Commission on Enhancing National Cybersecurity

Preparatory Working Group Meeting
DATE: October 19, 2016
LOCATION: O'Melveny & Myers
1625 Eye Street, NW
Washington, DC 20006
TIME: 10:00 A.M. – 4:00 P.M.

Attendees:

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

Others: Kiersten Todt, Matt Barrett, Matt Scholl, Alice Falk, John Banghart, Roger Cressey, Clete Johnson, Bruce Potter, Heather Murren, Jamie Crooks, Kimberley Raleigh, Jon Boyens, Rodney Peterson, Eric Goldstein, Jim, Chris, Heather King, Jeff Greene, Kevin Stine, JP Chalpin, Robin Drake, Mark Barrett, Karen Scarfone, Amy Mahn

Agenda:

I. Framing Discussion
II. Internet of Things – Matt Scholl and Jeff Greene
III. Critical Infrastructure – Matt Barrett and Eric Goldstein
IV. International – Kimberley Raleigh
V. Consumer Awareness
VI. Identity Management
VII. Insurance
VIII. Next Steps

I. **Framing Discussion:**

Mr. Gallagher: Strategy recommendations to consider carrying into the report:

- Ensure U.S. leadership in cyberspace
  - Doing everything we should be doing: include broadening and incentivizing cybersecurity framework
  - Bending the technology curve (include R&D, and theme of convergence of the internet and the internet of things)
  - Getting government ready for the digital age: (governance, consolidating what can be shared, developing a risk management posture)

Mr. Lee: Likes Pat's proposal; suggested second level could be:

- Shaping the internet of tomorrow (critical infrastructure, convergence, privacy-tension between national security and civil liberty)
- Security by default

Ms. Murren: Considering language for the Consumer section: Recommendations for safe coding belong in consumer protection, not consumer awareness.

Ms. Todt: Roadmap section to take note of relevant issues that do not fall in the main scope of the report such as the encryption/law enforcement debate, hack back, others.

Mr. Lin: Wants roadmap up front.

Mr. Lee: The convergence discussion regarding critical infrastructure vs. everything else needs to be included in the front matter of the report. Where is a discussion/recommendations that lie at the needs for national security/law enforcement and civil liberties? We don't want to get into encryption discussions.

Mr. Lin: Notion of the thinking critical infrastructure (CI) obsolete - Is it relevant still? Enabling good things to happen – frame changing opportunity to communicate cybersecurity as an investment and not a cost. We are not going to solve encryption debate (hackback debate). Relationship to Cyber Command and businesses – cyber command won't do that and we won't address. Each recommendation needs to have a goal for each and be measureable.

Ms. Anton: As provided previously, a goal needs to be provided for each. One goal is all IoT must be engineered to be secure by default and reflect a desire/outcome. Need to discuss encryption in some form here.

Mr. Alexander: Would like a set of ideas and a set of recommendations; for example the plight of small business, international roles and norms. Consequence is huge for companies. On role of government – we are not where we need to be if we cannot define the roles we require. Companies want protection to stop attack. What are big ideas? They could go into the Executive Summary.

Mr. Donilon: ***(agrees with Mr. Alexander)*** Believes some of the 'process oriented' recommendations are positive. Training, an Assistant to the President for the NSC, big agency, National Cyber Program is important stuff, OMB Risk Officer are all good. Public-Private relationship needs to be reflected in the Forward. We have some powerful ideas that need to be framed up right.

Mr. Chabinsky: Goal, outcome, how do we measure it? Attempt to change the paradigm focused on end-users (consumers, etc.). Shift cybersecurity from the end-user as much as possible. You won't have to develop workforce. The Enduring Security Framework Keith mentioned is a good example. Start at the high-level product and design level.

- Lead into products – IoT, building something into design, privacy by design. Deterrence; does it matter, horribly underfunded.
- First area should reflect the paradigm shift about how we're thinking about things. Should we have network capabilities? Not building up each agency. Calls into our views about the NIST Framework and regulation.
- Second area about emerging and enabling tomorrow. One missing area, our dependency on wireless infrastructure. Increasingly all cybersecurity is based on wireless. This needs to be included in a way forward section or somewhere in the report **(agreement by Commissioners on this)**
- Areas to ramp up government deterrence/observation of wireless tapping: Electromagnetic Spectrum and GPS (timing of that).
- Third area, notion of figuring out what is working and not working. Culture of adaptive-ness. Not pulling in data to measure.

