Commission on Enhancing National Cybersecurity

Preparatory Working Group Meeting
Department of Commerce
Herbert Clark Hoover Building
1401 Constitution Avenue, NW, Room 43019
Washington, DC 20230
September 20, 2016; 9AM-2PM

Attendees

Commissioners: Tom Donilon, Sam Palmisano, Annie Anton, Maggie Wilderotter, Peter Lee, Steve Chabinsky, Heather Murren, Herb Lin, Joe Sullivan,

Others: Kiersten Todt, Adam Sedgewick, John Banghart, JP Chalpin, Kevin Stine, Eric Goldstein, Diego Rosero, Matt Barrett, Jeff Greene, Mark Barrett, Robin Drake, Rob Knake, Jamie Crooks, Alice Falk, Matt Smith, Roger Cressey, Jon Boyens, Clete Johnson, Bruce Potter, Kimberley Raleigh, Michelle Harman, Donna Dodson, Alex Niejelow, Matt Scholl, Rodney Petersen, Amy Mahn

Agenda

I. Governance
II. Internet of Things
III. Education
IV. Workforce
V. Next Steps

I. Governance: Presented by Adam Sedgewick and John Banghart

a. We have been consistent for a while on the topic of making the government a leader in cybersecurity. We have had a few different documents submitted on the topic leading up to today.
    i. Kate Charlet, DOD, provided a paper on government positions.
    ii. Michael Daniel and Ed Felton presented to the commission last week.
b. There are key concepts that keep repeating.
c. Three requirements: The authority to act, the incentive to act, the capacity to act.
    i. Authority – What are the true authorities for cybersecurity? We heard the Commerce view yesterday in Secretary Pritzker's address.
    ii. Incentives – There is a general tendency towards risk avoidance. Is cyber one of the true priorities?
    iii. Capacity – Do all departments and agencies all have the capacity to act as needed?
    iv. Five areas

1. Chief information officer (CIO) should lay out the framework for all agencies. What is the strategy? Will add "Measurable metrics."
2. Government must consolidate and manage network architecture.
3. The next president should the lead effort for consolidated services.
4. Should include a place holder for slowing down procurement.
5. Congress must ensure OMB and DHS have sufficient resources.

v. Comments on Mr. Gallagher's document
   1. The bias has always been that there is not a shortage of authorities.
   2. We have tried to reframe with a different hypothesis.
   3. Agencies can be viewed as having two roles. Using IT to facilitate the mission. Then, what do those responsibilities look like?
   4. IT does not just replace the business process; it can re-factor the whole process of doing business.
   5. Incidents can be considered off-normal and normal. There is no complete incident response plan. It has been in draft for eight years. It should be in place and in practice.
   6. The technology prompts a rethink on where responsibilities lie. The federal government acts more like a group of small businesses than a single large enterprise.
   7. **Mr. Gallagher:** All agencies should have secure pipes. A cloud integrator may be the solution.
   8. We can move from a punitive mindset to a defensive mindset in terms of network requirements compliance by agencies. Turning off the network access is not punitive, but a defensive action to protect everyone.

vi. **Mr. Palmisano:** Provide a default set of services for small agencies. May offer alternatives if agencies are willing to pay for it.

vii. **Ms. Wilderotter:** What are the economies of scale for opt in/opt out?
   1. **Mr. Gallagher:** Urging buy-in with cost for service as incentive. Economics should work in government as well as in the private sector. Economic motivations will carry the day.
   2. **Mr. Lee:** As far as details of shared services. We need to be a bit careful. It may not be in the government's interest to have a sole service provider. There are also specific statutory requirements on agencies. Decisions are being made in a thousand different places currently.
   3. **Mr. Palmisano:** The government can build its own cloud. It may not need to be dependent on a different provider.
   4. **Mr. Lee:** Structurally, what does this look like? We may need to be very precise in the language. It may be possible to conceive of some parts of the government being offline, to take down parts of the infrastructure, on a timeline schedule.

