

## Meeting Minutes

### Attendees:

**Commissioners:** Tom Donilon, Heather Murren, Pat Gallagher, Keith Alexander, Herb Lin, Steve Chabinsky, Sam Palmisano, Maggie Wilderotter, Annie Anton, Peter Lee

**Others:** Kiersten Todt, Kevin Stine, Matt Barrett, Robin Drake, Amy Mahn

### Agenda:

- I. Revised timeline for topics and turnaround time
- II. Identity Management and Authentication Discussion led by Kevin Stine
- III. Next Steps/Wrap-Up

### Discussion

#### I. Revised timeline for topics and turnaround

- a. **Ms. Todt:** We will be sending a revised timeline to the commissioners. Each week we will discuss a topic and rapidly develop draft language based on discussions of that topic. Today, we will discuss identity management and authentication.
- b. Discussions last week were good and productive.
- c. We should try to turn around quickly discussions on workforce.

#### II. Identity Management and Authentication Discussion led by Kevin Stine

- a. We will walk through the proposal carefully looking at the core ideas.
- b. Identity management is a challenging area. There is a lot that can be done. We will be able to touch on some of the moonshot ideas.
- c. It has been an important idea for the current administration including government actions and public awareness. Identity management will impact other recommendation areas.
- d. We have talked about it as a distinct area, but there is intersection with other topics in the draft.
- e. The proposed recommendations we will talk about today have been heavily informed by the commissioners, namely Mr. Palmisano and Mr. Sullivan.
- f. The top line proposed recommendation is to establish requirements for an identity clearing house to be run by Commerce and the private sector for the certification regime. It will make a strong partnership with government and the private sector. Draft language references current strategies of this administration, and the Fast Identity Online (FIDO) Alliance.
- g. Should ensure that there is an understandable base line for consumers to understand how information will be handled.
- h. Broadly in the area of liability and identity management, we see the proposed recommendation that Congress should establish a firm foundation in other areas. It does not really exist in identity management today. It speaks to a lack of liability

- standards creating a one by one organizational approach rather than a unified approach.
- i. The President will release a plan for identities. We would like to work with Mr. Sullivan to further develop. The context really focuses on providing access to government services. It calls for pilot efforts.
  - j. The fourth area is developing privacy solutions, including limiting profiling individuals while they access services. We are talking not just about inter-operability, but privacy and usability of the end user while they conduct any online transactions. It includes retail and government.
  - k. There are a few others that reside with the identity space. Much of focus to this point has been on the identity of individuals, or individuals in organizations.
  - l. There is also the importance of identity of devices. Those devices may participate in a variety of services in different ways.
    - i. We are looking at a similar model for device identity.
    - ii. There is a second piece on consumer/public awareness. Consumers are already conducting online transactions in a variety of ways.
  - m. One of the major points to meeting consumer demand is greater inter-operability of different entities, retail, medical, others.
  - n. Questions –
    - i. **Mr. Lin:** From a privacy perspective, would like some discussion on whether or not trusted identities will be a mandated part. One of the concerns the privacy community has is that speaking anonymously is a big deal. It might not be taken well.
    - ii. One of the reasons we looked at the NSTIC strategy, is that there is a structure to allow for a range of transaction types, from anonymous to identified.
    - iii. **Mr. Gallagher:** We've talked about all these things, but we don't quite get there. What is holding us back? Is it technology, or something else?
      1. **Mr. Lee:** There are some technical challenges. They can be overcome with effort. There are also commercial barriers. It takes investment to own a large number of identities. It's not evident FIDO will win out on a voluntary base. What might the government want to do to increase adoption by the private sector? There are technical issues.
      2. Generally, there's a need to reveal the least amount of information necessary to develop trust in conducting transactions. A retail transaction requires more information to establish trust.
      3. **Mr. Palmisano:** Is the judgement that with resources and time it is solvable?
        - a. **Mr. Lee:** Yes, there is general agreement it is a benefit for all. Roughly speaking it resembles pre-internet days. People had their own network stacks, seeking their own value.
        - b. Standards and incentives created a unified internet. It seems similar to our idea of clearing houses.
        - c. There are some companies seeing value in offering complete anonymity. There is a commercial value in selling privacy. Companies want to know

