different people who may not like some of the technologies that are out there today? These are the kind of things that the market has been struggling with for years to overcome and frankly, hasn't gotten there yet. Try to zero in on these barriers and make a focused attempt from our side working in partnership with the private sector to address them is really sort of at the crux of what our national program office where NSTIC is focused upon.

So the next slide details what NSTIC calls for, which is a very different kind of effort than what you've seen with a lot of government programs. We've been very clear from the start, in fact, I can't just say we, the President was very clear from the start, this is something that the private sector will lead. It's not a government run identity program. There was a very strong belief as the strategy was being created that if the government tries to actually specify a solution here, we would fail. Technology's simply too dynamic, there are too many entrepreneurs that are out there constantly shaking up this field. The private sector is going to be in a much better position than the government to drive the suite of technologies and solutions that take hold in the marketplace; not to mention to ensure that the identity ecosystem offers improved online trust and better experiences for folks online.

What the government is looking to do is provide support. So given that this is going to be privately led, one of the most important things for us to do is actually how do you bring together different private stakeholders from different sectors. We spent a lot of time this last year working to develop a privately led governance model. In fact, in the next few days I hope, assuming our grants office cooperates, we'll be announcing a grant for a private organization. It will be a 24 month grant for an organization to serve as the convener and facilitator for a new identity ecosystem steering group that will be charged with bringing together stakeholders from across sectors to work on standards and policies and an accreditation process, to enable this ecosystem, this marketplace, that the strategy envisions. We can also, since we're NIST, a standards agency, work within this steering group to facilitate and lead development of interoperable standards. As government we can also help to provide clarity on some of the national policy and legal issues around things like liability and privacy, for where there aren't a lot of great answers today. And finally, as the government, because we've got a lot of applications online and we buy a lot of stuff, we can act as an early adopter to stimulate demand.

At this point, Naomi Lefkovitz, who is our Senior Privacy Advisor, is going to talk a little bit about some of the privacy and civil liberties aspects of this. So, I'm actually going to switch seats with her so she can get closer to the phone.

Naomi Lefkovitz – National Institute of Standards and Technology, Senior Privacy Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Thanks Jeremy. Can everybody hear me okay?

Deven McGraw – Center for Democracy & Technology – Director

Yes we can, thanks Naomi.

Naomi Lefkowitz – National Institute of Standards and Technology, Senior Privacy Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Great, thanks. So, next slide. So I am going to talk a little bit more about some of the privacy and civil liberty issues that we were dealing with when we drafted NSTIC, and what NSTIC is really calling for. So NSTIC calls for really the holistic implementation of the fair information practice principles and what does that mean in the identity ecosystem. So Jeremy already talked a little bit about sort of how the driver's license reveals too much information, we can actually do better in the online world, where we can really sort of show claims of, I am over a certain age rather than actually sharing the birth date, which can really help clearly in the area of data breaches, where we don't have to share as much PII when it's not necessary to. But there's a flip side which is that, in some ways, a stronger identity ecosystem could have certain adverse impact on privacy and so again, if you sort of look at the driver's license example. When you go to the movie theater or the airport or the bank and show your driver's license as a form of identification, it's not as if the DMV actually knows that you're using your driver's license in that way. So, there have been concerns that in the digital world, your identity provider would know all those transactions, and so that would be concerning.

And so NSTIC is really looking at sort of the use of both policy and interesting privacy enhancing technologies, cryptographic technologies that could help to limit that and I'm going to talk a little bit more about that in some of the upcoming slides. But before we get to that, I'll just say a little bit more about the voluntary side of the guiding principle and so that really goes to the fact that this is, again as Jeremy said, this is supposed to be private sector led. The government is not looking to make a centralized database or a national ID or any sort of legal requirements that citizens out there need to get one of these credentials. So the strategy is really founded on choice for individuals; choice to participate and choice among their identity providers. And again, just to reiterate what Jeremy said about preserving anonymity, all of this sort of leads to the very important point that anonymity is still an important principle and helps to support free speech and freedom of association and NSTIC is not trying to undermine any of those principles in any way.