5. Mr. Gallagher's paper touched on the issue of culture. The government has a very risk averse culture today, and how do we go about changing that? It is about empowering CEOs, and responsibilities to mission.
6. It is interesting to note government leaders almost never talk about the NIST framework; whereas the private sector almost always does.
7. If there is one place for getting commodities, it may be worth going with that one place (one-stop shop).
    a. **Mr. Lin:** Is additional legislation required? We should separate what creates legislation and what doesn't, and what can be done with existing legislation.
    b. **Mr. Gallagher:** If there is mismatch in authority, it sets up wrong expectations.
    c. **Mr. Lin:** Would not want to see the commission recommend a particular course, and then nothing is able to happen because of legislation.
8. **Ms. Todt:** Consolidation of priorities – Propose these five issues in the paper be called out (there may be others)
    a. Need for national cyber strategy,
    b. Create the Special Assistant to the President,
    c. Finish the national cyber incident response plan
    d. consolidation of civilian infrastructure and
    e. Small agency support.
        i. **Mr. Donilon:** Goal could be a consolidated agency in DHS for example.
9. **Ms. Todt:** Staff will work on what steps can be taken short of legislation to create change in the government (functions, people, leadership, etc).
    a. **Ms. Wilderotter:** We should always look for low hanging fruit in recommendations. We should also be careful about being proscriptive in what is recommended. It should be framed in a way that there is choice on course of action.
10. The pay scale in government cannot compete with industry (from Secretary Pritzker's comments).
    a. **Mr. Palmisano:** Pay scale will not solve the workforce problem in the near term. Real change in the workforce issue will not happen in the term of the next administration.
    b. **Ms. Anton:** Salary will help retain staff. The government will not be able to match on equity and people will jump to industry.
    c. **Mr. Palmisano:** It can team with private sector or academia. It can then reimburse the private sector for its participation. These teams can provide skillsets.

d. **Mr. Palmisano:** Government provides specific areas for collaboration, and work for results.
e. The government would fund research in large-scale projects. There is an existing model in DoD to work with private sector to help solve skill shortage issue.
f. **Ms. Wilderotter:** One suggestion is to raise pay to where it needs to be, however it can be accomplished.
g. There are models that can be scaled up. There are pay issues. Mid-career opportunities can be made available. Non-federal, the country has a problem in this area. We can learn from prior successful projects. There are over a million jobs open today that need to be filled.
h. **Ms. Wilderotter:** Can technology be used to automate processes? Can technology fill the gap in some areas?
i. Could there be an independent organization to broker partnerships? It's been done at the state level. It allows more flexibility in contracting and hiring.
j. **Mr. Donilon:** There is a valid point that cyber is handled at too low a level in the government. The CIO panel from the August 3rd meeting recommended creating an Assistant to the President position. It was originally proposed years ago, but was never done. It was the person in in the White House to coordinate all the part at a policy level.
k. **Mr. Donilon:** Currently, cyber comes under the homeland security assistant to the president. The cyber position needs to be someone who will be solely devoted to cybersecurity.
l. **Mr. Donilon and Ms. Todt:** Structure: new Federal CISO position is the person sets the standards. There should be a broader advisory function.
m. **Ms. Wilderotter:** Remove the "cybersecurity coordinator" language. Should it be changed to a "cyber-incident response coordinator"?
    i. It should be considered as a technical advisor. The position should be permanent. There have been two – one in the Clinton administration, and one in the current one.
    ii. The position could be called a "cyber incident coordinator".
    iii. **Mr. Gallagher:** It can also be argued that the term is too narrow. What will our position be at any international conference? Someone will need to coordinate. This is contrary to FISMA.

n. **Mr. Donilon:** OMB authority puts responsibility in national security. The OMB director will never be the one to coordinate a response to a cybersecurity attack.
o. **Mr. Gallagher:** The ability of the government to shift in posture in the face of an incident - Are there unintended consequences if we stay in that mode in normal operations? Yes, possibly.
    i. There is also an international piece. Is the U.S. giving aid and comfort to other countries?
    ii. **Mr. Donilon:** It becomes like a law enforcement action. We want to be informed by it, but not run by it. There is no way the 30-day sprint would have taken place without leadership from the White House.
    iii. **Mr. Lin:** If cybersecurity is placed under the NSC, it may be alarmist to privacy advocates and others.
    iv. **Ms. Anton:** I don't like the idea of "incident". It should be a technical advisor on the NSC, to make it more about design and networks. It is not a permanent position. It should be made so. Critical for privacy and civil liberties for the nation.
    v. **Ms. Todt:** Perspective on the government continuing to store, and never getting rid of data. It will help to address privacy concerns.
p. **Mr. Donilon:** In terms of elevating the Michael Daniel role, the paper argues for an empowered CISO role. This are in line with yesterday's discussion. Experienced people argued for it yesterday.
q. Reference to the job description and authorities is important to this section. It is the path to a more unified Federal network.
r. **Mr. Gallagher:** It is a case of muscular authorities. How will one person carry that out officially? It can be done within the software. The network can govern access and denial.
s. Discussion of leadership culture and accountability at the cabinet level is important to open with in the paper.
t. **Mr. Sullivan:** What do we want it to do? Run the federal network and incident response. Should they both be in the same place? Generally separation of functions should apply. The team that runs the network should not be the team that does incident response.