Mr. Alexander: Might be valuable to mention e-voting in context of timing for the report.

Mr. Sullivan: No one in the federal government that sees it as their job to prevent incidents for small and medium sized businesses. We are going to make sure that the federal government will build protection for small/medium-sized businesses. Concept of critical infrastructure doesn't fit within the digital economy. Civilian, military blurred. We've completely militarized technology in our lexicon. Would be great to move that CI discussion out of this report or rebrand it. CI doesn't resonate for small/medium businesses and consumers.

Mr. Donilon: There are workforce and societal challenges that need to be pulled up and reflected in the report. We have a pretty big success on the NIST framework. Expanding that and going through the next 6-7 steps seems right. It's building on success and worthy of a specific goal. Also, it seems we need to have an area that reflects: "Building an effective insurance capability." We're doing a lot of good work here. There's a DHS report where they are building a repository of actuary data. For the tone of the document, this isn't a "woe is me" approach. There are entities that operate well in the cyber world. We can't identify or foresee all the problems, but it's not a detriment. We need to reflect that in the document.

II. Internet of Things – Presented by Matt Scholl and Jeff Greene

Mr. Scholl: IoT recommendations by and large fit under the "Securing the Internet of Tomorrow" bucket. This section has three recommendations. I hear you about integrating convergence effectively into the recommendations. The first recommendation is primarily focused on harmonizing standards deployment – personal, industrial, manufacturing. For example, security on a health device (pacemaker) should be different than on a Fitbit. Each should come with the right privacy and security.

Mr. Lin: Where's the incentives?

Mr. Green: Comment on the second recommendation about assessing the current state of the law with regard to liability for harm. Tort structure exists for a physical device. We need the analysis of whether or not the same rationale is true for market security.

Mr. Lin: Recommendations need to not be process oriented. If tort liability is needed, then say it.

Mr. Alexander: IoT and internet convergence are both secure when it happens. We initially thought we could separate the two, but we know we can't.

Ms. Murren: There's a need to look at tort/liability overall – not just IoT, but consumer awareness and possibly others.

{Many commissioners: Nodded and noted agreement on tort liability and incentives and that there's a need there.}

Mr. Lee: We need to talk more about connected devices in the report, and a nutrition label.

Mr. Chabinsky: Tell us what standards you've used (FTC).

Mr. Donilon: What about staring with recommendation 1; in 100 days NIST will set these standards. Recommend label to start with, over time it will become the standard of care. If that fails, then government will look to the mandate for safety and security. A step-by-step approach. It will become the standard of care. This will be an ongoing NIST project, a life sustaining process. On safety and health, cite the DOT work for driverless cars. The president can say in those sectors that are regulated, we need to review this, and put in place similar standards. A significant set of steps. What do folks think?

Mr. Gallagher: NIST doesn't promulgate standards. We could use the Internet Industrial Consortium and they could be tasked to be responsive to this request. None of the regulated sectors are big enough to drive the entire space. You need consumer marketplace.

Mr. Scholl: Concern is wanting to converge, rather than add a voice. Need a forcing function. The cybersecurity framework is the example.

Mr. Lee: Want to limit focus to connected devices. One of the standards could be opt in default. Could segment IoT and limit what they can actually do. When thinking about labeling, define what standard if any is applied when developing your system.

Mr. Lin: Set the principle: Should tort liability apply or not apply to security?

Mr. Lee: Fault in device may not cause harm itself but may be a conduit for a malicious actor. How do you define fault?

Ms. Raleigh: Falls under FTC jurisdiction. Was the security of the device reasonable? Misrepresentation of the device? FTC could go after them in that route.

Mr. Donilon: Need liability in the right place. A recommendation could be for FTC and DOJ to deal with this in short time.

We've now experienced the largest distributed denial of service (DDOS) of a botnet. Take a shot at that here in IoT. The botnet issue is what's the bigger umbrella issue (credentialing, etc. can fall underneath). Could cross-reference the botnet issue as an overarching issue and reference into the Critical Infrastructure section.

Mr. Chabinsky: It's larger – behind espionage, credential theft. The botnet issue is a real issue.

Mr. Sullivan: I just want to caution that this conversation is trending into protection and liability rather than innovation and new technology. How to spur innovation – better infrastructure for IoT?

