# Meeting Minutes

## Attendees:

**Commissioners:** Tom Donilon, Peter Lee, Steve Chabinsky, Heather Murren, Joe Sullivan, Keith Alexander, Herb Lin, Ajay Banga, Annie Anton, Pat Gallagher

**Others**: Kiersten Todt, Mike Daniel, Tony Scott, Dan Prieto, Ed Felten, Grant Schneider, Andy Grotto, Adam Sedgewick, Amy Mahn, Donna Dodson, Kimberley Raleigh, Robin Drake

## Agenda:

I. White House Briefing on Federal Governance and Critical Infrastructure
II. Near Term Overview
III. Next Steps/Wrap-Up

## Discussion

**I. White House Briefing on Federal Governance and Critical Infrastructure led by Michael Daniel, Tony Scott, Dan Prieto, Ed Felten**

a) **Mr. Daniel:** Today's briefing will serve to take a step back and get a sense of where we are with issues we've been working on. We will also look at some of the big ideas from last week's briefing.
   i) We have made many strides over the course of the administration, but especially in the last five or six years. Coordination mechanisms have significantly improved at the Executive Office of the President (EOP) level, and elsewhere. Other agencies have matured as well. The FBI has solidified its cyber division, and more mature roles exist across the board. We have the Cybersecurity National Action Plan (CNAP).
   ii) In policy, great strides have been made too. Statutory policy, the Federal Information Technology Acquisition Reform Act (FITARA), policy for chief information officers (CIOs) and Federal Information Security Modernization Act (FISMA) reform passed last year. There are a string of Executive Orders, and other actions. Guidance on many topics has substantially improved. Cyber operations have improved, and there are new tools for cyber sanctions and cyber risk management.
   iii) There are new strategies for workforce development. The policy framework is now in place.
   iv) We have laid a good foundation in terms of capabilities that we can make available, like continuous diagnostics and mitigation to better protect what we have. The key is the foundation, but we will be talking about continuing to expand capabilities and get them deployed.
      (1) From the standpoint of expanding capabilities, there is much maturation. That is the good news. The downside is, the work is incomplete.
      (2) We still need to get the National Protection and Programs Directorate (NPPD) transitioned into a national cyber protection agency. The Cyber Threat Intelligence Integration Center (CTIIC) needs more resources. It needs to be somewhat larger than it is now.

(3) We need to rethink about how we employ these policies and carry out operating federal cybersecurity enterprises.

v) All these things led to the discussion last week. We announced the first Federal Chief Information Security Officer (CISO) and Deputy Federal CISO appointees. Later this month, we will launch the new consumer campaign, "Lock Down Your Login."

b) Current Ideas: Federal Cybersecurity and Critical Infrastructure.

i) In federal cybersecurity the biggest question is centralization vs. decentralization of capabilities

(1) At present, we are too decentralized to manage risk effectively.

(2) Moving to a centralized IT for the federal government is not the right way to go either. How do we hit the right balance? The real question is where to put the line.

(a) Traditionally we have had a very stove piped view of cybersecurity. Each agency has had its own version of cybersecurity.

(3) We need to start breaking the stack and thinking of it in a different way. What layers should be centralized?

(4) Network and transport layers should be centralized for federal civilian agencies. All agencies must plug into that layer. DHS and OMB together will enforce compliance if that is necessary.

(5) This way there is a much more centralized way to do cybersecurity.

(6) Mission applications remain at the agency level. Agencies must still protect their information. Agency CIOs may not be as interested in the transport layer. Agencies can focus more on their mission if the transport level is left to security experts.

ii) We have been looking at whether different sized agencies should be treated differently. Agencies smaller than a certain size may be connected a network for smaller agencies. This collects IT services for those agencies.

iii) How many commodity services can be done across the government? Log-ins and email may be candidates for consolidation. We can accomplish more centralization than we have done.

c) Budget and Acquisition

i) There is the idea of the Information Technology Modernization Fund (ITMF). The very way budgeting is done works against trying to create cybersecurity. It is easier to get dollars for old systems. It is extremely difficult to get money for new systems.

ii) It means taking on the budgeting process and the appropriations process on the congressional side. We will be asking some agencies to take on certain functions for the entire federal government and fund them.

iii) It's not just dollars for new investments that are hard to get. Money for maintenance can be hard to get too. Often CIOs must literally beg for those dollars. It is the nature of money and its governance. It makes for a significant barrier to progress.

iv) The way the acquisition and procurement works makes it very challenging. There may be things to look at in federal IT procurement differences across agencies.

v) Is it possible to start from a different proposition? Let's start new and say, what we want to bring in. Can we make a case information technology is fundamentally different than other areas?

vi) Contract Protest Discussion
(1) The idea for any contract to be contested, and have that protest go on for extreme amounts of time makes it impossible for the government to finish anything. There are areas there that can be looked at productively.
(2) **Mr. Lin:** Is there a penalty attached to protest process?
(a) Currently, there are no penalties for protestors at all.
(b) Protest becomes a mechanism for users to exploit the process and they liberally apply the exploitation. If we look at those areas, they may be fruitful to examine.

d) Critical Infrastructure Highlights
i) One of the fundamental questions to ask from the government side is, what is the value of naming critical infrastructure sectors?
ii) In terms of resource allocation decisions it is easier for the government, for industry it is less clear.
iii) Should there be a grant structure for small and medium business? Can the government provide what is needed?
iv) The other thing we need to look at is the value proposition, and how we can best use government assets. If we look at resource allocation for the government, we have made a large investment.
v) There is more money allocated for DoD cyber defense, than all other critical infrastructure sector areas combined. The commission should look at a civilian cyber campus. There is a case for co-locating functions on the civilian side of the government.
vi) We need to create a government wide set of principles for the federal government to judge cybersecurity activities of agencies against.

