Commission on Enhancing National Cybersecurity

Recommendations Working Group Discussion
1625 I Street NW
Washington, DC 20016
November 8, 2016; 10 AM-4 PM

Attendees

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

Others: Kiersten Todt, JP Chalpin, Robin Drake, Matt Smith, Mat Hayman, Kevin Stine, Matt Scholl, Rodney Peterson, Jon Boyens, Steve Chabinsky, Heather King, Rob Knake, Alice Falk, Matt Barrett, Roger Cressey, Clete Johnson, Evan Schlom, Jamie Crooks, Jeff Greene

Agenda

I. Welcome and Overview
II. President's Charge and Commission Approach: Recap of Recent Discussions and the Way Forward
III. Foundational Principles
IV. Imperatives
V. Lunch
VI. Recommendations and Action Items
VII. Structure and Tone of the Report
VIII. Review of Proposed Revised Imperatives and Recommendations
IX. Summary and Next Steps

I. Welcome – Tom Donilon and Kiersten Todt

a. Will be reviewing third draft of proposed recommendations and content, and additional commissioner discussion via email over the weekend.
b. Heather wrote a cover letter, well received by the commission.
c. Much of discussion will focus on language and priorities in the report. Substance is close; we will also work on presentation. The report does align with the President's order.

II. President's Charge and Commission Approach: Recap of Recent Discussions and the Way Forward

a. Imperatives – could adopt Ms. Wilderotter's statements for the imperatives.
b. Suggest the government imperative not be first. The order in the Executive Order does not have to dictate our emphasis.
c. Will be working today at several levels – Need to review foundational principles and make sure principles represent commission thought.

d. There are six proposed imperatives – workforce is now a separate imperative.
e. Recommendations – there are thirteen proposed at present; will address action items as there is time.
f. Mr. Lin brought up in email that there should be a statement to indicate that not all Commissioners agree with the final overall content of the report. The report has greater impact with greater consensus.
g. **Mr. Palmisano**: If commissioners want to expand on discussion on certain areas, it is ok. We should emphasize fixes for underlying issues. We can make the government perfect, but it won't fix problems. There is a sentiment in the commission that we are not addressing the underlying problems.
h. **Mr. Gallagher:** Lack of consensus is ok, but indifference is a problem. Dissent should only be presented if there has been serious discussion. Fixing the government is not the same as fixing cybersecurity. The government has become dependent on information. The government does need to be fixed but it is not the root. Ineffectiveness in the government can undermine any efforts.
i. **Mr. Palmisano:** There is a strong belief from those with a technical viewpoint, that we are compelled to fix the underpinning causes of the current issues. Would like to open discussion with this idea out there. We need to develop strong requirements, with technical assistance to deal with these issues. Internet of Things, identity management, and liability are the top three areas in the report.
j. **Mr. Sullivan;** I have been struggling with language on protecting the digital economy and protecting the nation. There is a military aspect, and enforcement of law on the street. We are not in the cyber-war business. We get pulled into the language of war and nation-state challenges. We should be in the business of making things safe for businesses, etc. Cyber war and safety are intertwined.
k. **Mr. Gallagher:** Our primary focus is on the civilian side. The military side can muddy things, but we need to stay to the civilian side and acknowledge the other elements.
l. **Mr. Chabinsky:** Initially attacks were problem of the companies, government became involved when companies took initiatives that Justice did not like.
m. **Mr. Alexander:** The commission does not dwell on cyber-war, but the commission should give the next President a path of what to do.
n. **Mr. Banga:** It must be addressed with the right balance.
o. **Mr. Lin:** Did we not agree that there were areas we would not address directly. We will acknowledge related but important issues.
p. **Mr**. **Donilon:** Regarding direction – We are not discussing .mil domain.