Mr. Scholl: When we edit, we will highlight specific areas identified during this conversation and pull the threads throughout the section. We'll cross reference to consumer awareness and CI (referencing the driverless cars).

III. Critical Infrastructure – Presented by Matt Barrett and Eric Goldstein

Mr. Barrett: There should be zero tolerance for degradation of service for CI.

Mr. Alexander: In terms of the front matter/introduction of CI, we say it's the government's responsibility to protect CI. But, what about the rest of the country? Our Constitution says it's a government to protect all the people, all the time. What about saying something along the lines of it's the government's responsibility to protect the nation and we'll start with CI? Digital age convergence is occurring. Government needs to re-examine the process. Intro needs to say we're moving into a digital age and we need to reexamine it. We use the same terminology to describe a very flexible approach as well as a minimalist approach. We could organize the recommendations by the theme of how to secure the nation in the digital economy.

Ms. Anton: Do not limit to intellectual property. In favor of investigation.

Mr. Alexander: Hack back can be bad. For example, Sony hackback to North Korea could be done incorrectly.

Ms. Anton: What about a cyber national guard?

Mr. Chabinsky: Private sector is doing that now with sink holing. Need to figure out how or if the private sector should engage. What can we authorize companies to do in their own networks? Approach that builds upon Keith's Enduring Security Framework idea.

Mr. Lee: Hack-backs: Dangerous for private companies to act unilaterally. Government isn't protecting private sector. Private sector says it's a basic right to protect themselves. The legal authority is not clear. The language is still broad.

Mr. Donilon: Suggest removing language about supporting hack-back. No broad statement should be included.

Mr. Chabinsky: We need to clarify existing law to facilitate a coordinated, legal responses.

Mr. Barrett: Clean ecosystem recommendation – notion of liability protection, they won't be able to clean everything up (so burden isn't on them, but aspirational). Spark innovation and how far we can get with the consumer (expand the carrot).

Mr. Chabinsky: People see their information getting taken. They could get their information back but area legally prevented.

Mr. Alexander: Industries come together on filtering issues, (e.g., child porn.), convene that type of group to determine the policies to define what is filtered.

Mr. Johnson: Acknowledged FCC's use of privileged communication (also included in a recent speech by Secretary Pritzer), so that they are able to protect the information exchange.

Mr. Chabinsky: Could incentivize R&D in this area. Need liability protection and understanding that you cannot clean everything. Rise up and get away from consumer; work with carriers to do that. Ambitious for this Commission to think that small and medium businesses don't have to worry about it. What is clean and what is not? Government role is to decide what is bad or not…botnets, malicious code, etc.

Mr. Lee: We would want a very clear government role described in the text.

Mr. Alexander: Let's see what's possible. The convener makes all the distance. Not just the internet provider, but multi-stakeholder environment. Net neutrality law.

Mr. Chabinsky: Start with botnets and then go further.

Mr. Donilon: Move to a study with an initial focus on botnets. Strong recommendation here for additional regulation of CI.

Mr. Alexander: We could use privileged communication – nothing you will say can be used against you.

Mr. Gallagher: We could use the Office of Information and Regulatory Affairs (OIRA) process to standardize sectors.

Mr. Donilon: Well, we've addressed by two issues – the findings calling for more regulation and the hack back recommendation.

Mr. Lee: We need to get a consortium in place.

Mr. Alexander: The idea of a study for clean ecosystem is the right approach.

Mr. Chabinsky: Capabilities are needed for government and industry to work together.

Mr. Donilon: A lot of work is needed on CI.

Ms. Todt: We could frame the front portion of the CI section with acknowledging that there are many things we can't identify /foresee in CI (for example, the electoral system wouldn't have been identified as CI a year ago).

NOTE: Agreement by several commissioners that the first recommendation (on baseline) should be removed, per group.

Mr. Alexander*:* If one did do everything right – and still got hacked --- are they free from losses? It's in our interest to maximize rate of adoption in these areas. Could reword second recommendation that

those that adopt the Framework look at some form of liability protection. With the Framework, much of it is business judgement. It does not compel you to do things so what is the metric?

Mr. Lin: Suggest that if you follow – you get liability protection.

Mr. Donilon: Suggest removing the counterstrike capability. Not worded right.

