Meeting Minutes

Attendees:

Commissioners: Tom Donilon, Sam Palmisano, Pat Gallagher, Heather Murren, Steve Chabinsky, Keith Alexander, Herb Lin, Peter Lee, Joe Sullivan, Keith Alexander

Others: Kiersten Todt Kevin Stine, Donna Dodson, Matt Scholl, Karen Scarfone, Alex Niejelow (for Ajay Banga), Jon Boyens, Greg Shannon, Alex (Sandy) Pentland, Irving Berger, Lee Badger, Clete Johnson, Robin Drake, Matt Shabat, Amy Mahn

Agenda:

I. Discussion of the Insurance Working Paper led by Jon Boyens
II. Discussion of the Research and Development Working Paper led by Matt Scholl
III. Next Steps/Wrap up

Discussion:

I. Discussion of the Insurance working paper led by Jon Boyens

a. Will briefly describe the research that went into the paper
   i. Cyber insurance has been around for a while. It's not new. The growth in demand for cyber insurance is new. Now it's done in combination with other policies. It is insurance that covers cyber risk, like traditional insurance on property. The key benefits are offering one more option for managing risk. The main benefit is it increases the use of standard and minimum requirements for underwriting. The capacity for underwriting has been, and is too small. Coverage is shallow, and doesn't cover intellectual property or other kinds of data loss, and infrastructure failure among others.
   ii. The challenge in doing research is a lack of information. The insurance sector does not share information with others. There are sixty cyber insurance carriers, with five or six having the bulk of the policies. This year, cyber insurance has grown to 3.5 billion dollars. It is growing, but slowly.
   iii. The problems are a lack of actuarial data. It is the nature of cyber.
      1. Frequency and impact are hard to quantify. The actuarial data feed is the number one barrier.
      2. Second, the effect of practices by organizations is not understood. There is no way to measure the effectiveness of controls.
   iv. Also, there is not a common lexicon in the insurance sector. Multiple policies must be compared to assess coverage.
   v. There must be current and long term focus to increase actuarial data available to companies. Getting data to ascertain risk to different sectors is important.
   vi. Is it possible to broaden the safety act or create a new cyber SAFETY Act? Incentives may drive market toward cyber insurance, but they don't address underlying issues.
   vii. **Mr. Shabat:** We started looking at cyber insurance in 2012.
      1. We learned there is an ongoing lack of data, and a lack of understanding of dependencies.
      2. DHS started talking about public private partnership at that time.

3. We continue to hear that we should focus on a data repository. It would be a trusted repository, with incident data for analysis.
    a. It would help increase awareness.
    b. Really intended to be broader than a breach or incident library.
    c. The repository would be managed by industry or academia not DHS.
    d. We believe who ever ends up running it, it should be oriented toward multiple groups.
    e. Use cases and usefulness to various groups is key. There is a white paper on use cases, etc. There was a comment period in the spring. The repository would contain incident information, and known details. The working group continues to work toward creating a pilot. Looking at potential roles of ISACs and ISAO's.

b. Questions on the Insurance working paper–
    i. **Mr. Lin:** Do you have information that people report data in a standardized way?
    ii. **Mr. Boyens:** Data is from private research firms. Insurance companies do not share data, as they feel the market is very competitive.
    iii. **Mr. Lin:** I like the paper, but I have questions. Why is cyber different from property insurance? I don't understand the cascading effect issue. Grid issues are networked. Why aren't those areas useful in cyber?
    iv. **Mr. Boyens:** The paper cites a study done on the power grid. It does not have an average cost for an incident because they don't have the actual metrics for an incident.
    v. **Mr. Sullivan:** How is the industry approaching cost of incident, when so much of the cost is damage to brands and trusts, as opposed to rebuilding physical structures? For cyber incidents, it is hard to quantify.
    vi. **Mr. Lin:** It also applies to the grid.
    vii. **Mr. Palmisano:** Insurance execs struggle with assessing a cost of a cyber incident. They are reluctant to write policies for larger amounts. Companies are trying to understand what cyber insurance buys them in terms of mitigating risk. The insurance must take care of catastrophic damage to brands.
    viii. The paper doesn't say how to come out with good output metrics. It has been an unsolved problem in computer science for a long time. There is no real correlation between adopting best practice and fewer hacks.
    ix. **Mr. Lee:** Are there any results from NIST predictive analytics project?
    x. **Mr. Boyens:** Actual work starts October 1st. We are getting partners lined up at this time. We will have much better information this time next year.
    xi. **Ms. Todt:** There has been discussion in meetings about the SAFETY act. Is there anything the discussions want to add on this area?
        1. **Mr. Gallagher:** One thought that keeps occurring to me is, that damages is the central issue. It relates to indemnification. Some of our discussions on liability relate. We have talked about the protective side, but not recovery. The cost of damages will play out there. It brings together a number of threats we've talked about separately.