So, next slide please. So in the next slide, we'll just talk briefly about the NSTIC national program office and what our role, which is that really we're just charged with leading the day to day coordination across government and the private sector in implementing NSTIC. And Jeremy talked about the fact that we're working towards a steering group and on the next couple of slides, I'll talk a little bit more about what we're doing facilitating coordination on the government side. And it's always helpful, I think, to know that we did get funding for FY12 and we got 16.5 million dollars; about 10 million of which we are using to fund a pilot and some to fund the secretariat to start off the steering group and the rest to mature our office. On the next slide I will talk about what we can do with Federal government to help us be an early adopter. I'm not sure how much everyone knows about how the Federal identity management activities are aligned, but, for those who don't, they are aligned through the Identity Credential and Access Management (ICAM) Subcommittee, and that is a subcommittee that is run out of the Federal CIO's Council. And under that subcommittee, there is a program called the Trust Framework Solutions and that's really how the US Government aligns with NSTIC. And the goal of that program is to develop a secure, interoperable and privacy enhancing process, by which Federal agencies can leverage commercially issued digital identities and credentials.

And the way in which they do it is that the ICAMSC crafts the US Government profile of widely used commercial identity protocols like OpenID or SAML. So, if any of you have a Google email, you actually have an OpenID and SAML is often used in the education and research area. And so, what the ICAMSC does is tries to take these profiles and turn them into government profiles that maximize security and privacy. In addition, there were a number of privacy criteria that were worked out for this program, and they too were based on the FIPPS. And if you are very interested in this, you can go to IDManagement.gov and there is lots of documentation on this process. But in short, the principles that were put in were for opt in and adequate notice, and they really work together and say that the user should understand what information or attributes are being sent over from the identity provider to the relying party, and they should have adequate notice and choice about that.

Minimalism, and this is where the government as a relying party is a good example for the greater ecosystem because really the government has already, through the Privacy Act and e-Government, strong privacy requirements already. One of those requirements is not to collect more information than they need for their purpose. And so really what minimalism is saying is that identity providers will abide by that and not send over more information than they have about a user. Activity tracking is pretty key which...really become non-activity tracking and it says that...and this goes to that issue that I was talking about earlier where the identity provider knows all the transactions or can know all the transactions of the user and so, for example, the identity provider may know that a user is going to NIH, but what the activity tracking criteria says is they can't use that information for anything other than to provide the authentication. So, when you as a user might come back to that identity provider to do something else, you will not see ads for healthcare, for example. And, then there are a couple of other privacy criteria around sort of termination and proper management of PII.

So, what ICAMSC does is it sort of takes that technical profile and those privacy criteria and it approves non-Federal organizations to be these trust framework providers. And what these trust framework providers do is, they're the ones who actually accredit the commercial identity providers and those identity providers are going to agree to use these government profiles and abide by the privacy criteria. And that's how this process works to ensure security and privacy for the user, and to minimize sort of the resource impact on the government to try to accredit potentially thousands of identity providers over time.

If you go to the next slide, I'll talk a little bit about some of the barriers that we've had with Federal adoption and some of the sort of food for thought it may give you in some of the issues you may be encountering in the healthcare arena, in health IT. So, what we have here, for those who can't see is, sort of a picture, and on one side are the relying parties which are the government agencies and the problem has been that government agencies really need to move forward with putting more higher assurance, sensitive transactions online, and get these services online. And so they are moving forward, but they've been moving forward in sort of a siloed fashion, which really undermines the benefits of what NSTIC calls for such as the user doesn't need to have more than one credential per agency, and that they can use their high assurance credential in multiple places, or lower assurance credential as the case may be. So what this shows is that there is a set of accredited identity providers, or soon to be and this is just illustrative, and the user can pick among them for the one that suits them and then be able to engage with any of the relying parties, the government agencies. And there is a cloud credential exchange in the middle that helps to support both the agencies and the identity providers, because it turns out that it can actually be fairly technically involved for a relying party to interact with multiple identity providers. And so the credential exchange can do this heavy lifting. And the reason that we sort of bring this to your attention is because we are seeing in the health IT arena, that there is a movement towards this kind of credential broker or identity hub is another term that you might hear. And so it's probably important to be aware of some of the security and privacy implications that we have actually started to deal with, as we move forward.

The White House actually put together a group of five agencies, the Veterans, HHS, IRS, SSA and Department of Education; and they've been participating in our own Tiger Team, the FSTICs Tiger Team, to develop these requirements. And that work is actually almost finished and it included an investigation of how to integrate some of that privacy enhancing technology using cryptographic techniques that actually keep the broker from knowing too much about individual users. So, it's a way to sort of preserve what we were talking about earlier, where the broker doesn't have to know where ... everything ... doesn't have to know a lot of PII about the user, but can sort of transmit attribute claims. And it also keeps the identity provider from knowing necessarily too much about what the...where the user is going and what they're using their credentials for.