III. Foundational Principles

a. **Ms. Anton:** Would like to re-write the privacy principle.
b. Importance of global means to deal with cybersecurity and global interconnectedness and inter dependencies. Could add as another principle.
c. **Mr. Gallagher:** The purpose of the principles is to expose our thought process. It can be noted there are two aspects to government – military and civilian. The idea of dependence - We are in a time when governments, institutions and individuals are dependent on technology. It is critical to get the incentives right. We can be agnostic as to the type. We can point out market forces and regulation can contribute to incentives.
d. **Mr. Lin and Mr. Lee:** Puzzled by the technical concept of privacy to the top level. The primary focus should be protection of civil liberties. Privacy is important, but

why is it elevated uniquely to the top level? Privacy does have places where it is important, but it becomes overly technical in other areas.

e. **Ms. Anton:** Will re-examine the privacy aspects from a technical point of view. The report must be understandable to policy makers and engineers.
f. **Ms. Todt:** There is some feeling the report is too technical in its language.
g. **Mr. Palmisano**: Can we talk more about what parts are too technical and develop simpler language?
h. **Ms. Murren**: It may not be the whole report, but there are some places where it can be examined.
i. **Mr. Lee:** Too technocratic.
j. **Mr. Lin:** In reference to IoT devices, they are not talking about laptops. Are we saying we don't care about others - cyber-physical devices or cyber only devices?
k. **Mr. Lee:** – The language can be too abstract.
l. **Mr. Donilon:** Must say things like "Popularly referred to as the IoT"; “We are speaking of;” etc.
m. **Ms. Anton:** Noting meanings of terms in the report is important.
n. **Mr. Alexander:** Must be language on the US effort to continue to lead in the internet.
o. **Mr. Lee:** There is concern to how the language will be received in the rest of the world. Some countries may find certain parts offensive.
p. **Mr. Gallagher:** If we are asserting leadership it may be a slippery slope. Speaking from an innovation perspective, it may be better received. We want to encourage thought leadership and innovation.
q. **Mr. Palmisano:** The US may have the best innovation model going.
r. **Mr. Donilon:** "It is important for the US to lead, invest, and ensure…"
s. **Mr. Lin:** What do we want to say about R&D in cybersecurity? Include investment reference in imperative.
t. **Ms. Murren**: Relate the order of the imperatives with the principles. Will look at relating the order.
u. **Ms. Todt:** We have agreement on the total of 12 proposed principles. The first is that government is information department and second is convergence. Should privacy remain a principle?
v. **Ms. Anton:** Would like opportunity to re-write on the importance of investment and collaborate with international standards organization. If we don't it will have negative consequences.
w. **Mr. Donilon:** Regarding one of the principles - Can we emphasize importance of incentives? There are recommendations for private sector responses, but regulation may be pointed to if there is not sufficient progress. Incentives can be driven by any combination of forces including market and others.
x. **Mr. Gallagher:** We know there are things we are not doing that we should be doing. What makes that happen? We should speak to that.
y. **Ms. Todt:** Will reorder, and revise.
z. **Tom Donilon:** Could combine fourth and fifth principles.

IV. Imperatives

a. Do the imperatives reflect commission priorities?
b. Some recommended not starting with the government imperative.
    i. **Mr. Gallagher:** There are a couple of major actions dealing with current threats – Identity is one area, information sharing, etc. Tackling large threat

vectors. Next, best practices; third-mission role of government, it is not the role of the private sector alone.

ii. Insurance deals with the future (not a present imperative).

iii. **Mr. Chabinsky:** Cleaning up the internet is part of a larger issue. It means shifting to a higher level and away from consumers. What are the things we can do now to start the process of moving away from consumers? Three main areas.

iv. **Mr. Gallagher:** IoT is a current technology, not future. Need to address preventative steps, and response measures.

v. IoT means connected devices, for definition terms.

vi. **Mr. Banga:** Identity should not be submerged as an action item. It should be a separate recommendation. It seems that identity management, information sharing, and protecting the weakest link must be in the principles.

vii. **Mr. Lee:** The reason the commission exists to respond to identity management. It should be fairly high level. We are not helpless on the internet. We have technologies. Mobilizing them in a meaningful way is the challenge.

viii. **Mr. Chabinsky:** Remove the burden from the consumer.

ix. **Ms. Murren:** We are here to create change, not just write a report.

x. **Ms. Todt:** Recommendations are broad ideas; action items are steps. Imperatives are key priorities.

xi. **Mr. Chabinsky:** Clean pipes – few things – eliminate known vulnerabilities; getting rid of threats, etc.

xii. **Mr. Lin** – We are intervening in the end-to-end design philosophy. Can it kill innovation? Some international counterparts will interpret it as government intervention in cleaning up the net.

