Meeting Minutes

Attendees:

Commissioners: Sam Palmisano, Peter Lee, Steve Chabinsky, Heather Murren, Maggie Wilderotter, Joe Sullivan, Keith Alexander, Herb Lin, Alex Niejelow (staff for Ajay Banga), Annie Anton, Pat Gallagher

Others: Kiersten Todt, Kimberley Raleigh, Jordana Siegel, Matt Barrett, Andy Ozment, Robin Drake, Amy Mahn, Merritt Baer

Agenda:

I. Discussion of the International working paper led by Kimberley Raleigh
II. Discussion of the Critical Infrastructure working paper led by Matt Barrett
III. Next Steps/Wrap-Up

Discussion

I. Discussion of the International Working Paper led by Kimberley Raleigh

a. The commission has received a brief paper requesting guidance from the international working paper team.
    i. The paper includes short descriptions of various possible areas for further development: Law enforcement, public-private cooperation, international norms and international law, and others.
        1. There is agreement that international law and conventions apply to cybersecurity, but how they apply is to be determined.
    ii. There are many countries that are not as developed as we are. We need to develop weakest link.
    iii. Information sharing is a topic of interest internationally. Government to government sharing and industry to industry sharing discussion could be useful.
    iv. International technical standards also could be discussed in terms of incompatibilities in different countries.

b. Questions on the international working paper and input on where to do further research
    i. **Mr. Lin:** Explain the rationale for some of the topics at the end of the paper about topics NOT to include for findings or proposed recommendations, such as hack-back.
        1. These other topics are being addressed in different forums.
        2. **Ms. Raleigh:** If the commission believes any topic in that group is appropriate, it can be added. It was not intended to be a final judgement.
        3. **Ms. Siegel:** The interdependent topics are included because they are related to cyber. They are viable topics that could be developed.
    ii. **Mr. Lin:** International norms and nation-state conduct during peace time is an important point. It is curious and concerning, that nations are conducting offensive operations in cyberspace during peace time. Will we address whether espionage for intelligence purposes is considered a legal activity in peace time?
    iii. **Ms. Wilderotter:** Should we propose a recommendation on that?

1. **Mr. Lin:** We should not make a recommendation. But not mentioning the issue at all, is an omission.
2. We may need to mention why we don't include particular areas in the interest of completeness.

iv. International norms
1. Cyber espionage is part of this area. It needs to be mentioned in some form.

v. The topics mentioned thus far are very good. If we are going to work international, these are good areas to include.

vi. **Mr. Lee:** If we eliminate international norms as a topic, does the paper make sense? It still makes sense as the remaining issues still represent issues the nation faces. There are still highly relevant areas. It may be a scoping issue.

vii. **Mr. Sullivan:** One of the issues we are trying to solve is there is a lack of alignment of standards, in areas such as prevention.

viii. **Mr. Lee:** Hack-back and areas of data transfer will be critical in the future.
1. Hack-back is a failure by the government in terms of cooperation. If there is no cooperation between jurisdictions, it is a problem.
2. The government should promote the rule of law, so that the private sector does not have to take on hacking back or other activities to defend itself.

ix. **Mr. Alexander:** The Microsoft botnet take down should be mentioned. Examples of this should be discussed with international entities to promote a common cause. Another problem, how does the government promote working commercial internationally? When we get to areas of cybersecurity, we are fracturing instead of uniting. How do we arrive at standards we all can abide by that make sense?

x. **Ms. Todt:** Are there targeted things on cleaning up the internet that we can clarify that demonstrates what that means?

xi. We can look at advanced persistent threats. How do we develop an international alliance that helps stop these attacks? We can develop a number of examples to put out that would help improve things.
1. What is the role of government in defending companies that operate internationally? An example is Ireland and Apple in the news this morning. We need to develop something to get this right.

xii. **Mr. Lee:** My struggle may be terminology. On the botnet takedown, an enabler is the belief that cooperation with multiple states will prevent incidents.

xiii. **Mr. Niejelow:** Data transfer across borders is a huge issue. It goes back to the technical standards. We would like that issue woven back in.
1. Vulcanization of information and restricting flow of cross border data.
2. Cyber and anti-fraud capabilities will not function without data. These are very important concerns.
3. **Mr. Alexander:** Data should be stored locally in native countries. Data for international customers should be stored in those countries.
4. There are two negatives in that there is increased security for fragmented data. It is essentially a red herring argument being used on the part of European countries.

5. **Ms. Anton:** Europe is making a political play. They don't want to entrust their data to the United States. There must be some agreements between the European Union (EU) and the US.
6. **Mr. Alexander:** That is the problem. Others are more aggressive than the US. What is the role of the government, and how do we do it? This is one area where the government should lead.
7. In places with emerging markets, they are following European arguments with no framework behind it.
8. **Ms. Wilderotter:** We can include recommendations for agreements for governments now and in the long term.
9. **Ms. Todt:** *[To Kim and Jordana]* Any additional thoughts? If the commissioners want a follow on call on international, we can send an email on that.
    a. **Ms. Raleigh:** Would like a short write up from the commissioners on data localization and cybersecurity. It would be helpful for framing purposes.
    b. **Mr. Lee:** We may have some white papers on that topic.
    c. **Mr. Niejelow:** Will also forward material on the topic.
    d. Are international norms and international law out of scope? We can leave those to other forums.
    e. **Ms. Todt:** We should follow up with Mr. Banga before we drop that topics. Mr. Alexander gave a good summary.