So the next steps are sort of determining the best option to develop this FCCX and we'll certainly be happy to keep you informed as to where we go with that and the lessons that we learn in that piece. Now I'm going to turn this back over to Jeremy for the next steps.

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

Could I ask one question before you leave this slide?

Naomi Lefkovitz – National Institute of Standards and Technology, Senior Privacy Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Absolutely.

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

Is the FCCX and integral part of NSTIC, or is that just a stepping-stone towards something that would replace that. I mean, it makes a lot of sense to have the broker in the middle that can do some of the pseudonymizing, but is that a core part of NSTIC.

Naomi Lefkovitz – National Institute of Standards and Technology, Senior Privacy Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Well, it's a service or a tool to enable some of the policies and the standards of interoperability and what we're trying to do is do it in a way that aligns with NSTIC, which is really a strategy of guiding principles. So, we're trying to do it a way that conforms with the privacy guiding principle and security and interoperability and ease of use.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Let me answer you the question a slightly different way, which is that NSTIC, because it's a strategy, doesn't actually prescribe any specific technical solutions. What the NSTICs Tiger Team has been looking at is actually how to look at a cloud credential exchange in large part because it's what we've seen a number of different private sectors start to look on is, how can you look at a hub like this that would help them rationalize...come up with an easy way to actually accept and trust different privately issued credentials. So, one of the challenges we've been looking at in government is as more and more private firms, like Verizon and Google and PayPal and Symantec buy into the government's vision for trusted identities through the ICAM process, it actually can become quite cumbersome for agencies to support all of them and we've been concerned. Howard Schmidt wrote a blog post last October basically pointing out that one thing you want to make sure is that if I'm a veteran and a college student and a tax payer, I shouldn't have to get a PayPal credential to access my records at the VA and a Verizon credential to get my ones for Federal Student Aid and a Symantec one to get my ones at the IRS. If I have a single accredited credential, I should be able to trust it everywhere. Likewise, agencies should be able to connect to all of the accredited credentials without having to do one-off connections every time a new vendor gets accredited. So the notion of offloading all of the hard work here to an enterprise cloud solution is something that we've seen the private sector start to embrace, and we said why don't we come up with requirements to do this at the Federal level as well. It really is a way to help agencies support the NSTIC vision. Does that help?

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

It does, although I think that the fundamental question is still there, which is, if you envision the cloud broker as an interoperability solution, where you create the interoperability, that makes sense and basically says that your interoperability standards aren't good enough to get away without having the cloud broker, and I understand that that might be a market reality. The question I was focused on is more that the cloud broker could be a mandatory step to create the pseudonymity, so that the IdP couldn't track the places where the credential was actually validated.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Yeah. I'll tell you, certainly one of the things we're looking at right now on the Federal side, as Naomi was saying, is how can you build that non-traceability into the solution, and it's something we're actually pretty excited about. I will say from the NSTIC side, because, again it's the government strategy and we're really trying to focus in implementing the strategy and, how can I say, coach the market towards certain solutions without actually mandating anything. We haven't recommended anything specifically yet as an architecture, but we are very committed to ensuring that the privacy enhancing aspects of the strategy are actually implemented in the marketplace and, candidly, a lot of what we're seeing is being done in the private sector right now. In many cases, we're actually trying to follow their lead in terms of what are major firms in the enterprise base looking at. It's what they're looking at today themselves, because many of them don't want to necessarily have to deal with that liability issue of all this data being archived.

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

Yeah. Okay, thanks.

Naomi Lefkowitz – National Institute of Standards and Technology, Senior Privacy Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

But I do want to make sure that you don't leave with the impression that you have to have the credential exchange to do that sort of anonymity. You can use those cryptographic technologies directly between the identity provider and the relying party, but again, it is sort of that same issue of the one-offness and sort of the technical burden and the incentive to actually...to overcome those barriers and that credential exchange can really help with that.

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

I have a question. This is Dixie.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Sure.

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

I can certainly see the need for something to assure interoperability among different credentials from a technical perspective. Do you guys envision that this exchange or this broker, let's just call it broker, this middle person, middle entity, would also do interoperability among trust levels? In other words, they would know that, and I'm making this up, PayPal uses level 2 of identity validation whereas Google uses level 3, so there's a difference in the trust level between the two, so there seems to be need for not only technical interoperability, but interoperability among trustworthiness levels.