u. There has been an evolution of risk management organizations from being subservient to being more independent or at the peer level.
v. **Mr. Sullivan:** There is more of a "risk leader role" today. General counsel is often the final risk officer in corporate settings.
w. **Mr. Gallagher:** Risk should not be totally segregated, according to Secretary Pritzker's comments.
x. **Mr. Donilon:** Question on proposal – the notion is, many of these capabilities already exist. It works most of the time, but it can be better. What is the proposal here?
    i. **Mr. Banghart:** Capabilities exist, DHS is doing this, but because of gap of how it's structured, we have capability in government that works most of time but not as well as it can. We should be providing more direction and focus to one unit to handle a single problem. Existing authorities and systems are not structured in a way that gives a consistent message over time.
    ii. **Mr. Goldstein** – The intent of the recommendation is that DHS is directly empowered to provide the security function. Incident response and agency support for the entire government. Putting a single body in charge of government security.
y. **Mr. Banghart:** The recommendations attempt to move to more of an enterprise risk view. It starts at the top with the President. It all takes place today, but it doesn't work as well as it could work.
    i. **Mr. Gallagher:** It essentially makes NPPD an agency.
    ii. **Ms. Murren:** Should frame it as a re-organization of efforts, rather than creating a new agency. DHS has current legislation in process to do this.
z. **Mr. Johnson:** Secretary Pritzker's points about accountability - Decentralized services should be in fact services. It establishes a customer services relationship rather than a hierarchical relationship (as in an agency).
    i. Should we list services to be included?
    ii. Protection vs. policy
    iii. **Mr. Palmisano:** Service providers should be trusted. Outages should not happen. There must be credible people providing services.
aa. **Ms. Wilderotter:** If we are making a recommendation specific to the mission, we must understand if they are

qualified to do it. There must be a level of talent and measure of accountability.

bb. **Ms. Anton:** GAO studies typically run on two year cycles.

cc. **Mr. Donilon:** There should be a set of requirements for agencies to get on the network. They should require GSA approved connections. There must be some way to police it. Need to discuss the agenda and federal systems as well as how to extend NIST Framework into the federal government. Is it adopted in risk management?

dd. Do agencies follow risk management approach? Some yes, some no.

ee. **Mr. Donilon:** Can the framework be expanded into more places? It should be used as tool to affect behaviors.

    i. **Ms. Dodson:** The framework is more oriented to small and medium organizations. It may not be oriented to larger organizations. Two parts to the frameworks – size bars and maturity model intended to raise levels.

    ii. **Ms. Anton:** Should agencies be at a certain level in the next two years? Agencies should be showing progress in audits.

    iii. The framework is designed to evolve over time. There should be evolutions upward.

ff. **Mr. Palmisano:** There is an enterprise risk model. Looking at end-to-end risk is a different level of requirements. Suggest an enterprise risk model for the federal government. Risk decisions are reviewed by OMB at least quarterly. There are defined processes for enterprise risk management. They should be coordinated with Inspectors General offices.

gg. **Mr. Chabinsky:** There is a need for chief risk officers. Tom Donahue said we don't have risk calculated. What is idea of creating agency just for infrastructure

hh. Agency type functions – Cyber FEMA

    i. **Mr. Gallagher:** Accountability is laid out. Greater capability of who runs networks covered under the Cyber Threat Intelligence Integration Center (CTTIC). DHS might be the most natural choice for certain services.

    ii. **Mr. Sedgewick:** For certain services, yes. GSA has evolved a lot in the last few years but still receive no appropriations. It would require some significant changes.

iii. **Mr. Palmisano:** Someone needs to be given responsibility. There will be an upfront bubble of expenditures. Someone must have authority and funding to accomplish changes.
iv. **Ms. Wilderotter:** A one stop shop may be simpler. Agencies can purchase using GSA schedules today. Agencies may deal directly with vendors. GSA charges a tax. Agencies may choose not to pay that tax.

ii. A challenge is trust in the current system. We have to own the whole thing – the entire process for agencies.

