Meeting Minutes

Attendees:

Commissioners: Tom Donilon, Sam Palmisano, Pat Gallagher, Steve Chabinsky, Keith Alexander, Herb Lin, Peter Lee, Keith Alexander, Ajay Banga

Others: Kiersten Todt, Kevin Stine, Adam Sedgewick, Eric Goldstein, Ben Scribner, Princess Young, Michael Kaiser (NCSA), Clete Johnson, Amy Mahn, Robin Drake

Agenda:

I. Discussion of the Public Awareness Working Paper led by Kevin Stine
II. Discussion of the Governance working paper led by Adam Sedgewick and Eric Goldstein
III. Next Steps/Wrap-up

Discussion

I. **Discussion of the Public Awareness Working Paper led by Kevin Stine**
   a. Public awareness is one of the areas that has received significant discussion over the course of the commission workshops. It has received a good bit of attention from industry as well.
   b. We want to understand the landscape of what is occurring today, and talk about challenges and initiatives.
   c. **Mr. Scribner:** It is a complex and challenging area. We have seen that 17.6 million people had their identities stolen in 2014. Smaller business can be driven out of business by cybersecurity threats. Organizations can only do so much to mitigate threats themselves. They need assistance.
      i. This is why awareness is such an important thing. Complexity is growing, it makes it hard to stay ahead of the challenges in this area. There are many programs taking place that are putting out great information to help communities from an awareness perspective.
   d. There is a spectrum of programs but there can be conflicting information given to the public. Government can play a role in what guiding information should be followed.
   e. The information in the discussion paper presents a range of topics.
      i. National Cyber Security Awareness Month is trying to highlight the work that is taking place.
   f. Stop.Think.Connect has been very involved.
      i. The approach has been about disseminating harmonized messages.
      ii. We are moving to a digital culture. The market place is quite large. We need to get the right messages to people about what they can do.
      iii. We feel we have gotten some good results. There are thousands of organizations participating, with 700 partners, nationally and internationally.
   g. Questions on the Public Awareness working paper
      i. **Mr. Gallagher:** What about outcomes? A lot of the analogies of effective campaigns have clear, distinctive goals. How clear is the goal here, and how do we assess progress?
         1. **Mr. Kaiser:** From the NCSA perspective, we send the messages, and look for behavior changes, but it is harder to assess. We do polls, and look at the

results. A new poll says younger people have a good understanding of the cyber message. Measuring behavior change is harder. We do see some evidence of change, but there is no easy way to measure it.

2. **Mr. Scribner:** Stop.Think.Connect and the cyber security awareness month represent broad national campaigns. We are also looking at more targeted campaigns. We try to have simple and clear goals, with more measurable results. It is challenging, because cyber is so broad. It impacts our lives broadly. Determining how those impacts relate to campaigns is the challenge.
3. **Mr. Banga:** On targeted campaigns, if we think of multiple messages, what are the simple messages for consumers? Possibly hygiene first; urging the use of strong passwords are easy, urging frequent password changes is harder. Getting measurement for how frequently passwords get changed may be accomplished by reaching out to banks who track this information. Is this part of what we should be looking at? There is the issue of getting companies involved, but small and medium business involvement is a challenge. It can be a new idea even for larger companies.
    a. **Mr. Kaiser:** There are a couple of things. We look at technical and aspirational architecture. Keeping machines clean, and how do we inspire people to do that.
    b. **Mr. Kaiser:** The industry being able to provide metrics. Industry doesn't want to report bad news. Perhaps neutral parties can gather and report that data. We are looking at ways to report that data. We are looking for a culture change. Instead of making it negative, we can cast incident reporting as in our best interest. Then we might get more.
4. **Mr. Donilon:** The proposed recommendations in the language are too small in scope. We need thinking on the level of what the next president should do. A piece of what the next administration does in cybersecurity will include awareness. We need something much bigger and bolder than what the paper has.
5. **Mr. Banga:** Small and medium businesses need to be involved. I'm thinking of the public statement yesterday. There should be a communication effort targeted at small and medium business. What can they do that is fundamental? The point yesterday was to make it a national responsibility.
6. **Mr. Donilon;** It should be a new campaign the new president can announce. It should be a persistent, multi-year campaign with targeted elements that include small and medium businesses. The hard challenge is we've heard this is important for the country. We aren't yet doing everything we could be doing. We have the opportunity to have it launched by a new president.
7. **Mr. Kaiser:** We can make a recommendation for that. We need also to make long term goals. The Smokey the Bear campaign has been around a very long time. It should be portrayed as a society issue; we need cyber in order to function successfully in society. Every government agency should be sending the same message. The private sector can also be involved via incentives. We must finally reach everyone.
8. **Mr. Gallagher:** The language does not make presidential recommendations. We can sharpen it up to be goal oriented. People must understand the threats, and know what to do against those threats. The Smokey campaign was compelling. It pointed out risk and what to do. It clarified what people should understand about threats and what they can do.