Mr. Gallagher: Recommendation 5 is not a big deal. Regulated companies – like energy – might need to get support from DHS because Enhanced Cybersecurity Services (ECS) is expensive and low uptake – allow a classified umbrella with funds for companies to get funds to get more uptake. Currently no funding for DHS to make that happen. Suggest we remove.

Mr. Chabinsky: Will work with Mr. Barrett to discuss wireless infrastructure.

Mr. Lee: Wording issue and concern that recommendation 9 is taking on life of its own. Process to move forward is right. Botnet is trending down, ransomeware is trending up.

Ms. Raleigh: Fourth amendment would really get in the way.

Mr. Chabinsky: Bounty approach is an example– instead of forcing people to solve – ask for help.

Mr. Donilon: With the timing of report after election, it needs words on state election systems.

Ms. Murren: Any way to have federal regulation over this? (Answer was no) Do we have steps to evaluate if cyber across democratic process (election systems) can be reviewed?

Mr. Donilon: Do we need to do anything about the electric grid?

Mr. Alexander: The electric system is made up of analogue systems (gas, turbo, nuclear). The biggest problem is that sharing of information is harder. And, the risk is greater than people are aware. Every time we think you can't do something with regards to the electric grid, someone proves that's wrong and shows how it can be done. I think the Energy Information Sharing and Analysis Center (ISAC) is doing good work. We need to continue to encourage them.

IV. International – Presented by Kimberley Raleigh

Ms. Raleigh: We need to do things we should be doing:

- Clean up co-opted infrastructure
- Facilitate transport access for evidence – Mutual Legal Assistance Treaty (MLAT) issue
- Assure U.S. leadership in cybersecurity – clarify application of international laws to cyber law
- Convene private sector and governments and push back against data localization

Mr. Banga: Big issue for Master Card. Should comment that we need international norms for harmonizing standards. Balkanization issue is hurting global multinationals. Too much time and money spent on trying to harmonize differing cyber standards in each country.

Ms. Raleigh: A coordinated strategy for standards building is needed.

Ms. Todt: We've seen the Framework in Italy etc. – does it make sense to take a body that Mr. Banga suggests, and do what?

Ms. Raleigh: Make it a standards body so that you can use with suppliers, for example.

Mr. Gallagher: Smart Grid international was flooded, but Framework was surprising to be very local. In the last workshop, there was a good showing of international. We need to internationalize the Framework and host workshops. What's the hold back in adopting the Framework internationally?

Mr. Barrett: There's no lack of support. It's a matter of getting around to everyone.

Ms. Raleigh: With regards to discussion of Recommendation 8, this would allow us to have a reciprocal process about US data stored overseas.

Mr. Lin: Wondering if you could work on the legislation separate from the technical issues.

Mr. Donilon: This falls under "Ensuring US leadership in cyberspace…" There should be a recommendation to adopt the Framework at its core, establish peacetime norms, start with Allies use of the Framework, then increase with other countries, such as China.

Mr. Banga: Uncomfortable with some of these recommendations' timeframes. They are too far out.

Ms. Raleigh: We're parsing our norms – have a few where bilateral success is made. Second sentence is geared toward due diligence type norm. Many wonder if that is an international law obligation. Suggest moving forward with a norm that is due diligence – but practical.

Mr. Donilon: We should note that the next President should propagate and implement the norms. We should be looking at how existing laws apply.

Mr. Lee: Wonder if in the framing front portion of this section there needs to be something about the norms (need to act to establish and set certain standards in place using common need for cyber internationally as a driver). We may be in situations that other nations are diverging (balkanization is occurring). We need to acknowledge that there are significant trust issues building between industry and government, and U.S. government and other governments.

Mr. Lin: The entire international section is cast in terms of maintaining U.S. leadership. A lot of the text sounds hegemonic. We need to be sensitive to other international readers who will be reviewing it. We need to focus on norms the way Tom was referring to. In light of Peter's thoughts, it made me think about it. Also, the trust gap between Silicon Valley and government is not acknowledged in the report, and should be.

Mr. Donilon: We should have at least an acknowledgement that this is happening and that part of it is addressing these issues (decreasing lack of trust, hegemonic trust, etc.)

Mr. Lee: Yes, we need some messaging about how the Administration wants to frame it.

Mr. Donilon: Well, I'm hegemonic. First, on the trust issue, the Executive branch is doing a bit on that. I just saw a DOD report that was given to Congress. Government does reserve the right to respond in kind or not in kind. All the elements of power are available, work multi-laterally and laterally to carry out cyber norms through economic, law enforcement, and military action.