II. Discussion of the Critical Infrastructure working paper led by Matt Barrett

a. Sources of input for the paper: The core team tried to have a good sampling of commissioner thoughts on which to build the paper. We also included panelist feedback from the other meetings.
b. We have interviewed 55 SMEs from different critical infrastructure topic areas. We wanted to include as many areas as possible.
c. We asked these questions: What are the biggest challenges, what is working or not working, upcoming research/innovations that could address challenges, and individual SME recommendations.
d. Highlights in the papers: Challenges, findings, proposed recommendations are threaded. Some areas of risk still not addressed.
e. What we hear from private organizations is about internal risk, not external risk. This needs to be paid attention to. We need to be mindful that piecemeal interaction is dangerous. Action by private sector may become dependent on money. It is worth a discussion.
f. Infrastructure integrators may not understand cyber security. It is not a new problem, but it is not addressed. Knowledge and skill may be addressed through labels that may provide awareness.
g. Mr. Ozment:
    i. It is important to start by looking at threats in terms of vulnerability and consequences.
    ii. DHS is not yet doing these things at the scale it wants.
    iii. We take a top-down and bottom up view. We look at entire sectors and individual companies. A top-down view shifts the whole economy, a bottom-up view assists individual companies.
    iv. Best practices, information sharing, and individual response are geared for small and medium companies.
        1. Examples –

a. Best practices: NIST; bottom up with risk assessments;
b. Information sharing goes both ways.
    i. There is the indicator sharing initiative and more traditional reporting by PDFs.
    ii. Incident response: The bottom up response helps one company (for example, the fire department and law enforcement assist at an arson fire).

v. On a national incident, the physical response should be led by FEMA; the cyber response should be led by DHS.
vi. NIST has done a great job with the Framework. It may need a more crisply defined standard of care. There is a need to harmonize standards across government and industry.
vii. We have the automated sharing initiative to share indicators. We need to share much more rapidly.
viii. Incident information sharing: There needs to be immediate and longer term, including what the incident analysis shows. For incident tracking, regulated industries already track and report incidents. Create a repository for that information. For non-regulated sectors, a non-profit repository can serve all sectors.
ix. Within DHS there is a proposal that the National Protection and Programs Directorate (NPPD) become a separate operational agency. It would empower protection, mitigation and response powers.

h. **Mr. Alexander:** One key point – we are focusing on responsibilities. There is the role of the Department of Defense to defend the nation. The DHS role is defining standards. We need to have a cyber command for cyber response. There must be some ability for the government to act corporately. We have not talked about it. There are no defined roles and responsibilities. This is the most important things to put on the table.
i. **Mr. Palmisano:** Is it your view that we need one focal point? What would be most effective?
j. **Mr. Alexander:** Secretary Gates had great insights to pull it all together in one agency. We should examine what he wrote, whether or not it is what we finally adopt. How do we ensure the security of the nation is the first priority?
k. **Mr. Ozment:** There is DoD presence on the DHS watch floor, so they know immediately. We need to have government roles clearly articulated. It must be defined for industry, critical infrastructure, and the nation. When you ask at the senior level, they get it wrong.
l. **Ms. Todt:** We are trying to get an answer to that question. We were trying to get an understanding at the August third meeting.
m. **Ms. Wilderotter:** The commission should be the catalyst to get a recommendation that provides clarity to that question. It is all three categories.
n. **Mr. Sullivan:** It must be incident response and prevention.
o. **Mr. Gallagher:** The current state of affairs and how it works is unclear. I am skeptical pulling it all in one place is the answer. DoD should not be dealing with civilian law enforcement. It must work at the highest velocity. No other event or coordination has to deal with this type of challenge.
p. **Mr. Gallagher:** What is the National Cyber Incident Response Plan status?
q. **Mr. Ozment:** It is in draft. A public will be draft out in September, followed by delivery to the President. Further clarity is always needed.

r. Are there any metrics for timeliness, or is everyone just making the best effort they can? Metrics are in terrible shape. Is there anyone with better internal metrics? Any feedback on metrics is welcome.
s. **Ms. Wilderotter:** It might be good to provide a description on your understanding of who is responsible today. It would be good for the commission to see.
t. Mr. Ozment will develop a one or two page document outlining current responsibilities for the commission.
u. **Ms. Wilderotter:** Is there a proposed recommendation for redefining critical infrastructure for the digital economy? It came up late in the discussion.
v. **Mr. Barrett:** We did not differentiate types of critical infrastructure, we did not propose specific recommendations.
w. Additional questions from the commissioners?
    i. *Mr. Lin:* An observation about lacking risk management. It is a very important point. There is not a better example of market failure. Each organization acts in its own best interest alone. Coordination with others is not in the picture. It is a good example of how the market has failed in cybersecurity.

III. Next Steps/Wrap – Up

a. **Ms. Todt:** We are working on a document to organize commission input for the September 20th meeting.
b. **Mr. Palmisano:** The commission should be critical in its evaluation of the proposed recommendations in the papers. Topics are complex and need to be considered carefully.
c. **Ms. Todt:** Minutes will be distributed for review and feedback as soon as possible.
d. Mr. Ozment and team will send paper on roles and responsibilities.