Naomi Lefkowitz – National Institute of Standards and Technology, Senior Privacy Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Yeah, that broker can certainly do that as well.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

And I think particularly where you have firms like Symantec that actually have solutions certified at multiple levels, you'll need to what kind of credential is being presented, what level of assurance or trust is built into it. We've also looked at, in the Tiger Team, although I don't know that we would necessarily look to have it be part of the key requirements, at least for version 1 of this, but how could you have a credential exchange that could also potentially do trust elevation, which is a term that gets talked about quite a lot in our world. If I'm coming in with say a Google ID and I actually need to have something else in order to get access, how could that plug me in to a service that could ask me a few questions or validate something else about me that would elevate me to a higher level of trust, thus getting me into a new application in a relatively seamless fashion.

OASIS has a technical committee looking at trust elevation, it's just put out its draft report, and I think there's a lot of excitement within the private sector for those kinds of solutions, recognizing that sometimes people are going to need different types of credentials or verification in order to get into different systems.

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

Oh, that's good. That's very good. I'm glad I asked the question.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Again, it's not ... yet, there's a lot of work going on right now. What we're trying to really do is ensure that with FSTIC, that the government can be at the forefront of it, not to mention there's certainly an interest from a good government perspective in making sure agencies don't keep building these same systems one by one on their own; it can be quite costly that way and you don't get the interoperability.

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

Thank you.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

So I was going to move on, I have a couple more slides to wrap up with, next steps and then we can have a little bit more discussion.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, go right ahead Jeremy.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

So the next slide just really talks about three things we are focused on for next steps. The first is convening the private sector. I talked before about how we're close to making a grant, a two-year grant to fund a privately led steering group to convene stakeholders to build an identity ecosystem framework. Our current timeline suggests that we'll probably have a virtual pre-plenary session for this toward the very end of July, where the firm that's chosen to serve as the secretariat and the convener will actually have one or several sessions online to sort of lay out how the group will be formed and they would then be targeting the week of August 13th at some place to be determined, probably geographically in the middle of the country, for a two day meeting that would be the first, in-person convening of the steering group. So, keep those dates in mind.

The second thing we're focusing on is we are getting very close to selection of pilots. We had published, back in February, a federal-funding opportunity for a ten million dollar pilot grant program. We're expecting to make 5-8 awards, probably in late August or early September. The federal funding opportunity really took a challenge-based approach, identifying a number of barriers the marketplace has not overcome around trusted identities, and challenging bidders to come up with solutions that would actually smash through some of the barriers and provide a foundation we could build this thing off of.

And finally, we are continuing to work, as Naomi was talking about, to ensure government can be an early adopter to stimulate demand. In addition to the work on FSTIC, we're working with a lot of other parts of agencies across government to ensure that they can actually align with the FICAM roadmap that's in place today; and certainly I'd say while ONC is not a traditional government customer, the work that they are doing and that you're doing in partnership with them to help catalyze the adoption of health IT systems, certainly falls under that.

In terms of what you can do, and I'm actually really looking forward to the discussion that comes out of here, I think the first thing, this is on the last slide, is to participate. Talk about the value of NSTIC to colleagues and look to support NSTIC pilots, as some of them are awarded by, potentially if any of you represent organization that might want to be a relying party to some of these new pilots, look to do so. We're also looking to have great participation from the health sector in the identity ecosystem steering group that could set up later this summer. The second thing is be early adopters. We're looking for more and more organizations who want to help leverage new trusted identity solutions to move services online, and look for ways to potentially support identity and credentialing in partnership with trusted third parties. Finally, stay in touch with us; give us your ideas. We view all of our external stakeholders as key partners and want to hear from you. And on the very last slide, both Naomi and I have our contact information listed.