Mr. Chabinsky: Deterrence of nation-states and criminals are different and we need to acknowledge that. May be worth talking about FBI's cyber legate program. How do you build up capacity to support FBI's legates? The U.S. private sector has a dominant role. How do we parse that out and how does US government support that? Private sector has often broken down the barriers. How do we think about that?

Mr. Alexander: We have to talk the talk. Clean pipes; look at it at the global space. Start with those countries who have already started on the botnet issues. We will need to read the report to see what will other states see and think when reading, and read it from an international perspective.

Ms. Raleigh: I'll reframe a lot of it, avoiding demonization of the internet. Deterrence can be included. There is a portion that we're not addressing regarding deterrence and the role of DoD.

V. Consumer Awareness – Presented by Kevin Stine

Mr. Stine: Relevant areas – informing and empowering consumers, and protection. Acknowledge Tom's buckets from previous calls. During a previous discussion, the suggestion of government to purchase deployment of devices can be related to empowering consumers and developers.

Ms. Murren: I've been thinking that Consumer Awareness may be too narrowly defined. We need to talk about consumer rights, protections, and awareness and then reference the original Consumer Act by Kennedy. We can combine some ideas here. For the software companies, we many need to re-mention the liability conversation from the IoT discussion here. I don't know that we should call for a six-month campaign and let folks determine how long and not suggest six months. Social, behavior, and public health scientists need to be involved in determining the specifics.

Ms. Anton : Consumer should know their role and use best practices as much as they know to lock their door. Developers should help that. Research can help establish validated methods to ensure systems are usable while maintaining security (non-tech users need intuitive systems, those more savvy need inconspicuous security, policy makers need tradeoffs).

Mr. Gallagher: Agree with Heather's point that it's bigger than consumer awareness.

Mr. Chabinsky: The language needs to reflect that its part of the civic fabric of our society. How do we trust the technology?

Mr. Lee: If people didn't trust our products, then we would have a major problem. Trust is everything.

Mr. Gallagher: How to develop trustability of this information/infrastructure? How can you live a full life without access to the internet?

Ms. Murren: People deserve to be educated on a topic that is important to them.

Mr. Gallagher: If no access, can you bank, access education and healthcare…

Idea of one page tear sheet was proposed on "this is why these things are important to you" – Mr. Lin liked this.

Mr. Donilon: We need to research a bit about the Bill of Rights, specifically about useable security and privacy.

Mr. Lee: Usable security and privacy …. Any examples people can relate to?

Ms. Murren: Hospital trying to do two factor authentication and failed; put second factor in the garage entrance key.

Mr. Stine: A few examples fall in identity management. A bill of right can also be the responsibility of the citizens – and what the awareness campaigns can drive towards as well. Can write basic needs to citizens. "Responsibilities of digital citizenship" – and a bill of rights a complimentary piece.

Mr. Banga: Too wide a definition of consumer can be confusing.

Ms. Anton: A tear sheet is better than a bill of rights.

VI. Identity Management – Presented by Kevin Stine

Mr. Stine: The identity clearinghouse suggestion describes what is currently used by USG and private sector. Two things to call out are liability and looking toward shared responsibility model and how ecosystems have evolved. The second piece new since last time we saw is the suggestion of moving beyond the people identification, and bringing together body of experts from public and private, setting up identity management requirements.

Mr. Banga: Not sure about the "hampered" language in front section; suggests a friction of the system that if removed, could enable these to be delivered most effectively. Hampered makes it sounds more bad rather than a roadblock or friction. Second comment has to do with limiting the liability of credit card industry. Liability shift – the highest security form used is where the liability goes away from. If you're a merchant and had chip, there's fraud in transaction it would be to issue of back. If merchant didn't have chip and card came, the merchant isn't invested. What does an identity clearinghouse (or trusted agents) include? What would this mean?

Mr. Alexander: Could we put in assessment of how to use identity, that doesn't have you going into a machine, but have an ID card? Will it be something we just ignore, or something the government has to take time to address, and take away overhead and concern?

Mr. Gallagher: In terms of strategy, trusted identities, case in question – identity management always felt like thing of the future, but is there anything actual that really launches something significant, since we're still on passwords?