e) Legacy Systems and Challenges
i) It is important to not underestimate the problem created by the old legacy IT that exists in the federal government.
ii) It is costly to operate and maintain and secure. There are fewer people to operate older, less used systems.
iii) **Mr. Scott:** We must facilitate, upgrade, and replace infrastructure. The ITMF will have a part to play in this. The other is in CNAP, but inspired by the Baldridge quality recognition.
(1) We will be launching an initiative in the fall to improve quality in multiple sectors. It goes back to the effort to changing the perception of lack of quality in American-made cars.
(2) We will attempt to do a similar recognition to Baldridge, but for cyber security. It will recognize efforts to improve security using Six Sigma methodologies for process improvement. I would encourage commission support of this effort.
(3) Major consulting firms have endorsed the effort, and are looking for ways to encourage efforts.
(4) **Mr. Felten**: We have made a lot of progress. The CNAP was designed and built with the assumption to get something big started in a short time, and with the commission to carry that progress into the future.

f) Integration and Planning

i) Three main points: First, the need to make sure we have good integration between cyber and technology efforts more broadly in the government.
   (1) There is a tendency by agencies to treat cybersecurity as separate from the technology they are building. This gets into a wrong mindset. Cybersecurity and technology should be treated together.
   (2) Second, there is the opportunity, when done right, to design systems and policies with cybersecurity in mind. The ITMF will make a difference here. Once we have money and authority and people to do this, we will be able to be proactive to do these things.
   (3) Third, as we do this, we should think about how the technology should be. We must be future oriented, rather than being behind or eternally playing catching up.

g) Commission Questions and Discussion
   i) Is the ITMF new money or a working capital fund? In the original conception, it was a one-time 3b fund for groups of agencies to propose uses for, and later pay back the fund.
   ii) **Mr. Lin:** If someone from GSA scoped out Mr. Daniels' idea - What would that look like?
   iii) To expand on that, if there is a set of proposed reforms, it would be good to know what they are. The White House will assist with developing a set of proposed reforms. The White House will reach out to GSA to coordinate.
   iv) **Mr. Alexander:** The government should lead the way for cybersecurity for the nation. We should think more about prevention than increasing response. Progress today pushes on intelligence community response. We need to focus on prevention for the nation as a whole. It takes time, but we should have the vision to have that capability. On the idea of a cyber university, we can advocate service for tuition.
   v) We considered the service for tuition idea, but couldn't get it over the Hill. It is in CNAP, to have those who graduate from accredited universities to have some assistance. It would be a step forward.
   vi) We should consider a physical co-location on a federal FBI-DHS campus working with civilian side.
   vii) We may walk through protective measures, and discuss with staff. All the discussion with senior management in government says we solved the problem, but there are more specifics.
   viii) On students and loan forgiveness, the private sector may want to collaborate on these types of efforts, not just loan forgiveness but opportunities.
   ix) Explain the concept of unplugging if an agency is not compliant. The analogy is the Defense Information Systems Agency (DISA) for DOD. We often see disagreement on what is implemented. Unless these certain activities are done by an agency, we will consider disconnecting it until they are. It's meant to help people to think of enterprise wise cybersecurity. It gives DHS more tools. It has worked successfully on the Defense side as an incentive.
   x) Regarding students, what's been said will bring people in at the junior level. We also need opportunities for senior level people.

xi) One of the themes is designing for security at the start. It all speaks to embracing innovation more. Are there ways to approach this? Are there ways to encourage agencies to take some technical risks in order to embrace innovations?

xii) Ultimately, for that model to work, agencies must see the value proposition or they will not support change. There is too much room for slippage otherwise.

xiii) **Mr. Lin:** A key question is agency vs non-agency risk. We talked about Federal Acquisition Regulation (FAR). Companies are overly focused on compliance and protests. There is room in there, but they don't focus on reducing enterprise risk. FAR really wants to us to think about reducing risk. Regarding enterprise risk, FISMA says agencies own enterprise risk. There are things in FISMA and FAR that allow innovation and better processes.

xiv) Existing processes say everything we do must be needed. Proposals from companies often turn into requests for proposals (RFPs), and then they are competed.

xv) **Mr. Lin:** Are there ideas on incentives that could be provided? There are positive incentives. But also reducing risk of protests, and other ideas, can make things easier with acquisition. There is misinterpretation of current guidance. There are a few acquisition officers who make the system work - what can we learn from them?

xvi) There is a lot that can be done here. It's on the commission. We can do new things, but we have to do the basics too. The federal government has been very slow. We can set a number of baseline ideas that will have an effect.

xvii) Some of the administrative barriers can get in the way of rolling out shared services.

(1) There is a concern on the part of CIOs, that if they are outsourcing something they are responsible. They are still accountable for their agency.

(2) The second part is the budget process, and how they are divided on the Hill. It makes a reluctance to try to move money across silos. There could be resistance. How do we knock those things down to do shared services?

xviii) Ms. Todt will collect follow-up questions from the commissioners, and forward to the White House group.

xix) To follow up, it would be very useful for Mr. Daniel and his team to make specific recommendations from the whole list of items discussed today. It would be useful for them to take the next step for the commission and present ideas.

II **Next Steps/Wrap-Up**

a) Conclusion- A lot of material was covered today. The challenge for next week is to frame this by category and choices for recommendations for next week's discussion.

b) Overview of Next Week –

i) Monday the 19th is the commission meeting at American University Law School. It will run similarly to the other workshops.

ii) Tuesday the 20th is a closed preparatory working group meeting.

(1) The meeting is scheduled from 9 a.m.-2 p.m. to look at proposed recommendations, particularly on governance. There will be no public presence. Commission and staff only will be present at that meeting.