xiii. **Mr. Chabinsky:** The language was carefully chosen. The current law in the US is that carriers should be aware of bad traffic. The backbone must be able to protect itself. Carriers are sorting traffic now, but it must have purpose.

xiv. **Mr. Lee:** Clean pipes in the report is very risky for the commission. The language must only be interpreted in one way. It may also need to disclaim certain things.

xv. **Mr. Donilon:** There are systemic attack vectors. Second idea – identity management. Passwords and identity have been at the center. It is a complex idea relating to cost. How will it be paid for? There is responsibility to not have known malicious activity. Suggest it be studied by working together. It could be a phased approach. First the goal, then action (going after botnets, for example). The identity management idea (from Mr. Banga's paper) – moving to multifactor identification (MFA), improving citizen interfaces with the government, and federated identity management. Small, medium businesses also important.

xvi. **Mr. Lee:** Clean pipes came from the White House. We need to be careful how we speak of it.

xvii. **Mr. Palmisano:** Internal fraud, identity management, safety.

xviii. **Mr. Lee:** Concerned about carelessness on the part of the White House. Pandora's box has been opened. US leadership needs to address what is happening.

xix. **Mr. Donilon**: We start by identifying known unlawful internet programs that should not exist. Should move from there to getting agreement they should be eliminated. Describing a path forward is the goal.

xx. **Mr. Johnson:** The inquiry is not just about the pipes. It is crucial to look at malicious traffic. "Clean ecosystem," not pipes.

xxi. **Ms. Todt:** There are threats to the internet today; recommendations will follow what is here. Threats, identity management, small medium business, are the big three.

xxii. **Mr. Palmisano:** Idea of clearing house to protect digital identities for life. If the technology can work, it is a huge portion of the issue.

xxiii. **Mr. Gallagher:** The ideas that have been spoken of have not been put into practice on any large scale.

xxiv. **Mr. Palmisano:** If the government establishes all interactions happen through that interface, it will come to pass. We can start with named consumer-facing government programs. We can then build next steps.

xxv. **Mr. Sullivan**: We should encourage the government to lead on identity management. Social security numbers, airports, etc. There is no reason why the government could not build digital identities for citizen interactions. "Government as an authenticator." It should start with something simpler like unified identity for government services.

xxvi. **Mr. Banga:** MFA does help with authentication, but it slows adoption of digital services. The wording makes it look like citizens must accept MFA to use government services. It will create enormous friction. A true digital identity is what could solve the problem.

xxvii. **Mr. Gallagher:** The strength of the authentication is the key. Define "strong" and the technology will follow. The proofing side is where the challenge is. The government must drive adoption.

xxviii. **Mr. Lee:** Does this proposed recommendation imply a common identity management across all agencies? Every agency could be managing its own identities, but joining the Fast Identity Online (FIDO) Alliance is good. The identity management federation will be done by the government. Want to avoid app passwords, etc. It becomes very difficult.

xxix. **Mr. Gallagher**: It won't work unless it goes to scale. Requirement government to use some form of higher authentication makes sense.

xxx. **Mr. Donilon:** AI 2.2.3 Requires government to use "strong" authentication. Performance based standards; the current definition of strong is too restrictive.

xxxi. **Ms. Todt:** Botnet, identity management, and separate small and medium businesses, IoT – should it be in this section?

xxxii. **Ms. Anton:** There is no independent body in the government to investigate major cyber incidents, to figure out what happened and how to keep incidents from happening in the future.

xxxiii. **Mr. Chabinsky:** It's better to fix current things than create new bodies to do jobs that are already being done.

xxxiv. **Mr. Donilon:** The President just issued presidential policy directive (PPD) 41 – staff can analyze further information (Information Security and Privacy Advisory Board {ISPAB} speaker for PPD 41), and CERT, National Transportation Safety Board (NTSB).

xxxv. **Mr. Palmisano:** If we use the "connected things" definition, it is implicitly in this section. Adding device authentication to the concept of individual authentication. Insurance is a means to adopting these standards.

xxxvi. **Mr. Chabinsky:** Representation and certification to get coverage. Requirement to report to law enforcement when breaches happen. The NIST framework is one way to mandate risk management principles, but it is not the only way. The government should use the framework. We want to head to improving security.

