Meeting Minutes

Attendees:

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

Others: Kiersten Todt, Matt Barrett, Eric Goldstein, Amy Mahn, Robin Drake, Clete Johnson, Heather King

Agenda:

I.   Discussion of Critical Infrastructure led by Matt Barrett
II.   Questions on Critical Infrastructure (CI)
III.   Discussion of Recommendations for State, Local, Tribal and Territories (SLTT) led by Eric Goldstein
IV.   Questions on SLTT
V.   Financial Sector Discussion Led by Sam Palmisano
VI.   Next Steps/Wrap-up

Discussion

I.   Discussion of Critical Infrastructure led by Matt Barrett

   i.   Mr. Donilon had some thoughts from the White House on clean pipes from internet service providers. These as well as Michael Daniel's thoughts on response and recovery have since been incorporated into draft language.

   ii.   The work group is also reconciling Mr. Gallagher's framework email to the document.

   iii. Mr. Barrett provided content to Ms. Todt Friday, October 7th that affects seven sections of the draft report. There had been redundancies and inconsistencies in the draft in the CI and cyber insurance sections that have been reconciled.

   iv.   One proposed recommendation related to capability for response and recovery.

            1. Mr. Goldstein mentioned that in terms of establishing a cyber crime center, the commission should consider the costs of having one place handle all sectors or establish one per sector, as there are costs and benefits to both options.

   v.   Proposed recommendation for classified connectivity for Section 9 companies – It typically takes two years to get a SIPRNet drop. In many cases, a federal contract is required to get classified connections. Mr. Barrett asked if the Section 9 designation was too narrow and if the commission would like to consider broadening this recommendation.

    vi.   The group is deriving a model based on Section 9 companies, and the commission could consider the downstream implications, since funding might be addressed upstream.
1. Questions asked: Will people pay under that model? Or will they wait until the government pays?
2. DHS is still considering providing indicators to the private sector. Is there also related value to putting classified infrastructure over Section 9 companies?
3. Mr. Goldstein noted the commission should consider the issue of how to measure value of giving classified connectivity to the private sector and whether it is worth significant cost of buying Enhanced Cybersecurity Services (ECS).

    vii.   A proposed recommendation was raised addressing closing gaps in governance and authority.

    viii.   A proposed recommendation is being expanded based on Mr. Gallagher's thoughts in a draft right now. The draft recommendation may possibly move to the "innovation promotion" section. The Office of Regulatory Affairs may be helpful with rules and may want to add language on circumstances where conflicts exist to the draft.

    ix.   General Alexander's papers provided material for additional draft recommendations. More discussion on these needs to take place. Mr. Barrett also noted the below:
1. In one proposed recommendation, there is a lot of implementation detail for counter strike actions.
2. One proposed recommendation contains some negative implications and raised the possibility of a retaliatory cyber attack.

    x.   One recommendation linked the concept of a rigorous measurement regime to the Framework measurement working group.
1. The National Cybersecurity Public-Private Partnership (NCP[3]) is a new advisory organization for the President.

    xi.   Two new proposed recommendations not in the current draft that Mr. Barrett described and said he will add to the draft:
1. Clean pipes: The Administration should eliminate known bad traffics. This is not a new topic. Re-engage with industry botnet group to determine course of actions telecommunications can take.
2. Interdependencies: Should provide tools to private sector hands to enable organizations that are not well resourced to do analyses. This topic drew from papers from Paul Stockton and thoughts from Mr. Gallagher, and has been recently reinvigorated by the White House.

II.   Questions on Critical Infrastructure
a. **Mr. Chabinsky:** My previously submitted document on removing cyber from end users mentions the current Connect America act. We can extend it to create a "Protect America" fund. The commission can consider this further

as one area to explore. There is support for this idea and the private sector will receive it well. A new business model can be created to accompany this concept.

    i. Is this mandated or voluntary? It will be mandated and paid for by the government. Making it mandatory also creates uniformity.

    ii. We have to figure out economies and efficiencies. There is more we can do. It brings a profit center to telecom carriers. It reduces workforce development problems because it removes from end users.

    iii. **Mr. Lin:** Do we think critical infrastructure is legitimate? If everything is converging, then critical infrastructure may be or will become obsolete very soon. What do others think? (Mentioned Mr. Lee, Mr. Gallagher, and Ms. Wilderotter have brought this up as well)

b. **Mr. Gallagher:** There is concern about language in the Homeland Security Act. If everything is connected, and the government focus is on critical infrastructure, is the language really that effective? Also, in the broadest view it raises questions on government over-reach. There has to be some attempt to get the underlying structure of the security.

    i. **Mr. Alexander:** We need to be aware of how devices can potentially attack nation-states and across borders. We see harmless devices can become weapons. How do we look internationally at the definition of IoT and things that are not harmful but can be if used maliciously? The commission has the opportunity to formulate a recommendation or finding on where this is going. Someone should look at convergence, how to set standards and work with international. It will be vital for this area. We need to get ahead of the curve.

    ii. **Ms. Todt**: Is there a thought on how the commission would like to propose that idea?

    iii. **Mr. Chabinsky:** It impacts botnet and also internet of things. It should be an over- arching finding.

    iv. **Ms. Todt:** There has to be a serious effort to re-visit all these areas in the immediate future.

c. **Mr. Banga:** Should we take it one step further and include technology that enables the internet of things? Can we create categories of "critical" and "nearly critical" for infrastructure?

    i. There are things that are not critical but can be used for malicious purposes. It is very nebulous now. This is a good line of thinking. We need to look at underlying platforms.

    ii. Those enabling techs have a responsibility to reach some baseline of performance.

