**Testimony to HIT Standards Committee Privacy & Security Workgroup**
**Jeremy Grant, Senior Executive Advisor, Identity Management, NIST**
**March 12, 2014**

Good morning, and thank you to the members of the committee for inviting me here today to talk about the National Strategy for Trusted Identities in Cyberspace (NSTIC). I lead the National Program Office (NPO) that was established at NIST to lead implementation of the Strategy, and I am excited to see this Committee choosing to focus the better part of today on the topic of Trusted Identities in Cyberspace.

Next month will mark three years since President Obama signed the NSTIC. As we've discussed in previous hearings, NSTIC is a national initiative that calls for government to collaborate with the private sector to raise the level of trust in online transactions in a way that improves privacy, security and usability for all Americans.

While a government-issued strategy, NSTIC calls on the private sector to lead its implementation, driving creation of a vibrant identity ecosystem *"where individuals and organizations will be able to trust each other because they follow agreed upon standards – both technical and policy – to obtain and authenticate their digital identities."*

In simple terms, NSTIC seeks to catalyze a vibrant marketplace where all of us within a few years can choose from a variety of different types of advanced identity solutions that we can use everyplace we go online – in a way that is more secure, convenient and privacy-enhancing than the password-centric systems that we use today.

For health care – where the promise of electronic health records largely depends on trust for EHRs to reach their full potential – NSTIC is especially important. At a time when passwords are the number one vector of attack in data breaches – 76% of all breaches in 2012 were executed by exploiting the various weaknesses of passwords – and identity theft in all sectors including health is a major issue, NSTIC lays out a path for the creation of market-driven, standards-based solutions that will enable health providers or patients to easily log into EHRs in a way that ensures good security and protection of privacy.

Among sectors participating in the implementation of NSTIC, health has been at the table – although as I will detail today, there is a lot more that the health community could be doing to help advance the implementation of the Strategy.

And there are material reasons why health should be doing more. At the end of the day, the success of electronic health records will be largely dependent on whether providers and patients are willing to trust them, and whether they are easy to use.

Particularly for patients, the idea of enabling initiatives like Blue Button that allows patients to easily download their health data and share it with others is exciting – but the full potential of these initiatives will only be realized if patients have an easy way to assert that they really are themselves online, and not the proverbial "dog on the Internet."

Protecting sensitive personal information with passwords is akin to building a massive stone fortress and then securing the front door with the kind of lock I use to keep my two-year-old out of my bathroom.

NSTIC lays out a path to solve this challenge, enabling providers and patients to easily and securely log on to multiple health applications in the cloud, without having to go through the hassles and costs of obtaining a new credential.

Identity is certainly not the only layer of security needed, but it is one of the most important – and given the need for the end-user to play an active role in asserting his or her identity, it can be one of the trickiest layers to implement. The solution can't simply be secure – it has to be easy to use, or else users won't bother. Solving what we often refer to as the "identity conundrum" is not something that can be easily done by any one player or sector – it requires collaboration across many types of stakeholders to craft scalable, standards-based solutions that are interoperable across sectors.

NSTIC calls for a voluntary, multi-stakeholder collaborative effort to tackle this challenge. If there is one message I want to leave you with today, it's that voluntary efforts do not succeed without committed volunteers. I hope that today's hearing will help to increase the commitment of health stakeholders in advancing the NSTIC.

++

As we approach the three year anniversary of NSTIC, there is a lot of good progress to report:

1. **12 NSTIC pilots are helping to seed a marketplace of trusted identity solutions and tackling barriers the market has struggled to overcome.** Six of our 12 pilots have some nexus with health applications. You'll have the chance to hear from some of them today. Our office just last week closed our most recent pilots solicitation; 42 applications were received and we expect to make another round of awards in September.

2. **The Identity Ecosystem Steering Group (IDESG) is working to craft a framework of standards, policies and operating rules to support the Ecosystem.** Key to the implementation of NSTIC was the creation of a privately-led steering group that would bring together stakeholders from across the spectrum to oversee the process for policy and technical standards development.

   The IDESG first convened in August, 2012; today it has more than 200 members who are collaborating each week to advance the implementation of the NSTIC. Membership is quite diverse: the Board alone includes representatives from firms like Oracle, Aetna, LexisNexis, Neiman Marcus, Gemalto and Salesforce – as well as advocacy organizations like the AARP and Electronic Frontier Foundation (EFF). The diversity of participants is quite remarkable – as is the fact that all of the parties I just listed not only all agree on something but are all working together to advance it. It is rare in these times…

   Since its establishment, the IDESG has established a Priority Action Dashboard of deliverables needed to create the Identity Ecosystem Framework and is making good progress against it.