Mr. Stine: We haven't been able to kill the password. There's a bit of the core NSTIC principles, usability etc., learned a lot through pilots, how do you learn through pilots, successes we've had, and taking things to the next level. The notion of clearinghouse gets to the federated model

Mr. Gallagher: It's not a voter registration issue. Doesn't leverage the power of today.

Mr. Gallagher: These recommendations feel like we're building from scratch and not building. Is there anything actionable that launches things in the future? Anything to further amplify the National Strategy for Trusted Identities in Cyberspace (NSTIC) principles? How do we take what we've learned from many of the pilots and move to the next level? It feels like we're being cautious.

Mr. Lee: Acknowledging Steve's consistent push for moonshot - the goal to achieve within a reasonable timeframe one ID and one password for everything you want to do for every citizen from the vendor or government of your choosing. Recognize we need to stay away from a national ID. Define a clearinghouse idea. Establish your credentials with a vendor of your choice. Government wouldn't be the only source of identity.

Mr. Chabinsky: Loves the idea. Part of the design element is being able to shut it down if it was impacted. People are able to look different because we have different passwords and such. There are privacy concerns and this would be voluntary. One sign-in and pulls and takes into your account information. There are trust barriers and the technology is holding us back.

Ms. Todt: We don't have the technology (single point of failure with where the technology is). And, where does that leave us?

Mr. Lee: Perhaps it's acknowledging a single point of failure. How it might be considered would be different (provided examples of Microsoft and Amazon Cloud).

Ms. Todt: Do we want to go with the moonshot idea and talk about where the technology needs to go? Essentially, inoculating a trust broker and validating IDs.

Mr. Gallagher: The problem with moonshot is it's anti-NSTIC; I like the idea of big push on this, and have to figure out where pressure point is. A trust broker is what's missing, someone everyone trusts, where everyone could establish relations with that person.

Mr. Lee: We shouldn't counter NSTIC, which is highly problematic. There should be a shared responsibility to take notice and care by every citizen. Grouping for a way to engage everyone and get people to sit up and take notice.

Mr. Gallagher: Some business models use a federated single password.

Mr. Donilon: Let's start with government.

Mr. Lee: The internet started with the ecosystem (proprietary network of technologies) – each owner saw a value. It took government to set standards around IP. I don't buy that the ecosystem is better. We have an ecosystem with a nightmare of managing proprietary networks or challenges. Failure of the business model not the technology model.

Mr. Donilon: Why not start the identity management section with the framing of killing the password and having a single identity. Some companies are reliant on technology for the Cloud. Acknowledge that there is very bad stuff that actors are trying to get.

Mr. Lee: Big data analytics today properly corrected email accounts. Over 10 million have been decreased. The scale that's achieved enables more money and data**.**

Mr. Banga: Identify behavior and the scale to manage it. We're building trust, which becomes a priority.

Mr. Alexander: Clouds are more secure than a network because of volume.

Mr. Lee: Gave example about fingerprinting and injecting silicon. The cost it took to design the system with security in mind was significant.

Mr. Alexander: Most small to medium sized businesses will push their stuff into their cloud. We can acknowledge we are creating an ecosystem to get to the goal. Play off of the efforts of NSTIC; near-term is the ecosystem and long-term moonshot. Lay out the process to getting more ambitious.

Ms. Todt: We can layout next steps (tactical) and then move to more strategic moon shot. When motivated by innovation and security, we have created the solutions, others have the solutions and we have to be able to wrap those concepts into what we're presenting.

Mr. Donilon: IBM testified with optimism about distributed ledger technology being the solution to identity management. There's a huge amount of basic technology to be done that should be called out and emphasized. Are we five years away from having the technology available?

Mr. Banga: There's still time needed to get there. Blockchain is further away because it is still small, when you get into larger blockchain with regards to security. Blockchain and biometrics need to be in this section in some way.

Mr. Gallagher: Does liability shielding make sense? An attribute given to trust broker, would allow them to recover costs. Higher assurance might occur. It would be against identity fraud. There's no business model.

Mr. Sullivan: Is it too dangerous to walk into the number system?

Mr. Lee: My frustration with this section is that this Commission was created to deal with the identity management issues resulting from the Office of Personnel Management (OPM) hack Do we provide any suggestions to address this hack?

Mr. Gallagher: Acknowledges that the commission's work is more broad than a particular incident.

Mr. Chabinsky: What about having disposable identities?

Mr. Lin: You would have to validate you are who you say you are. That would be moving back.