jj. **Mr. Donilon:** Is there a list of approved connections?
i. **Mr. Banghart:** Yes, there is a list of approved connections. There are also rogue connections.
ii. **Mr. Donilon:** Why is this tolerated?
iii. **Mr. Banghart:** It may also be a case of bad metrics.
iv. **Mr. Lee:** Exact provisioning of fiscal pipes is one question. There is identity management and authentication. These are all things where there is cyber security value.
v. **Mr. Sullivan:** The major debate is network services vs individual applications.
vi. **Mr. Palmisano:** New equipment should be internet ready, legacy equipment should be killed and not made internet compliant at all.
vii. **Mr. Lee:** Will there be a clear set of goals that are also accessible? Can we show some movement or actual change we can call out with some level of assessment?
viii. Statement at the beginning, followed by suggested initiatives, and measures of success and continuous diagnostics and mitigation (CDM) recommendation.
ix. The end result is some metrics to measure success.
x. **Mr. Donilon:** Should include enterprise risk management as a principle for the federal government, federal network requirements for access. Should consider pulling NIST framework throughout the recommendations. We should attempt to pull out core themes for the next president, and possibly a statement the leadership that owns accountabilities should provide metrics at least annually.

xi. **Next steps** – Staff will continue to update proposed ideas for the commission.
xii. All will continue thinking about the agency question.

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

a. Definitions – What does "internet of things" mean? The paper focuses more on how devices are used. It may be different in different places. Is it too late to weigh in on IoT security? We think it is not too late. There is still an opportunity to create change in a significant way.
b. Everything still fits under risk management. The same principles of IT security will apply.
c. Broader applications – Next generation devices should be secure, delays in implementation for security weigh against lifesaving potential and potential gains in security overall.
d. In critical infrastructure, the government will have more control.
e. IoT is an architecture that connects a lot of things. How can we avoid building the legacy of the future?
f. This morning DOT released their rubric on vehicle to vehicle communication. It has ratings SAE0-SAE5. It includes external standards, responsibilities for agencies and vendors. Commissioners may wish to take a look at this document and determine if it can be a sample for other sectors.
g. Did not propose a recommendation oriented to consumers regarding options to connect, how, or not to connect. It should be dealt with in the consumer section.
h. Consumer Product Safety Commission (CPSC) does have a role here. Patterns of injuries, etc. Some vertical regulatory agencies are looking for standards on cybersecurity.
i. The proposed recommendation does not take a clear position. Is there a correct path here? Also must deal with the threat of regulation.
    i. Recommendations should be focused on achieving outcomes, not directing what to do. Context will be important. Fully automated device (such as for cars) requirements will be defined by states. Infotainment should not integrate with vehicle operation system.
    ii. Medical and auto are areas where the government has authority.
j. **Mr. Lee and Ms. Wilderotter:** Proposed recommendations are too vague and open ended and will not be taken well by industry. There must be balance in dealing with technologies with personal safety implications.
k. **Mr. Chabinsky:** If there are areas of critical infrastructure where there are no federal authorities it is important for the commission to know. We need to research. Regulations vs communication. Does the federal government have authority in DC? We should know.
l. **Ms. Murren and Ms. Todt**: Security at the application level - How should mobile be treated? Is this discussion here or at the consumer side?

i. It calls attention to how the document is organized. Maybe consumer is where IoT and some other areas may fall.
ii. Need to discuss some clear organization of the document.