    iii. It enables a middle point for discussion.

      iv. **Mr. Chabinsky:** Companies don't want to be designated critical infrastructure. The situation must change to be companies that are critical infrastructure and allow them to get help. Protection of wireless space needs to be considered. It is critical, and needs to be wrapped in.

d. **Ms. Murren:** There is concern with the placement of topics in the draft report. Botnets may not be critical infrastructure, but should be in the more forward looking areas in the report.

e. Summary for critical infrastructure:

      i. **Mr. Barrett:** Place a finding on decreased meaning of critical infrastructure over time.

      ii. **Mr. Alexander:** It could be a value proposition issue. "Infrastructure of critical infrastructure." There is more security improvement by looking at what they use, rather than what they are.

      iii. **Mr. Lin:** It is easy to arrive at insecure systems out of secure components.

      iv. **Mr. Alexander:** We should arrive at a baseline that sectors can build on top of. Different sectors are regulated by different government sectors. There can be harmonization issues.

      v. **Mr. Banga:** It is important enough to include in all sections of the draft report. We are not trying to reduce burdens, but increase the efficacy of efforts.

      vi. **Mr. Lin:** There should be multiple findings in overarching section.

      vii. **Mr. Johnson:** Secretary Pritzker sent her address to the Chamber. I can walk through the address for commissioners if needed.

      viii. **Mr. Banga:** I also have content to forward.

III. **Discussion of Recommendations for State, Local, Tribal and Territories (SLTT) led by Eric Goldstein**

a. Proposed recommendation 1: Sixteen states have integrated framework into their strategies. More need to follow.

b. Proposed recommendation 2: Congress is enacting a separate grant program for cyber. This establishes a separate grant exclusively for cyber. It will not compete with existing programs.

c. Proposed recommendation 3: Establish cyber apprenticeships in SLTT governments. They may be most disadvantaged employers in the market. It will encourage talent at that local level.

d. Proposed recommendation 4: DHS's National Cybersecurity and Communications Integration Center (NCCIC) become a one-stop shop. There is already work done through the Multi-State Information Sharing and Analysis Center (MS-ISAC).

e. Proposed recommendation 5:- State legislatures need to update their code, and at a minimum align with current federal standards.

        f.   Proposed recommendation 6: The National Guard should establish public-private collaboration. As members leave active duty, they can join the guard and have full time employment and be available in times of need. It will expand the capabilities of civilian employers.

    i.   Consider cyber regions for efficiency. There is no standard for where cyber resides right now. It will be difficult for smaller states to be responsive. States may also be able to share resources.

IV.   Questions on SLTT

    a.   Two thoughts:

    i.   Leverage students in universities.

    ii.   There is a new set of regulations and requirements in New York State. How do we ensure the right balance between states, national, and international governments?

    b.   **Mr. Banga:** It goes back to the issue of regulatory confusion. It also goes back to the weakest link in the chain. It should be included that we need to give support to municipalities. Not sure that point is addressed adequately.

        1.   We can look at Urban Areas Security Initiative (UASI) grants and how they can be used.

        2.   Also contact Greg Conti from West Point, who gave a black hat on how to take down a city.

        3.   Suggest contacting Jay Healey's group at Columbia University on examining New York City's critical infrastructure under a hypothetical attack. They may have models that can be used.

    c.   Can we add more about how people can do more with the National Guard? Suggest including admission requirements, clearances, etc. It will allow for collaboration by volunteers. Ms. Murren noted that maybe physical tests could be removed as barriers for people who are joining to work cyber issues.

    d.   **Ms. Todt reading question from Mr. Palmisano**: Is it efficient to take a regional approach to cyber?

V.   Financial Sector discussion led by Sam Palmisano

    a.   **Mr. Palmisano**: The structure of the proposed recommendations are that there should be a section regarding the financial sector for the industry. The CEOs are willing to add resource and talent to solve the problem. They feel the problem is best solved as an industry or partnership. They are looking for a more effective model.

    b.   **Mr. Lin:** The nexus to CI and SLTT should be explored. Do we need to change name of or find a new acronym? There is a fair amount of regulation of critical infrastructure that is state based. It needs to be expressed and explored a little bit. There is a political sensitivity in this issue. There are issues with states refusing federal aid for cybersecurity when they are way behind where the federal government is.

    c. **Clete Johnson:** It also talks to harmonizing requirements and engaging with the government. We need to come to harmonized approach. This speaks to removing structural impediments.

VI. Next Steps/Wrap-up

    a. Commission receives its next draft on 10/17.

    b. There will be a preparatory working group meeting on 10/19. It will be all day in DC, possibly at the Access Board. Everyone will review governance, identity management, and public awareness recommendations text this week.

    c. The Tuesday call next week is still on as scheduled.

    d. Recommended Outreach:

     i. Greg Conti from West Point

    ii. Suggest contacting Jay Healey's group at Columbia University for models examining New York City's critical infrastructure under a hypothetical attack

    e. For action on CI Section (Lead – Matt Barrett)

       i. Continue to reconcile Mr. Gallagher's comments in Framework section.

      ii. Consider Protect America idea

     iii. Add a finding on decreased meaning of critical infrastructure over time

     iv. Add a finding on Mr. Lee's thoughts on convergence

    f. For additional action on SLTT Section (Lead – Matt Barrett and Eric Goldstein)

       i. Look at Urban Areas Security Initiative (UASI) grants and how they can be used

      ii. Incorporate any additional Commissioner feedback

    g. Other staff actions:

       i. Incorporate idea of overarching findings into draft report (for all)

      ii. Look at financial sector proposal