Mr. Donilon: If we could require a dual factor authentication, I would.

Mr. Gallagher: The Real ID Law is the closest to what we have. And, that has not gone all that well.

Mr. Donilon: Let's explore the federated model, government relying on industry.

Ms. Anton: Let's bring the nation's brightest people together to develop a policy and technology solution. We can say "move from x to biometrics to x by x."

Mr. Chabinsky: We could put this out as a grand challenge. We can say what the design features should address (e.g., privacy, security, etc.). We describe the desired outcome, how you get there is the challenge.

Mr. Donilon: Are we making the same mistakes?

Mr. Lee: Target was a vendor problem. OPM was an everything problem.

Mr. Alexander: We don't allow companies to pass information back and forth to help them. Consider companies sharing exploit data. There's no way. We need a cloud market for small and medium sized businesses. Roadmap needs to include a way forward and the items that we'll still need to address.

Ms. Todt: We could add to the R&D section to address increasing of funding for identity management.

Mr. Banga: We have put money into the blockchain. The legal environment around the blockchain ledger is a way to transition. We should include in the R&D section.

VII. Insurance – Presented by Jon Boyens

Mr. Boyens: There are many myths and misunderstandings about the cyber-insurance market. Understanding what is true in the sector will help clarify what action should be taken. The insurance space is growing. How can we support it? The insurers are having a hard time quantifying the risks. The data is out there in the organizations and though it's not shared, they could do a risk assessment.

Mr. Chabinsky: Some policies require reporting to a law enforcement agency (LEA). If you're a victim of crime, you have to report to LEA, which might help aggregate data.

Mr. Boyens: Reporting to LEAs is stymied. Companies often refuse to share until an investigation is complete.

Mr. Chabinsky: Industry could require the information of incidents to share with one entity, then have the data get back out for sharing purposes to the insurers. On the intake, the data could be captured in a consistent way. Could allow the insurance industry to use it and force government to do something

with it. Not saying we should require this be put into policy, but does this jive with data and how we use it?

Mr. Boyens: Yes, we can work together on it.

Mr. Donilon: Suggest recommendation be written up to have insurers require incidents being reported to an LEA.

Mr. Lin: Self-insurance is not a market. Often a complaint from CISOs is there's a lot of internal data in companies they can use to make decisions more effectively…the idea they can't isn't that they can't, they just don't know that they can. Wondering whether there's view of that under self insurance category, such as guys who want self-insurance in this business, and are there ways of making rational cost effective decisions of where to spend next dollar in cyber.

Mr. Donilon: NIST Framework does not cite insurance?

Mr. Scholl: No.

Mr. Barrett: Insurers did endorse the framework.

Mr. Gallagher: the insurance companies were involved in the framework process from very beginning.

Mr. Scholl: Insurance, privacy, supply stream were involved – looked to downstream, and some things were included in roadmap at end; this is long way to say no.

Mr. Boyens: We also didn't have a way of showing the effectiveness of mitigation practices; the Framework would help get a better idea of how organizations were managing. In the midsection, a lot of input we received in recommendations for cyber insurance have largely come from brokers and insurers. A lot of recommendations are to grow the market. I could go into the SAFETY Act and the thought process on that, and back to myth that market isn't growing fast enough. A lot of state regulators talk to insurers and caution against growing too fast, since they're not sure of risk they're undertaking.

VIII. Next Steps:

The Commission staff will consider the following proposed actions:

(1) Revise input on topics based on commission feedback received today and,
(2) Consider organizing recommendations into the "buckets" outlined in Pat's email (which also align with the goals outlined in the Executive Order). These "buckets" are:

1. Protecting and defending our current internet (EO Goal: Bolstering partnerships between Federal, SLTT, and the private sector);

2. Shaping the internet for tomorrow (EO Goal: Fostering discovery and development of new technical solutions);
3. Getting government ready for the digital age (EO Goals: Fostering discovery and development of new technical solutions AND Strengthening cybersecurity in both the public and private sectors while protecting privacy);
4. Preparing our citizens for a digital age (EO Goal: Strengthening cybersecurity in both the public and private sectors while protecting privacy); and
5. Ensuring U.S. leadership in cyber (EO Goal: Ensuring public safety and economic and national security)

Staff will complete these actions by COB Friday and will send the revised organizational recommendation structure with recommendations to Commissioners on Monday for Tuesday's call.