m. **Mr. Lin:** Suggest dividing IoT section into consumer and critical infrastructure.
n. **Mr. Lin:** May need to re-examine and redefine what critical infrastructure is.
i. It is bold but creates a degree of risk for the report.
o. **Ms. Anton:** Who is reviewing comments from the request for information (RFI)?
p. **Ms. Todt:** Comments are online by topics. Responses to the RFI are available publically at Nist.gov/cybersecurity. There was a late surge of responses on the last day. Comments will be distributed when available.
q. Recommend discussing NIST publication of "networks of things."
r. **Ms. Wilderotter:** Transparency issue. Should take a look at the National Security Telecommunications Advisory Committee (NSTAC) report and 15 CEOs with DHS. The material is still current. "Carrot" - Gold set of standards and "stick" - liability. What do we use to drive standards? There are regulated sectors and consumers side with those agencies.
s. The question is can we use any or all of those, and should we try to get at the standards. We need to define a path forward to protect the country.
t. **Mr. Donilon:** Sectors are becoming blurred. Sometime in the future, there will be just things on the internet. The NSTAC report raised flags.
u. **Mr. Lee:** In principle, critical infrastructure is separate from social media.
v. **Ms. Todt:** There are different equities for the nation in critical infrastructure. The definition of critical infrastructure is dynamic.
w. **Ms. Murren:** Where these fall can be reframed. The group can speak of present and the future, which means all these areas will converge.
x. **Mr. Sullivan;** The way the government is structured, there is a gap in protection of consumers. The government doesn't have a team to predict consumer harm. That may be why there is no idea about how to fix IoT. The Federal Trade Commission (FTC) deals with some related areas. This falls into the harmonization discussion.
i. **Mr. Donilon:** Suggest we don't remove IoT and make it a separate discussion. It points to an emerging problem. NIST works with industry to develop core standards.
ii. **Mr. Palmisano and Mr. Chabinsky:** Should be against broadly adopted devices with no protection. The Commission can spend a lot of time on critical infrastructure, but there is an emerging consumer protection gap. It becomes an educational and disclosure information sharing activity. It should fall to agencies that attempt to protect consumers.
y. Manual controls as backup - less specificity on manual, and more on fail-safe.
z. Possibly have a goal on UL lab certification or label? UL has already started that effort. Documenting checks done while building. They do not feel they can now certify digital devices but are working towards it.
aa. **Mr. Donilon:** The commission may want to consider talking to the FTC about device security and physical security.

bb. **Mr. Chabinsky:** Liability – Some level of stick needs to exist. When dealing with personal safety it is not acceptable to allow unsecured devices. It is time for people to comply. Things can be done today to make devices safe. Old techniques could apply. Software was designed never to fail.
    i. Propose an argument for simplistic devices. Allow industry some time to comply, but after that consequences apply.
    ii. Development techniques are less important than the possibility of failure. Consumers have a risk based choice about purchasing risky technology.
    iii. **Mr. Palmisano:** Labels may help define where risks lie.
    iv. **Ms. Murren:** Consumers can only make risk based choices when they are adequately informed.
    v. The argument "it can't be done" is a rationalization. There must be some incentive for things to be done and for the creation of products that will not have negative effects.
    vi. **Mr. Lee:** This is an important recommendation. What is liability in scenarios involving connected devices, particularly if there is direct physical harm?
    vii. Liability issue needs further discussion. The commission and staff will work with Ms. Raleigh to get information from DOJ.

cc. Will think about structuring IoT, consumer and critical infrastructure in a thoughtful way.

dd. IoT will be a key part of critical infrastructure. Commission will consider defining in forward-looking language.

ee. Liability in terms of government action? Only in terms of personal safety not inconvenience. Need professional advice in this area. Government action on a narrow set of circumstances. Definition of critical infrastructure is moving beyond traditional definitions.

ff. Snowden interview with Financial Times: no protection until there is liability for faulty software.

gg. Mr. Palmisano: Should not have to accept that single purpose IoT devices can't be secure. A pacemaker shouldn't browse the internet while it's in your heart.

hh. **Mr. Greene:** There are technologists in favor of software liability.
    i. **Ms. Wilderotter:** Must be careful not to stifle innovation. There could be a regulatory aspect to the discussion.
    ii. **Mr. Palmisano:** Safe harbor may be applicable. If we are truly willing to save lives, we will go to those lengths.
    iii. There was the first mention of facing up to a tradeoff. More of that discussion needs to happen. Sometimes something we have to give up something we want to get security.

ii. Cars need to be designed in a secure and automated fashion so that they cannot be hacked.

jj. Software development practices for IoT are becoming blurred over time. It is an opportunity to improve software engineering practices across the board.
    i. Reducing functionality in devices is safer.

ii. Design fault tolerant networks.

kk. **Mr. Greene:** The Safety Act was designed to solve a problem. It may not apply as it solves a problem that does not exist in cyber. It may encourage stagnation and keep smaller companies out of the market.
   i. The Safety Act has become something different than what it was originally intended. It is being proposed is that the bar be lowered to include terror acts or cyber incidents.
   ii. Secondly, it puts DHS in direct competition with the private sector and certified products.

ll. Should address privacy in the report.