2. **Mr. Boyens:** The metrics and measurement and getting the data seems to be the foundation to a lot of this topic. Many companies are hesitant to share information because of liability fears. Whether that fear is real or perceived, it is the main hurdle to getting data.
3. Additional thoughts in this topic can be sent to Jon and Kiersten.
4. **Mr. Donilon:** We could possibly have more work done, on an expansion of the safety act, or what might be in a cyber safety act. The data repository idea would include a liability discussion. There is a recognition we would only have data with less focus on liability in order to get it started.
5. **Mr. Alexander:** Metrics are important for insurance, but for liability protection as well.

II. Discussion of the R&D Working Paper led by Matt Scholl

a. **Mr. Scholl:** The paper is very government focused. It was structured that way because much of the data is available from the government. We have people from industry on the call who can assist with the industry point of view.
b. **Mr. Scholl:** Cybersecurity is still a very new science. It still needs a lot of basic research that would develop axioms and laws that would drive basic research.
c. **Mr. Shannon:** The primary role of the government is to clarify the long term problem that exists for society. It is providing short term solutions, and a long term view. Any system has weak links. We want those links to be difficult to identify and exploit.
    i. The state of secure tool development. Organizations are starting to add security measures to design. The ability to update systems security whether working or at rest.
    ii. The role of data is important. We are finding it is important for research to have access to actionable data. We tend to share everything because we don't know what is important. It has been found that anomaly detection on anonymized versus non-anonymized data is different. It must be socially acceptable. Scientific validity is key with research results, and touches into insurance and reasonable technical metrics.
    iii. One of the challenges is how to ensure technical security is improving and then consider how liability affects these areas.
d. **Mr. Pentland:** Providing an academic perspective. It needs to be addressed as a new platform for data exchange including transparency, auditability etc. We should do live deployments that include people doing real things in communities and hospitals to get immediate feedback and see real reactions. We have done this with companies and universities in Italy and Spain and telecom, banks and retail. We are examining issues of privacy. It was influential in the European Union privacy protection policy.
e. Assess impact of damage in incidents.
    i. Has there been policy research? During political research on policy, it was brought up to the agencies. The agencies ignored it.
    ii. A recommendation on policy research might help.
    iii. Is cybersecurity a science or is it more like engineering?
    iv. What about emphasis on an R&D plan. There is limited evidence.
    v. There should be more emphasis on anomaly detection.

f. Two comments on the value of a living lab: One thing we have here is a negative impact or ability to access data. Is there a political solution to enable access for research to high-value data?
    i. The commission has been asked to look ahead ten years. We can add quantum and other ideas to recommendations in the report. The Defense Advanced Research Projects Agency (DARPA) and Intelligence Advanced Research Project Activity (IARPA) are examples of programs with operational data.
    ii. Block chain type transaction histories can be used for some things. General comparisons on encrypted data. Audit certification compares certain types only.

g. A possible data exchange layer on top of secure layer. Living lab tests may change management, efficiencies, and may alter user perceptions.
    i. We found what happened in Italy was that some of our preconceived ideas of how things would turn out were wrong. Some user computations were easy, some hard. It was not what was expected.

h. **Mr. Gallagher:** In reading the report, there is a clear sense of gaps and research capability issues. What was not there were key research questions and/or grand challenges. We have a clear framework.
    i. **Mr. Boyens:** We have not figured out the ramifications of these things on the rest of the system. As that happens, there will be refinements.
        1. Data is now controlled, there are limits on the safety of revealing things. There is a glimmer of promise in security. There will be a series of evolutions that will lead to changes. At the beginning of the internet, we never expected to have what we have now.
        2. It may take 50 years to play out. Real transformation will start in the next five years.
    ii. **Mr. Donilon:** What might that transformation look like?
        1. Financial – Banks can't share now, because they don't own the data. There will be a dramatic risk reduction in financial systems.
        2. Medical – The medical community can't share because data is not encrypted. When data is encrypted, it will be possible.
        3. It is just beginning to be thought of, to aggregate and share without revealing personal data.
        4. **Mr. Boyens:** When things are encrypted all the time, it will be transformational.
    iii. In the draft language, there is a statement about defensive versus non-defensive technologies. Is the contrast there as stark as it is described?
        1. There is a lack of feedback, and until there is feedback it will be hard to get things to market.
    iv. It is hard to understand where the separation comes from.
        1. In a workshop a couple months ago, there was a real fear about money. Transformational ideas are not being looked at. If all data is

encrypted, that is a game changer. Most companies look at money as the short term return. Venture capital money is not in transformational ideas.

2. This is why a living lab approach and real solutions for real problems are needed. There is not enough synergy focused on what we need to do.
3. The commission could possibly recommend that. It can be described in different ways (developing a framework that works).

v. The view is 50 years for some of the longest term transformations to occur. It may be 50 years based on the pervasiveness and operational realities. We need it sooner rather than later. Promoting pilot programs is one role for government.

III. Next Steps/Wrap up

a. **Ms. Todt:** Minutes will be distributed for review and feedback as soon as possible.