9. **Mr. Lee:** Thinking about the transition process, where are accountabilities and who would focus on the transition in first 100 days?
10. **Mr. Donilon:** No matter who wins, cybersecurity must be a focus. A new president needs a set of propositions to embrace. Process and measuring effectiveness must be clear. What behaviors being influenced must be clear and be presidential.
    i. **Mr. Kaiser:** There is shared vested interest in cyber. Everyone gets that it is a team project. A safe internet is in everyone's interest. There are many willing partners. There is a very clear interest here to prevent a downward spiral to less security.
        a. **Ms. Todt:** The challenge is there is no binary message. The Ad Council was discussed yesterday. They have had success with public-private partnerships.
        b. **Mr. Kaiser:** We worked with 25 companies, and government agencies doing Stop.Think.Connect. Arriving at an ad campaign will involve marketing research. The Ad Council was not willing to make the investment in the past, but may be now. We need all resources at the table to solve this problem.
        c. **Mr. Donilon:** The commission should not be constrained by willingness. We should propose what is most effective. The President has the ability to overrule willingness issues. The president can accept or reject what we recommend, but they should have our best effort.
11. Heather wrote a great paper on these topics. It is worth reviewing.

II. **Discussion of the Governance Working Paper led by Adam Sedgewick and Eric Goldstein**

a. Overview of findings: We have two papers with the commission. One is a summary, and the other is a deeper overview done by Kate Charlet, Department of Defense.
b. The scope of the challenge for the government: Spending on IT is estimated at ninety billion dollars and includes approximately fourteen billion dollars for cybersecurity. There is debate over the accuracy of these numbers.
c. Government is perceived as a laggard in cybersecurity. We are trying to change that image.
d. We can consider taking advantage of the current marketplace, and how to shape the future.
e. There has been a good discussion of centralization of authorities. Authority is generally covered by the Federal Information Security Management Act (FISMA). Agency heads have the responsibility for protecting their agency information. FISMA gives audit authority to inspectors general offices.
f. Procurement and budget are challenges. Management structures are confusing. We also hear about getting the right people. Recruiting and competing with the private sector

i. Key topics: To what degree mandates are effective, and to what degree enforcement should be centralized.
    1. Many agree the current structure is not effective. Any entity with enforcement authority has enough info to actually enforce.
    2. What is the trigger for enforcement and how does it work.
    3. DHS issues binding operational directives. Two directives have been issued thus far, and been successful. The key to the success was granular and independent data on which to base enforcement action.

4. Agencies should report accurate data to authorities.
    a. OMB has budget authority. That authority is tied to the budget cycle.
    b. GAO has audit authority via the inspectors general offices.
    c. DHS enforces the FISMA power of compliance.

g. What other methods of enforcement are there?
    i. Restricting internet access at the agency level for non-compliance. There are immediate implications for budget.
    ii. **Mr. Chabinsky:** Noted the possibility to take agencies into receivership. Replacing an agency CIO is a possible method, but may not solve immediate issues.