xxxvii. **Mr. Lin:** We are at the start of growth in the future. Are there areas where cyber insurance should be required? We can observe it may be required in the future.

xxxviii. **Mr. Palmisano:** If we stick to the principles of the NIST approach, it becomes accessible. There is procurement aspect for the government.

xxxix. **Mr. Palmisano, Mr. Gallagher:** Describe insurance in procurement practices. As the government implements NIST principles, it will be in there. Those kinds of change are commercial, not regulatory. It does create large scale change. Strategy is become about driving its adoption. Regulatory harmonization is a powerful tool.

xl. **Mr. Donilon:** Identity management – goal major public private sector activity in identity management. Government to identify citizen facing services, and improving authentication; requiring strong authentication for agencies. "Strong authentication solutions." Tech path forward?

xli. **Mr. Lin:** Must stress it is not a digital national ID card.

xlii. **Mr. Lee:** There is an edgy aspect here. We can be a force for thoughtful intervention in these areas.

xliii. Imperative three – Internet of Things

1. NIST standards for IoT devices. Oversee adoption of standards by IoT manufactures. Also labelling aspect (IoT, UL)
2. Perhaps the sense of urgency in this area was not captured in the draft. Mr. Potter wrote a paper on weaponization of the internet, and changing default user names and passwords. These aspects should be included in terms of liability and balance between manufacturers and consumers.
3. **Ms. Anton**: Consumers do not need to understand the implementation of the IoT. There is still a lot of burden on end users, as opposed to engineers. Understanding standards will take longer, but there is education that can take place.
4. **Mr. Gallagher:** Two distinctions – scale and primitive state of many of these devices, the idea of a standard of care for these devices. Also, the IoT that controls things, such as medical devices - these devices do things that have kinetic effects. Should attach liability where the kinetic function lies.
5. **Mr. Lin:** Because something is connected, it is not exempt from liability. The report does not actually say this. There are exemptions for IT companies.
6. **Mr.** Lee: These are relevant issues, and could be included in the sections where baseline standards are. The process for determining these standards, should consider these ideas. Passwords stick out in a way in the list of vulnerabilities. There are many types of

vulnerabilities. It is a moving target. We are not recommending or requiring any update capability for connected devices.

7. **Ms. Todt:** Is there a broader principle at play we can apply here? We can determine the language, if there is agreement on the approach.
8. **Ms. Anton:** In terms of proposing to increase funding over the next ten years - how were funding numbers arrived at? The numbers came from the Office of Science and Technology Policy (OSTP) based on their current funding. They were estimating scale of budget for a 10 to 20 year time frame. Should we make comparison of spending between US and other countries? It is difficult to get R&D cybersecurity numbers.
9. **Mr. Donilon:** We are attempting to identify what will make inherently secure systems.
10. **Ms. Anton:** Do we need to rationalize the number of dollars we present?
11. **Mr.** Donilon: Probably not. Can we phrase in more moonshot language?
12. **Mr. Gallagher**: We should be wary of setting research goals. We can comment on more specific things: the capacity argument – symptoms of underinvestment in cybersecurity R&D. It should not be tied to any particular moonshot. If there are identifiable gaps, we can speak about those without impinging on existing R&D agendas. Agendas should be set by research organizations, not the commission. In traditional R&D, government does basic and private sector does the translation. There is a third part. There are times when the government use has a direct role in the process. Cybersecurity is one of those areas. It plays into the capacity argument. What is missing is a technology agenda, driven out of the government's need.
13. **Mr. Alexander:** Separate out classified. How do we look at the long term issues, including identity management?
14. **Mr. Lin:** We need to make sure these things are not seen as separate. We know a lot about how to do things, we need to do them. It goes back to incentives. Getting us to do what we already know how to do is important. The major improvement will not come from new programs.
15. **Mr. Gallagher:** We need an R&D to focus on integrating technologies.
16. **Mr. Palmisano**: It means system level thinking and design. We can solve many problems this way. The scientific community should establish the agenda.
17. **Mr. Donilon:** The section describes a system project. Can we bring in the idea to design for security from the beginning? We then have the opportunity to really improv*e* security*.*
18. **Mr. Gallagher:** We need to be sure we don't say this is *the* R&D agenda.
19. **Mr. Lin:** We should add the need of system development as context.
20. **Mr. Gallagher:** Capacity, tech transfer, government should add system integration in the narrative.