One thing we didn't address directly in the slides was actually what Deven laid out early on which was the previous recommendations of the Tiger Team and whether it makes sense to have a discussion in terms of whether to well, discuss some more, in light of some of the work that's actually going on with the President's strategy and our program office. The only thing I would mention sort of outside of that, is one thing we're seeing a tremendous amount of support for in the marketplace is actually in the health community, where a number of...in fact, if I had to say there was a single largest commercial driver right now for firms to get their NIST level 3 multifactor authentication solutions accredited through the FICAM process, the GSA run, it's the DEA e-Prescribe market, where a lot of the vendors are looking at this and saying, most physicians are going to need to get a level 3 credential as mandated by the DEA spec, for electronic prescribing. And that had actually had some of them have come to us with the conversation, given that the majority of physicians are going to have this credential anyways, why shouldn't say CMS or other parts of HHS, also be able to accept that same DEA credential if a physician needs to interact with one of those agencies for something online. And why shouldn't that also be that the...credential that they have to use in order to access health IT systems. Our take is, that's a very interesting question, we're not setting the standards on the health IT side, but we're certainly talking to the folks that are, and so, I won't say any more there, other than to say I'd love to open up that conversation.

Deven McGraw – Center for Democracy & Technology – Director

Well, and personally Jeremy, and this is Deven, I actually think that's an avenue that if we can explore it more in the hearing, would be one that we should explore further.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

We haven't actually talked much about the hearing in terms of who will be speaking, is there a list yet of folks who will be talking, because there are certainly plenty of folks in the private sector who have come to us and said, we think DEA is really the...those credentials are what's going to set the standard for the rest of the physician community.

Deven McGraw – Center for Democracy & Technology – Director

Right. You know, we're still sort of working on that, but that was definitely the...sort of DEA angle is one that I think we wanted to try to get some folks to come in and talk about. Whether that can be DEA or whether it's more appropriate for that to be...or more likely to be somebody else I think is a little unclear. I don't know, Kristen or Joy, do you want to...I know you've been working on trying to sort of pull together some potential testifiers, I didn't know if you wanted to add anything on that at this point.

Joy Pritts – Office of the National Coordinator

Kristen?

Kristen Ratcliff – Office of the National Coordinator

Nope. I think that at this point we're still kind of coming up with the list of who we think would provide the most well rounded perspective on a number of different issues, so we'd welcome your feedback and anyone's feedback on the call. If you want to inform the panelists or if you know of work, being done in this space that you think would be particularly relevant for the workgroup to hear from, please let Deven or Joy or I know.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Yeah, let me throw some ideas out. I'll say one of the things that we've been trying to do from our office, because we're trying to catalyze the marketplace is, look first and foremost to see what is the marketplace doing today and, to mix our ocean metaphor, as we often say, we're not trying to boil the ocean, we just want to go surfing where the waves are. So, there seems to be a lot of waves already around this space and it certainly would be one perspective that we'd urge everybody to look at in terms of what the marketplace is already sort of naturally gravitating toward, or could with a little bit of a push.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, well, building on solutions that are beginning to work, whether that's in the health sector, which is ideal, or in other sectors is certainly easier than trying to reinvent the wheel. Do folks have...we can open this up now, including if folks have been sort of more involved in the identity authentication end or NSTIC space who want to make some suggestions for entities or individuals who might be good to bring to the hearing, this would be the time to weigh in; not that it will be your only one, what I think we want to do is, as staff are working to try to pull together an initial witness list, we would also try to circulate that, when we can, to get some additional input from you all. But certainly, if there are folks on the call who already have some great ideas, we'll take them.

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

So Deven, this is David.

Deven McGraw – Center for Democracy & Technology – Director

Hi David.

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

I have one name or suggestion, just to consider pursuing, which is you might want to talk to some of the folks at MITRE that are working on this RHex project, the RESTful health exchange. They're trying to figure out the right way to use O-F2 and OpenID Connect to send assertions about identity, so, it's really more about the transfer of identity from an identity provider to a relying party, without requiring a subsequent login. That may be too technical for the July hearings, but Joy Keeler could give you a list of experts that are deep into the healthcare issues.

Deven McGraw – Center for Democracy & Technology – Director

That's a great suggestion David, thank you. I mean, recall that we're sort of trying to meet the needs of both the Standards and the Policy Committee in one hearing, so, we may have to take on some of the technical...we will...

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

Yeah, unfortunately you're going to be stuck with this.

Deven McGraw – Center for Democracy & Technology – Director

(laughter). I'll be taking copious notes during those portions of the hearing.

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

I actually have a policy question, and that is, not a technical question, when you're ready to go to questions.

Deven McGraw – Center for Democracy & Technology – Director

Well, I think we're there David, so go ahead.

