Meeting Minutes

Attendees:

Commissioners: Tom Donilon, Heather Murren, Pat Gallagher, Herb Lin, Annie Anton, Peter Lee

NIST and Others: Kiersten Todt, Kevin Stine, Matt Scholl, Matt Barrett, Robin Drake, Alex Niejelow (for Ajay Banga), Amy Mahn

Agenda:

I. Public Awareness Discussion led by Kevin Stine
II. Questions and Discussion
III. Next Steps/Wrap-Up

Discussion

1. **Public Awareness Discussion led by Kevin Stine**
   a. We briefed the commission earlier, and the feedback at that time was to make the proposed recommendations more presidential. We have taken input from multiple sources, and added more from the public discussions. We have the following possible recommendations for the commission to consider:
      i. At a high level, the next president should launch a campaign aimed at a wide audience.
      ii. The White House should convene a summit on public awareness in the first 100 days of the new administration. President Bush designated October as National Cybersecurity Awareness Month. It continued in the Obama administration.
      iii. Points from Ms. Murren's paper - There are organizations that exist that are good at creating this type of content. It would be in the interest of the commission to use them. Should particularly consider the Red Cross material for disaster preparedness.
      iv. It is an inter-disciplinary space. If the President did have an announcement in the first 100 days, Education, and other agencies should be included.
   b. The President should name a single agency to lead the initiative.
      i. DHS and others have roles here.
   c. We have had different campaigns in the last few years. The most notable being "Stop.Think,.Connect". There are activities under the Cybersecurity National Action Plan (CNAP) that also relate.
   d. Propose a recommendation to fund an organization through the grant process. There are many private sector participants who support these types of efforts. DHS

is going through a re-up of its grant process, to expand and reinvigorate the existing campaign.

e. The Peiter (Mudge) and Sara Zatko labelling idea as testified about from the Minnesota meeting - It may warrant its own sub-bullet in the report.

f. Calls for a series of targeted six-month campaigns. CNAP has related ideas. The White House announced the "Lock Down Your Login" campaign and moved toward multi-factor authentication. There is a video with dancing bananas and sharks focusing on authentication. There will be private sector entities that are supporting the effort announced by the White House, including MasterCard.

g. At the meeting in Houston, there was public comment to the commission on the complexity of the cybersecurity space, to the effect that more than one campaign may be needed to adequately spread the message.

h. Propose a recommendation to begin a series of campaigns on safe coding practices. It is new, different and very important. It is important to consider. Building it right, and having greater impact by building better technology.

i. Tom Donahue brought up at the American University DC meeting the concept of making it easy to do the right thing, hard to do wrong thing, and easy to revert back to the right thing.

j. Finding the right words to the right audience in the right way is important.

2. **Questions and Discussion**
    a. **Ms. Murren:** The draft paper accurately characterized my thinking. It may be a way to simplify the buckets in the consumer space. The paper does a good job in laying out the right things. It's a matter of narrowing what we want to say.
    b. Mr. Lin sent a note focusing on consumer conduct and easy to use technology.
        i. There is a debate on teaching consumers to be more safe vs. not, it's too complex for consumers to understand.
            1. Why are systems set up in a way that imposes tension on consumers making choices?
                a. Generally consumers are aware of the need for security. However, decisions in specific situations can be difficult.
                b. **Ms. Murren:** The conditions are not mutually exclusive. Informing consumers is important. Informing them should happen regardless of what happens with technology. It is best for everyone if consumers participate in self-protection, it is good for everyone.
            2. If it takes a series of campaigns for consumers to be educated, what that means becomes somewhat scary.
                a. The safe choice in a situation like that, is not to make a choice, even if it means going without a service.
                    1. Mandatory wording in software gets to be dicey.

2. At what point can software become a utility? Mandatory language on software products is difficult.

b. **Ms. Anton:** Regarding mandatory campaigns for coders - It should not be on the consumer to control these choices. It is an interesting path in terms of what we can do, and are we expecting too much from consumers? Maybe calling software a utility would enable us to support them better.

c. **Mr. Lee:** On the technology side, I don't know how to even start. If we go to Linux OS, in internet of things, does that meet the bar?

d. We might think about a shared responsibility. Does it resonate with software as utility?

e. **Ms. Todt:** Where is the burden, and where are the conduct changes most effectively placed?

f. **Mr. Donilon:** Is this an effective thing to do in terms of consumer education?

   i. Effectiveness of education?

   ii. There is a consumer protection aspect. It includes things like the Mudge-Sara Zatko nutrition label proposal. It is a consumer information issue that would be useful.

   iii. How to encourage security by design, it does lead to better consumer protection. Reducing errors in code.

   iv. There is also an R&D piece. Tom Donohue touched on an R&D agenda that makes it easier for people to do the right thing, and avoid the bad thing.

   v. It can make people more biased toward doing the right thing. It underscores the need for research in anything we propose.

g. **Ms. Todt:** Is there consensus on to consider the proposed nutrition label approach? It should not be framed as mandatory, but rather, a "consumer report" type approach. Informational for consumers, information and market impact.