III. Education – Presented by Rodney Petersen

a. Worked with Burning Glass and CompTIA to develop a cyber job map. It will help develop a standardized picture of demand. We don't know if corporate budgets will support actually hiring people.
b. The Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) grants were announced today. There will be five recipients around the country. The grants will address local workforce needs.
c. NSF and NSA are key players in this area. The Department of Education is not a major player in this area.
d. Proposed recommendations –
   i. There is a focus on apprenticeship. It may be one of the more promising areas over the next ten years. Apprenticeships in cyber should be a recommendation.
   ii. There should be a focus on developing cyber elementary school curricula. Awareness is very important. We want to introduce kids to careers as soon as possible. Safety messages and career messages may be more important than "how to."
   iii. President's program, Computer Science for All was a budget proposal with funds for states to implement.
e. **Mr. Chabinsky and Ms. Todt**: Are there metrics to demonstrate apprenticeship is working?
f. **Mr. Petersen:** Research is done in Canada to show positive returns on apprenticeship. We have not done as much here. The move to apprenticeship is a change. Primary technical schools have sprung up around the country. Technical and diploma at graduation and job at reasonable rate. Administration has been very supportive of the program.
   i. For workforce, there are many good ideas, but metrics have been hard to define.
   ii. People should receive a job at a market rate in government. There should be some definition of success and determine percent of completion, etch.
   iii. May be support for adding cybersecurity to existing curriculums.

iv. Linking to computer science may be counterproductive when we are moving to interdisciplinary majors.
    1. **Ms. Wilderotter:** Could it not be opened to current government employees? They have a propensity to stay.

g. K-12 education - Since there are other efforts to inject more serious education at the primary level, are there possibilities for working together? Middle school level may have greater possibilities than primary. Career and technical education (CTE) tracks in high school include cybersecurity studies.
    i. **Ms. Anton**: Middle and secondary education are not mentioned.
    ii. **Mr. Lin:** A boot camp in cyber may be helpful. There are many more positions that require familiarity in cyber that currently do not require that knowledge.

h. There seems to be a big lack in skills at the base apprenticeship level, which could be presented as a findings. While not a recommendation, it should be recognized.

i. Anyone who uses a computer can use cyber knowledge.

j. **Mr. Donilon:** Do the proposed recommendations currently present the number in the finding?

k. **Mr. Petersen:** Not currently. The hundred thousand jobs by 2020 can come from multiple sources.

l. Are we going to train people for jobs that won't be there because of automation?

m. **Mr. Palmisano:** Analyzed skill set by class of job from work on China.

n. **Mr. Petersen:** Ideally, recommendations should support the finding by 2020.

o. **Mr. Petersen:** The National Initiative for Cybersecurity Education (NICE) has a strategic plan it presented to Congress. It contains apprenticeship element.
    i. Incentives for this program - Will require employer partnership. Employers want skills, not degrees. Certifiable, online curriculum would be helpful.
    ii. Certifiable professions. Skills are transferable. Companies pay for training. If students leave before an agreed upon term, they repay employers. Long term metrics could be collected.
    iii. Online courses are easy to implement.

p. **Mr. Lin:** The skills needed to do cyber in real time are different from traditional IT work.

IV. Critical Infrastructure Workforce – Presented by Matt Barrett

a. The group did multiple interviews with infrastructure people. They are not IT or cybersecurity experts. Components are showing up with IT built in. New infrastructure elements may need code to integrate with old elements.

b. Federal desktop core configuration – a group of entities created a standard set of Windows settings.

c. Proposed Recommendation – A standardized set of system settings.
    i. Can we bring security infrastructure assessments into this area?
    ii. Update cycles for infrastructure are very different from software.

iii. From Houston discussion - took 8 years to deploy to the grid. Infrastructure can be made more resilient using these methods.

d. Can view the label concept as applicable to the critical infrastructure area.
e. **Ms. Anton:** I am concerned with language in proposed recommendation using word "encourage," needs some incentive if it's what you want to see happen. "Encourage" seems vacuous as a word. There is a need for a workforce that understands what's built is secure by default. It shouldn't be on consumer; devices should just be secure.
    i. **Mr. Lin:** Everyone should issue products secure by default but not everyone's going to do that.
    ii. This proposed recommendation may not be getting at the ultimate goal, so staff will revise.
f. Section on the federal government includes three proposed recommendations from Secretary Pritzker.
    i. **Mr. Donilon;** Workforce section on federal hiring - some places in the government do it well (flexibility, pay, shorter term opportunities).
    ii. There's a separate section on hiring technology talent into the federal government

V. Next Steps

a. Staff will meet tomorrow and review sections discussed today.
b. Talk through timeline of remaining areas.
c. Carry on discussion in the weekly calls.
d. Set schedule for the next five weeks.