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

So, I appreciate the value of reducing data exposure with a proper credential that only releases the sufficient data necessary to complete a transaction and how that is privacy preserving, and your age over 17 is a good example. But at the other end of the spectrum, I'm concerned, from a privacy point of view, about the potential for data aggregation across disparate entities who now have, at least in theory, a clear identity for you. So, the movie theater may only care that you're over 17, but they know who you are by virtue of this identity token and could join that data against a marketing firm or whatever, and use it to exploit aggregation across IdPs...I mean, relying parties. So, does the model account for that with cryptographic techniques, or is that just a policy issue as to whether that's allowed or not?

Naomi Lefkowitz – National Institute of Standards and Technology, Senior Privacy Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Both...I mean, it actually starts with sort of, yeah as a policy about...derived from the FIPPs on data minimization; that is, so the movie theater should only ask for what it needs, which is really only an assertion that the person in front of them is over 17. But the fact is, they actually don't really need to know who that person is; and so that's an important part of the credential, which is that it doesn't actually have to say that this is Naomi Lefkowitz who's over 17, it's merely that you can trust that this credential is properly bound and that the holder of it is over 17.

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

But I can't imagine any movie theater being happy with that as the sole outcome of implementing this kind of a transaction. In other words, they're going to have a frequent watcher program and they're going to want to know which movies you liked and didn't like, and they're going to use this technique to validate you when you log in. And now they've captured a lot of stuff about you because that's the business they're in and they have a joinable identity token.

Naomi Lefkowitz – National Institute of Standards and Technology, Senior Privacy Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

That is true and so one of the ways that that is handled in the government space, and this sort of goes to what I was alluding to in terms of the US Government profiles of OpenID and SAML and others coming down the pike like OpenID Connect is that, for example, in OpenID, the requirement is that each relying party get a different identifier, that they cannot correlate among relying parties and aggregate information that way. So, yes, the particular relying party can collect information and do it for their own personal marketing and likewise, if you don't like that, you can go to a different movie theater, but movie theaters across...cannot correlate information. So there are certainly technical ways that can be done, even before you even get into some of the higher-level cryptographic techniques.

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

Okay, well I have zillion questions, but I'll cede the floor.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

I also just note, real quick, there's nothing in NSTIC that would preclude you, as an individual, if you wanted to share that information in exchange for some benefit, say being part of a loyalty program, from doing it, but the default behavior has to be that that's something that you don't have to do. So, I mean, I was at the movies on Saturday and AMC has their loyalty card program that among other things, you don't have to pay a fee when you buy a ticket online, if they can track what movies you're seeing and send you offers. There's nothing that NSTIC would put in place that would preclude any business from offering you that ability to give up more of your day, perhaps in exchange for something. What we're really focused on with NSTIC is ensuring that the default behaviors are that you don't have to and they can't take that information and aggregate it without your permission.

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

So the need to create what I would call partitioned identities is what I guess I'm really concerned about. I mean, one benefit of passwords, user selected passwords is, you can partition your identity and if we give that up, that's a significant privacy loss. So, there would be some need to enable partitioning of identity.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

I'll say conversely, there's nothing that's trying to preclude folks...there's nothing that's trying to promote everybody to get a single credential in NSTIC. In fact, we envision that people will want to have multiple credentials in the ecosystem, much as...I mean I partition my identity today; I've got two Hotmails, a Google and a Yahoo account and I use them all differently when I go online. So, in theory you could have ... you could choose to have as many keys on your keychain as you'd like.

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

A pocket full of tokens, okay.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Or a pocket full of apps on your smartphone, which honestly is where most of its going these days.

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

Yeah, yeah, as long as your smartphone vendor supports it, which is a problem because of the way they do those SMS codes, but anyway ...

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Well, so, without getting too much into the tech details, I'll say, haven't been around this space a long time, the amount of innovation going on around the apps base and smartphones right now, including ones that are being supported by Verizon and AT&T is pretty amazing, and I think we're actually ... I'll candidly be surprised if two or three years from now, when we're really implementing this, if it's a onetime password the way that you and I are used to it today, that ends up being the solution. There are some pretty impressive entrepreneurs that are out there that are coming up with things that I've never seen before that are a lot more useable and user friendly than what we've seen today.

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

Great.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

A couple of them are going to stick, I think.

Deven McGraw – Center for Democracy & Technology – Director

Other questions.

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

You know Deven, these entrepreneurs that are coming up with solutions; it might be worthwhile to include at least one of those in our hearing.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, agree.