21. **Mr. Gallagher:** Is there an arena of learning for connected devices? Is there any anticipatory things we can do?
22. **Mr. Lee:** Heard three things from manufacturers – one, being able to update; consumers are not motivated to buy or look for updated products, so we are not motivated to produce them; regulation is not a good idea.
23. **Mr. Lin:** If the commission agrees, if it is determined something is not working, then should possibly go to regulation.
24. **Mr. Gallagher:** Regulations are fragmented. If regulators develop regulations on their own it will not work. There must be a core set of practices. This element must be present. We must be aware of how it unfolds. Whatever it is, it must be muscular.
25. **Mr. Chabinsky:** Regulatory bodies should be assessing utilization now.
26. **Mr. Gallagher:** Guidance on desired outcomes - If there is not compliance, recommend regulation.
27. **Mr. Chabinsky:** Much of the activity we want to see is in unregulated industry. Could use the term "mandate" for unregulated sectors.
28. **Mr. Donilon:** Some proposed recommendations are different ideas. Health and safety regulators should see this as a problem, and not be held back from starting to work on solutions. We don't want to stop the current regulatory system from working. We need to encourage adoption of these other practices.
29. **Mr. Gallagher:** If we are looking at connected devices, is it not saying all devices must be regulated? Not necessarily. There are standards for some things.
30. **Mr. Lee:** It is one of the toughest issues for us.
31. **Mr. Gallagher:** Careless language in this section will have big consequences. In areas where there is consumer harm potential, we are in pretty good shape. There must be risk based assessments.
32. **Mr. Chabinsky:** Minimum function as a design property; categorization of consumer device.

xliv. Consumer

1. Two proposed recommendations in this section: Labelling and usability. Labeling cross-references to connected devices. Has awareness and consumer bill of rights.
2. **Mr. Palmisano:** Raise awareness within the technology itself. We can create the opportunity with in the recommendation itself to allow development of these technologies. "Security awareness by design" is a good recommendation.
3. **Ms. Anton:** FTC enforces unfair or deceptive actions. Companies can sidestep these. ***(Identified other language issues to work on with staff).***
4. **Mr. Lin:** Is the bill of rights aspirational? (Commissioners agreed yes).
5. **Ms. Anton:** Was the whole idea of a rating system replaced by a label? Yes. The label provides information. The rating system gives means of comparison. Confirm the use of both with Mudge and Sara. Is mandatory disclosure being considered? Mandatory disclosure is a

company process. Rating on software security products, provided as self-certification. We should confirm the language.

6. **Mr. Sullivan:** The recommendation seems wishy-washy with the organization not being identified. Consumer Reports model is familiar to most people. It gives greater comfort level. Language will be added.
7. **Mr. Lee:** It is indirect.
8. **Mr. Sullivan:** What is the role of the next administration here? Self-certification is the usual now.
9. **Ms. Todt:** We can revise language of the label to get the right language. Could cite Mudge as an example, and welcome others.
10. **Mr. Gallagher:** We have talked about this as a consumer section. It might be where a general education could be called for. Also, privacy framework could be built up. Some of the other things in the report could fit in this imperative.
11. Government – there are things the government can do to fix itself. Two pieces to present. Potential recommendations – government as role model. Second builds on cybersecurity framework.
12. **Mr. Alexander:** Several issues in this part: Separate operations from mission; clarify roles in government; industry is more confused with government roles; people confuse response with defense. There is no plan that integrates industry and government response. One reason is that we don't understand what the government roles are. The commission must address preparedness in this area. Mr. Gallagher's description helps speak to the role of government.
13. **Mr. Sullivan;** There should be an agency in the government to work on prevention.
14. **Mr. Palmisano:** Could create agency, have it report to DHS.
15. **Mr. Gallagher;** When we look at the mission side, we have to talk about what happens. The report needs a strong recommendation about it.
16. **Mr. Alexander:** It comes back to clarification of roles. Not everyone understands who responds when, and how it is differentiated. The question is do we organize differently than we do today. The question is how to do it. We have the National Guard for state, local, tribal and territorial (SLTT). We gain more by unity of effort, than with so many pieces that no one understands.
17. **Mr. Donilon:** In regards to a new agency – Can one agency have civilian and military in the same? It is a difficult thing. It isn't legal today, and could be a bridge too far.
18. **Mr. Alexander:** There are a series of issues that impact ability to do missions in cyber.
19. **Mr. Gallagher:** We may not want to make a recommendation, but speak to the current situation. PPD-41 deals with incident response and prevention. Consolidating capabilities is the challenge. Ensuring accountability is also a challenge. Agencies don't tell each other what to do. The White House giving direction works. Issues are broader than CISO responsibilities.