Among early activities, the steering group has developed a functional model, defined core use cases and developed a novel privacy evaluation methodology (PEM) that is being used by many NSTIC pilots as a way to evaluate the privacy risks of identity solutions.

Among the early sector-specific groups to form in IDESG was a Health Care Committee; you'll be hearing more directly from its chair, Dr. Tom Sullivan, later today. It's fantastic that the Health Care Committee exists – although I will note that if you look at the participants (http://www.idecosystem.org/group/healthcare-committee), many major players in the health sector are not at the table. Given how important an issue this is to the success of Health IT, we'd like to see broader involvement here. I will note that HIMSS last month announced the formation of a new secure identity task force that will work closely with the IDESG, and I'm hopeful that this may help to attract some new players.

3. **The Federal government is helping to drive the Identity Ecosystem by making major advances in its use of federated identity.** As background, NSTIC called upon the Federal government to lead by example on NSTIC – being an early adopter of the Identity Ecosystem in the services it provides to citizens and businesses online.

   Key to this is finding an easy way for agencies to integrate with the growing array of externally-issued credentials that are approved for US government use under the GSA FICAM Trust Framework Solutions (TFS) program, which Anil John will discuss later today. This approval program is one of the first of its kind, and an important step in government demonstrating the feasibility of accepting identity solutions that are not its own. The government is somewhat blessed to have 12 approved identity services today, with several more in the pipeline. But agencies have made clear that integrating with twelve different solutions is no picnic – and have been asking for a solution to simplify it.

   The upcoming launch of the *Federal Cloud Credential Exchange (FCCX)* is specifically designed to address this simplification issue – and its launch will be a key milestone for NSTIC. Doug Glair from the US Postal Service will tell you more about FCCX later today, but I'd suggest the key takeaway for this Committee is that FCCX represents the kind of commercially available identity hubs that are out in the market today as a solution for helping online service providers integrate with a variety of different identity solutions. As the health sector looks for ways to help providers big and small – and patients – join the identity ecosystem, we believe identity hubs are likely to play a major role.

4. **The marketplace is responding to NSTIC's call for better technical standards and interoperability.** February was a great month, with two major new technical standards advancing in the world of online identity. The first was the formal finalization of OpenID Connect, which provides a strong authentication layer on top of the widely used OAuth 2.0 standard. And the second was the release of the draft FIDO specifications, which aims to create a "wrapper" that will enable online service providers to leverage the dozens of different

alternatives to passwords for authentication in the marketplace through a standardized approach. As you'll hear today there is still more work to be done on standards – but these are two industry-driven advancements that together go a long way to providing a better technical foundation for the identity ecosystem.

++

Today marks more than two years since this Workgroup last held a hearing on NSTIC. As a result of that hearing, a decision was made to upgrade security recommendations for health care providers to include multi-factor authentication. And the recommendations called for ONC's work on providers to be "informed by NSTIC." For patients, likewise, the Workgroup recommended that ONC to develop and disseminate best practices that, among other things, are "consistent with NSTIC."

A key driver in these recommendations two years ago was that NSTIC has just been launched and the committee was reluctant to recommend specific actions around solutions that did not exist.

This was not an illogical outcome – it would be hard for this Workgroup to recommend the adoption of technologies or processes that are not yet widely available in the marketplace.

That said – if the Workgroup or the broader health sector are of the view that this marketplace will soon be created while everybody sits back and watches, I believe folks are going to be waiting for a long time.

As I noted earlier today, voluntary efforts do not succeed unless people volunteer. NSTIC will only succeed if sectors in need of better identity solutions step forward and demonstrate a willingness to roll up their sleeves in support of the collaborative effort. Likewise, if every sector takes a wait and see approach, it is certain that we will not get very far.

**NSTIC is an opportunity for health care to solve a vexing problem.**

I would suggest that this Workgroup – and, indeed, the health community as a whole – look at NSTIC not as a program, but rather as an opportunity.

- By throwing down a marker for the future Identity Ecosystem that was embraced by industry and advocates alike, President Obama created an opportunity to change the marketplace.
- By funding NSTIC, Congress created an opportunity for pilots to test new, better approaches to online identity and a venue in the Identity Ecosystem Steering Group for stakeholders across different sectors to work together to advance the marketplace.

These are not opportunities that come every day – nor are they ones that are likely to exist in perpetuity.

To capitalize on the opportunity, stakeholders must decide to seize it – meaning that they step up to the table and proactively engage to make the vision laid out in the NSTIC a reality.

Given what is at stake, I hope to see much stronger involvement from the health community over the next year. NSTIC offers an opportunity to help inspire patients and providers to trust in electronic health records – and empower them to leverage EHRs to play a bigger role in their care.  If they come, we can and will build it.

Thank you, and I look forward to your questions.