   i. **Mr. Lee:** The labelling concept is feasible with the right public awareness. Can we spark viral adoption by vendors for this type of labelling? It has the potential to be very useful.

   ii. **Mr. Gallagher:** We are acknowledging humans have a part in the system. It is still devoid of actionable recommendations. It is too focused on awareness. There may be more actionable items to focus on. A market incentive model might help the process. Is there a usability standards framework that applies to security? It might get to Mr. Lee's concern, it can be a one size fits all. The reasoning is good, though.

iii. **Mr. Donilon:** Staff should look at what we might have in the ecosystem of usability and R&D. We can certainly point out the harms to consumers of insecure software. Perhaps NIST might begin a project on software standards.

iv. It speaks to the level of care for software. It ought to come from industry. NIST might provide the authority to convene a group to do this. The Software Engineering Association in cooperation with industry.

v. Engineering has standards for physical infrastructure. Why wouldn't we push for standards in software like there are in other engineering practices?

vi. It's not software per se, but connected devices that are the target of risk.

1. Many hackers develop exploits for Xbox. You can get physical templates for cutting the right wires to enable cheating.
2. People also use x-ray devices to extract keys. It is not unique to Xbox. It extends to other kinds of devices and software.
3. **Mr. Lee:** It is primarily software that may be susceptible to attack to compromise connected devices. It is too narrow and too broad at the same time. It is difficult to determine what appropriate standards would look like.

vii. **Mr. Gallagher:** Is there an analogue of the professional engineering license in software? Professional engineering can provide a certification. It has been studied.

viii. The conclusion of the study was that the certification may have benefits in certain areas, but excludes many people.

ix. For Microsoft, it is human usability. Microsoft probably has spent a lot of time on usability. Is it an area of study worth identifying? There is an academic community. One of the leaders is Lorrie Cranor of

Carnegie Mellon. Her work has been influential. Getting behavior to change may be difficult. Part of the required annual training of every employee, is training on cyber, including how to handle phishing and those types of attacks. It supports the idea that public awareness has value.

x. Lorrie Cranor has written on privacy. It may be good to have her speak to the commission.

xi. **Mr. Lee:** We need to remember the testimony from Defense Advanced Research Projects Agency (DARPA) and National Security Agency (NSA) from the last hearing. Automated software checking is an R&D priority.

xii. **Ms. Murren:** A lot of what we're talking about will require a lot of investment for government and others. There will need to be some public support for those efforts. Public awareness needs support, and will provide a platform for additional support.

xiii. **Mr. Donilon:** We also have testimony from Ted Schlein. He has been pressing for a numerical assessment system for some time. Does that add to the labeling idea?

xiv. **Ms. Murren:** Usability testing can be in support of consumer report awareness.

xv. Staff should provide more specificity in the content on what the proposed campaign might be.

h. Other questions? We have several potentially important proposed recommendations. We may not need to arbitrate what level of consumer awareness is needed now. Calling for awareness is important now. Setting standards in the industry is tremendous, if it can be accomplished.

i. Have we circulated Mike Daniel's new ideas? Clean pipes initiative - builds on Rob Knake's paper from a year ago. Having the ISPs be responsible in some way for known malicious activities in their infrastructure. The White House has talked to the FTC about this. The commission can expect proposed recommendations to provide clean networks as utilities provide clean infrastructure.

j. **Mr. Lin:** The mandate is half the battle. Some subsidy might be needed to assist with cleaning up. The same requirements need to be imposed on all.

k. It came up in some of the discussions. The tragedy of the commons applies. They all need to do it or not. Since we are controlling traffic, they will want appropriate liability protection. It seems a good idea. The implementation would need to be uniform.

i. It is an interesting idea. There are governments that do this and do it well. Having clear boundaries, and a clear way to talk about it to steer it away from seeming like oppressive regimes. Staff can do further research.

l. US Telecommunications council and others will have positions.

3. Next steps/Wrap-Up

a. Ms. Todt will send out an email with workforce and IOT revisions.

b. Staff will revise draft language for public awareness based on today's discussion. There will be a new draft for the 17th. Before then, Ms. Todt will be provide sections to the commission for review.

c. There will be an October19th meeting in DC with conference call capability.

d. Finalizing the date of a final public meeting to be held around Nov 18-22nd approximately.

i. The final public meeting will raise findings from preparatory working groups to the commission. It is not a validation of recommendations. It will approve all remaining unapproved minutes. It will not expose the content of final report prior to delivery to the President. It will receive and approve content from the working groups.

ii. Remaining sections to be discussed: Critical Infrastructure, State and Local, R&D, insurance, International. There will be some carryover on topics past the 18th.

iii. Some standout sections: Have gotten good testimony on extending the NIST framework, and extend through the federal government, industry and to small and medium sized business. Mr. Gallagher had some notes on extending the framework. We don't want to lose that information. It could appear in the report somewhere. Staff will work to incorporate language into draft report.