- customer addresses and credit card numbers while giving people a sense of control in what they release.
- d. One of the big challenges is there are two issues: one, non-spoofable identities of end points, and how to establish and manage trust relationships among end points. There are more and more wireless devices in intensive care units. They should be communicating over encrypted channels to other devices. Many devices communicate over non-encrypted channels. It becomes difficult because of the large number of devices.
  - e. These are all symptoms of the tension between wanting more devices and managing trust relationships.
- iv. Have others talked about looking like we are migrating toward national identity mechanism (electronic national identity card)?
1. **Mr. Lin:** There are no answers, but there is a concern. It has a flavor of a national identity card. Would like Ms. Anton's input on this.
  2. Current draft language does not appear to capture this.
  3. **Ms. Wilderotter:** It highlights how challenging this subject is. What I like is the suggestion that there are great minds out there. We don't have to solve the problem, but outline the issue and recommend the right talent together.
  4. **Mr. Donilon:** The report should flag the policy issues it might raise. Is there any wisdom to be gained from prior efforts? Can staff develop some analysis that might be of help?
  5. Jeremy Grant and Ms. Todt have spoken on this. From NIST senior people, why did NSTIC have such a difficult time getting traction? There has been a strong effort to do something on this,
    - a. **Mr. Gallagher:** The National Strategy for Trusted Identities in Cyberspace (NSTIC) strategy laid out a pivot to get a solution. It called for an inter-operable trust framework. It is more functional but much more complex. It includes a range of transactions and more.
    - b. **Ms. Anton:** There has been focus on underlying technologies that can support it. It also gets into proofing. What it did, was lay out the basic framework supported by a grant program for pilot projects. It was fairly experimental. It closely tracks to Mr. Lee's assertion that the technology is less a single point technology solution, but an interoperability solution.
    - c. There is a chicken-egg problem on who would be the first mover so that the process could unfold. It is possible some of the underlying assumption (voluntary uptake), keeps coming back as one of the failures. It may not unfold to give us a workable answer soon enough.
    - d. **Mr. Lee:** About Herb's national identity issue. There is the possibility of looking at this as a state issue. We have driver licenses, and voter registration. Those are not subject to hacking because there is not commercial value in them, as there is with social security numbers.

When national IDs are raised, there is a question whether an alliance of state-managed IDs might be better.

- e. A lot of those come out of post 9-11 bills for stronger forms of identity. Voter ID movements have had backlash, because large segments of the population don't need that kind of credentials.
- f. **Mr. Lee:** Identity is so fundamental to secure cyberspace. We do seem to have technical ideas to consider. It would be frustrating if we could not find something to suggest.
- g. **Mr. Donilon;** As Maggie suggested, we can find a fundamental idea, and it can be laid out in a grand challenge mode. The paper has good things that can be cited.
- h. Regarding draft language showing comparison to credit card market and liability:
  - i. **Mr. Stine:** In today's model of credit cards, there is a shared model of liability between the consumer and the card holder.
  - ii. There is nothing similar in identity space today. The gap is the need to have that type of construct in place for identity.
  - iii. When a credit card swipes, there is private authentication. We may not have to solve every issue, only that of people using the internet.
    1. We may be able to write up a proposal for the commissioners on identity management that passes these kinds of things.
    2. **Ms. Anton:** Privacy and civil liberty concerns in this area are the largest we will encounter. We should tread cautiously. We need to determine exactly what is the problem we want to solve? There is a slippery slope in monitoring. We are suggesting creating yet another national database when we don't know this is the approach. It can promote discrimination and harassment.
    3. **Mr. Lee:** One of the President's motivations for our work was identity theft. The impact on the economy, and people's sense of safety and security is one thing we are trying to solve. There has to be some way for people to be in control of how much of their information is revealed to other parties. Personal identity information revealed to vendors should be the minimum required to do transactions.
      - a. **Mr. Lin:** What you suggest implies an equal power relationship. There may be voluntary situations, but it is not always the case. Annie has a point that must be addressed.
      - b. If we assume this is less technical, and more about business innovation.
      - c. This foundation cited in the recommendation that pools liability and defines limits for those in the eco system and