h. Discussion on the Governance working paper
    i. **Mr. Lin:** The Federal government is just as complex and private sector and then some. We can't "command and control" into the private sector. Why is that the right way to do that for the federal government?
        1. **Mr. Goldstein:** Centralizing authority in one agency may not have results. Compliance with the president may be a bit different issue. A chief information officer (CIO) or chief operating officer (COO) acting to gain compliance of subordinates is different from something coming down from the President.
        2. **Mr. Alexander:** Promoting risk management framework where security operations are not separated and are brought into C-suite.
        3. The real issue is accountability in risk context. We may have a problem of missing authority, and how to use the authority we have.
        4. It's not clear that having power works without a basis to use the power. Congress and others have a role in the budget process above the agencies. There has never been an effort to work with Congress to modify budgets based on security performance.
            a. The enforcement angle is not necessarily the one to use. We talk too much about who is in charge. FISMA has the authority, and the President is in charge.
            b. The government has not federalized the responsibility. Agency roles are not well defined. In operations and architecture we do a bad job. Some things make sense at the agency level, some are closer to infrastructure.
            c. **Mr. Alexander:** It is not clear what is assigned under normal ops, and during incidents. It is fundamental. OPM the agency was hacked, but it was an attack on the govt.
        5. **Mr. Palmisano:** I cannot explain the strategy or plan of action for operations or incidents. There is no written strategy or plan. We never get out of the weeds to focus on the goal of what we want to accomplish.
        6. Network operations are a place where central authority makes a lot of sense. There is an intrinsic authority that comes with that kind of role.
            a. An authority to operate (ATO) implies an authority is present. Using that authority to enforce cybersecurity is problematic.
            b. **Mr. Gallagher:** It breaks the relationship between IT and delivery of the mission. The White House will not support cutting off an agency supplying a critical mission. We must map out

responsibility for normal and extraordinary circumstances. Analysis should reveal what is needed.

7. **Mr. Lin:** The paper addresses procurement and points out acquisition gets in the way of IT procurement. Having talked to many people, the system does have some flexibility, and more often it is not used. Some people know how to make the system work for them. It is possible, but takes some bureaucratic insurgency. There is an important question. How do we get those who use the system effectively to share their knowledge, rather than only going the route of legislation?
   a. **Mr. Sedgewick:** Often there is flexibility but it involves a lot of people accepting risk. There is a more fundamental issue, in how things are funded by Congress. It is easier to fund missions rather than to fund management. We are working with a GSA detailee to develop this topic further.
   b. **Mr. Lin:** Procurement and acquisitions systems can get in the way of doing things.
   c. **Mr. Alexander:** The problem was never inflexibility, but priorities. There are many competing authorities. It comes down to the risk management and accountability not being right. I would rather see cyber integrated into program funding, rather than having specific financial buckets. It makes for immediate accountability for those using the money. We need not to split responsibilities.
8. **Mr. Donilon;** Staff should look at past priorities. We have a goal to protect the federal network, and to make it a model not a problem. Agencies do not have experience and capability in top-down and direct enforcement. There needs to be a methodology and standard for the government. On procedure, there is a lack of cybersecurity process experts.
   a. Ted Schlein in his testimony before the commission in California, used NIST, etc. as examples. The issue is culture and accountability and leadership. The President can lay it out to the Cabinet secretaries.
   b. The issue exists for the government to extend NIST. There is a longer list of things we can dig into. Roles and responsibilities, and structure needs to have clarity. Arriving at a baseline is a place to start. Leadership and accountability must be front and center.
   c. **Mr. Gallagher:** On incident recovery, there is no cyber recovery authority (like a cyber-FEMA) to respond to major events. There would be a visible person to point to in the case of events. Then states know where to turn as well. It must not be an enforcement agency. There is a need to emphasize personal accountability. Help is needed now for the agencies.
9. Mr. Gallagher will provide cyber-FEMA thoughts to the commissioners by email. Most agencies will not have the capability without assistance. Disaster recovery becomes disaster resilience. Lessons learned can then be shared with everyone else.

Investigations are done at the network level, but we also need investigation to define attribution.

10. **Mr. Lee:** There is a built in opportunity to learn and improve. I'm not hearing the word "innovation," and no talk about culture change. Industry has had to quantify risk taking to embrace new technologies in order to stay at the leading edge. Bad actors embrace innovation whole-heartedly. We need to encourage technology innovation.

III. Next Steps/Wrap – Up

a. **Ms. Todt:** Thanks for everyone part in the call yesterday. Two more papers with draft proposed recommendations to be reviewed next week. Minutes will be distributed for review and feedback as soon as possible.