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

Yeah, I think that's a good point. I would second that because the smartphone onetime generator stuff is not very friendly at the moment and I'd love to hear why they think that's going to get better.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

We can probably help put you in touch with some folks. I'll say the one company who has actually gotten accredited so far through GSA for level of assurance 3 is Verizon. Given that they actually have made the investment and become the only certified provider, I think you'd probably want to have them; but if you wanted to bring in some others with what might be considered disruptive solutions, I'm sure we can help you understand some others that are in the marketplace.

Deven McGraw – Center for Democracy & Technology – Director

Yeah, I think that would be great.

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

I think in particular to kind of reset people's mind away from just passwords as our solution, have somebody present some of these innovative approaches.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Okay. We can work offline on some ideas there. It's...I will say, one of the things that a friend at Google reminded us when we first started is, this is no small feat what we're trying to tackle, not only because of the differences in technologies, but everybody in the world has been conditioned for 20+ years to look for the login box everywhere they go online. And you're now actually talking about changing that, that's not a small feat.

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

Yeah.

W

So, but it might be nice not to have it anymore.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

There's also an increasing amount of people who seem to be demanding that there be a different solution, so yes.

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

And the efforts that we've had in electronic voting, where you want to capture someone's vote without necessarily associating the vote with their identity, has not been completely successful. This is hard. This is hard.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Most definitely.

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

Yeah, I mean, because people really want that identity, they want to know who you are, and not just how old you are. So, there's going to be a lot of tension there.

Deven McGraw – Center for Democracy & Technology – Director

And I think we have to, this is Deven, I think we have to think through what it is in the physician identity space that's going to be needed to sort of be part of the credential, especially for cross-network access.

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

For one thing Deven, this is David again, that a number of us have been talking about is, if direct catches on, and physicians obtain direct addresses for their secure email, that that can be leveraged as an identity provider. Essentially your direct account provider becomes an IdP, and then you can use your direct address as your identity. So, that's another interesting possibility for the hearing. I think the MITRE folks could address that approach.

Deven McGraw – Center for Democracy & Technology – Director

Right. Terrific. Any other thoughts?

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

Someone is bound to raise the question about patient identity and a national patient identifier, as was the case in Privacy...no, the Bipartisan Coalition meeting a couple of weeks ago when someone from NSTIC was there with Farzad, and so, I don't know, you probably want to stay away from that, but I bet somebody will ask about it.

Deven McGraw – Center for Democracy & Technology – Director

Well, undoubtedly, and we do need a patient identity solution for patients being able to access their own information and be able to move information, which is sort of a distinct purpose from an identity that gets used in order to...well, I mean maybe it's not distinct, but, sort of being able to match patient data in a provider-to-provider exchange as well. But one of the things we have been asked to do by ONC is to think first about credentials for physicians in NwHIN and then, secondarily, we can take up the issue of patients.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

And let me just say on patient, especially understanding that it may be a secondary priority, the vision with NSTIC, if we're all doing our jobs and this thing succeeds is that in three or four years, a significant proportion of the US population is now carrying a credential. Again, I personally think it will be something bound to a smartphone, but there will be different form factors supported, that can then be trusted everywhere. It can be trusted when the log onto their bank, it can be trusted when the log onto Amazon, it can be trusted if they log into the IRS and it can be trusted if they're accessing a private hospital to download their health information; that's really the vision of where we're trying to go, is ensure that there's a common set of standards and policies in place that will allow that vision to be realized. If we succeed, it solves your patient authentication challenge.

Judy Faulkner – EPIC Systems – Founder

And this is Judy. One of the things I think we do have to consider with patients is that they may be in a different situation than doctors in that sometimes you're going to want to get information from them that they won't be carrying around a card, because maybe they got suddenly ill and they don't have a card or maybe they don't have a cell phone with them. So, we do need a backup way to do it without those things.

Joy Pritts – Office of the National Coordinator

This is Joy, and this is exactly the reason why we want this. I wouldn't say it's a secondary consideration, the patient ID, I would not use that term because I would have my head handed to me if I...

Deven McGraw – Center for Democracy & Technology – Director

I appreciate that, bad nomenclature, because it wasn't exactly what I meant either.