- be subject to certain requirements such as minimum exposure, etc. Could that be enough to drive early adoption?
- d. **Mr. Gallagher:** We need something to drive innovations. It could involve private sector identity brokers. It could be a powerful way to push this.
4. It involves how to increase consumer demand through awareness and easier solutions for a variety of online transactions.
  5. The foundation could have a number of functions. It could be a customer advocate. It might also hold certification. It may ensure quality control. It put some muscle in a voluntary system.
  6. There are a series of issues: Businesses, civil liberties, and privacy. There needs to be some way to ensure integrity of networks. Need a recommendation to drive policy and technologies. The individual decides what they provide. There must be some way to ensure identities of individuals for transactions.
  7. **Ms. Anton:** It is a great example of why we need a chief privacy officer for the government, possibly OMB.
  8. **Mr. Donilon:** We could have a recommendation from the commission. Thoughts on the privacy position in the draft?
    - a. **Mr. Alexander:** More along the lines of, just because something is legal, doesn't mean we should do it. We need someone in the government to advocate that idea.
    - b. In the system we are talking about, does that get us in a zone where a chief privacy officer could work with it? Yes, it gets in the right direction.
  9. **Mr. Lin:** It doesn't really say people don't have to use this system at all. There is a community that will object to use of any mandatory system.
  10. **Mr. Stine:** Opting in is not expressed as clearly in the draft section as it could be. It was implied in Mr. Alexander's comments. Mr. Lin has a good point.
  11. **Mr. Lin:** It must be discussed in terms of factors of power.
  12. Any sense of US government control over identities in cyberspace operates in a global context. We should be aware of the appearances of what we're doing outside the US.
  13. **Mr. Lin:** Can the US government revoke credentials and make people disappear?

- a. **Mr. Donilon:** If the government bans the use of individuals or groups who are planning attacks, what would the posture be?
- b. As Mr. Lee said, the Executive Order directs us to talk about identity management. Are there other concepts or ideas we should discuss?
  - i. There are other activities that could be done in the short term.
  - ii. Staff has other proposed recommendations that were distributed early in the process, such as retailers offering multi-factor identity solutions. Others can be distributed to spark discussion.
  - iii. Can staff talk to Jeremy Grant on trusted identity management in the machine context? Perhaps set up a joint briefing from Mr. Grant and the current director of the program.
- c. **Mr. Lee:** The proposed recommendations given here head in the right direction of trying to unify mainly private sector identity management systems.
- d. Perhaps the point of the moonshot was to think harder about boldness. I was trying to take a more user centric approach.
- e. What might be missing is crystalizing the ultimate benefit to individuals and national cybersecurity.
- iv. **Mr. Palmisano:** Taking a step back, its' much better than what we have today.

### III. Next steps/Wrap-Up

- a. **Ms. Todt:** We will turn revisions on this topic around in the next seven days. Will ensure draft sections get out to the commissioners to check that we have captured key ideas. Will follow up if there are any outstanding issues.
  - i. **Mr. Chabinsky:** We have an opportunity. The areas of greatest need of the country have the lowest privacy impact. We can roll out some of those areas and some suggested privacy recommendations.
  - ii. **Ms. Todt:** I will send email regarding cancelling the New America event due to Federal Advisory Committee Act implications.
  - iii. Rigorous revisions to the draft are in process, any further submissions from the commission are welcome.