20. **Mr. Gallagher:** The problem is not lack of authority; it is confusion on authority. Use of information security technologies cannot be separated from mission. It is not a structural problem, it's a leadership problem.
21. **Mr. Lee:** It seems cyber operations and missions will become an increasingly consuming part.
22. **Mr. Gallagher:** There are multiple functions that all have to build capacity, and there must be an effective interagency process to make things works.
23. **Mr. Gallagher:** There is uneven capacity. DHS has insufficient capacity for their mission. There is another set of issues that are in the mix. Many other agencies use information as well.
24. **Mr. Gallagher:** We are managing to requirements, instead of managing risk. I would not argue for a central budget. If we integrate risk, then integrate management. Capital expenditures, need to become operational expenditure. Repair is better than refresh.
25. **Mr. Alexander:** We do need to clarify roles and responsibilities. We may need assistance from the next administration.
26. **Mr. Donilon:** Develop mission statement for the civilian agencies, with some responsibilities defined. How do priorities get set?
27. **Mr. Gallagher:** Integrate NIST framework into what the agencies are doing. Accountability happens now, but cyber is not part of it yet. Orders come from different places, with insufficient budget to do either. The framework allows movement from simply following rules, to being innovative. It is true the government has largely ignored the NIST framework. It is a different way to manage risk. Initially there could be a basic measurement process. The evaluation process for mission is done through OMB process currently.
28. **Mr. Alexander:** Security functions are typically risk managers, not builders.
29. **Ms. Todt:** Staff can work with Pat on language for joint, deliberate planning, precision on roles and responsibilities.
30. **Mr. Lin:** There’s a paper on why there is inactivity in the government from Mr. Gallagher. Can it be referenced in the report?
31. **Ms. Todt:** We will make sure the content is in the current report.
32. There is no manager for operations at agencies. Appropriate people can report, including cyber.
33. **Mr. Lee:** Architecture – Mr. Alexander’s discussion - the concept may have been abstract, but it may have helped to resolve questions we are currently discussing. A defined architecture can help people understand functions. Staff will work with Mr. Gallagher on language.

xlv. Workforce

1. One recommendation for national workforce, and one for government workforce.
2. The primary recommendation is to address gaps through surge, while the rest develops.

3. **Ms. Anton:** Why is it called PMF? It is an existing program, but create a group for cybersecurity. It should be called PCF. This program is for students coming out of grad school; but it could be done for mid-career as well.
4. **Mr. Gallagher:** This mixes strategies for government and national. Can we promote general activities? Innovation will tie to workforce.
5. **Mr. Chabinsky:** Noting Secretary Pritzker's reference to poaching in the government - we should not make that problem worse.
6. **Mr. Sullivan:** We should not be afraid of poaching. People moving back and forth from government creates a healthy respect for government.
7. **Mr. Chabinsky:** We should consider the problem from the government point of view. It is a real issue for the civilian agencies. It makes the government compete with itself.
8. **Mr. Lin:** We were going to speak about the need for cyber development for managers.
9. **Mr. Gallagher**: The tone sounds like we are treating people like commodities. We want to avoid that.

Summary and Next Steps

10. **Ms. Todt:** Will revise first four proposed imperatives by this Friday. Commission feedback on these by 11/14. Next imperatives on 11/16. Remaining sections 11/21. Draft returned by the 23rd. Final draft the following Monday. I will provide schedule in writing. The table will be revised tonight, to be distributed tomorrow.
11. **Mr. Donilon:** Comments on memo, revision on SME internet of things – language should not recommend re-creating the wheel.