Joy Pritts – Office of the National Coordinator

Yeah, I know it isn't. But, because these are distinct use cases, and we well recognize that when we raised the use of NSTIC with respect to consumers/patients that is probably going to be its own...a lengthy enough discussion to be its own hearing. We did not really want to focus on it at this hearing; otherwise, it would have been twice as long. So we just have to break them up in order for them both to get adequate consideration. And Jeremy, when we were at that...I was at that meeting that David just was speaking about, and I think a short answer that was voiced at the meeting was that NSTIC helps you avoid having that national patient ID, and it helps you avoid the patient having to give all of their demographic information to everyone all the time.

Jeremy Grant – National Institute of Standards and Technology, Senior Executive Advisor, National Strategy for Trusted Identities in Cyberspace (NSTIC) Program

Absolutely. This is...I mean the whole focus of NSTIC, whether it's looking into health domain or the retail domain or anything else that we're doing online is, how do you avoid having to have a national solution where there's a national issued credential and instead, how can you leverage the marketplace to provide a whole ecosystem of solutions that individuals, if they chose to, can choose to accept, and obtain it and present different places. So, it's...what we get asked all the time isn't this a national ID and the answer is no, it's a digital identity strategy for the country that specifically does not rely on a national ID. The bottom line is, when it comes to patient identity, there's really three options; one is you could continue to rely on user name and passwords and as a guy who's sort of committed to replacing the password, I say that's probably not the way you want to go. The second is everybody can issue something just for healthcare. Given the cost and other issues with that, that's also probably not the way you want to go. And the third is, wouldn't it be wonderful if the marketplace was simply catalyzed where everybody had a compelling case, or the majority of the population had a compelling case to simply get a credential on their own, and health systems could then trust it because it actually followed the standards and policy that are outlined in the NSTIC. And we think that's going to be the best solution and where you'll probably be able to achieve the greatest market penetration most quickly, but there's a lot of work still to enable that one as well.

Deven McGraw – Center for Democracy & Technology – Director

So I'm looking at the time on my clock and we're nearing the period where we need to move into public comment. But before I do that, can I get a sense of which of you on the Tiger Team is planning to attend the hearing on July 11th in person, either as yourselves or sending a designee?

Gayle Harrell – Florida House of Representatives

This is Gayle; I will definitely be there.

Deven McGraw – Center for Democracy & Technology – Director

Judy, how about you?

Judy Faulkner – EPIC Systems – Founder

I'm trying to find a designee.

Deven McGraw – Center for Democracy & Technology – Director

Okay, great. David?

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

I'll try to be there, I haven't looked at the calendar yet.

Deven McGraw – Center for Democracy & Technology – Director

Okay. I mean, there's always a phone option, but we're trying to figure out room size basically.

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

Oh, yeah.

Deven McGraw – Center for Democracy & Technology – Director

So, just let us know when you can.

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

Okay.

Deven McGraw – Center for Democracy & Technology – Director

I don't think John's on the phone any more.

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

I'm planning to attend.

Deven McGraw – Center for Democracy & Technology – Director

See, I knew you would be.

MacKenzie Robertson – Office of the National Coordinator

Hi, this is MacKenzie; I'll just put in a plug here. The save the date calendar appointment that went out had a link included in the appointment, for you to RSVP. So if it's easier, once you've all checked your calendars just to go back into the save the date, click on the link and the appointment and just click yes, you'll be attending.

Deven McGraw – Center for Democracy & Technology – Director

Was that from you personally or from ONC FACA?

MacKenzie Robertson – Office of the National Coordinator

That was from the ONC FACA.

Deven McGraw – Center for Democracy & Technology – Director

ONC FACA, okay. And it does say save the date in the subject line, I did...that was really clear.

MacKenzie Robertson – Office of the National Coordinator

It does.

Deven McGraw – Center for Democracy & Technology – Director

All right, great. All right MacKenzie, why don't we open for public comment?

MacKenzie Robertson – Office of the National Coordinator

Okay. Operator, can you please open the lines?

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. We do not have any comments at this time.

Deven McGraw – Center for Democracy & Technology – Director

All right, terrific. Thank you everyone for being on the call today. Thanks especially for Jeremy and Naomi for the presentation on NSTIC. It was incredibly helpful to sort of lay the groundwork for what we're going to do, and we appreciate also the suggestions on the hearing. So, anything else anybody has to add before we say goodbye? All right. Thank you again. Everyone have a good rest of your day.

W

Thank you.

M

Thanks, you as well.

MacKenzie Robertson – Office of the National Coordinator

Thanks everybody.

Joy Pritts – Office of the National Coordinator

Bye Deven.

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

Bye.