Meeting Minutes

Attendees:

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

Others: Kiersten Todt, Kevin Stine, Donna Dodson, Matt Scholl, Robert Silvers, Burden Walker, David Stearn, Jeff Greene, Amy Mahn, Rob Knake, Karen Scarfone, Alex Niejelow (for Ajay Banga), Camille Stewart, Lisa Barr, Robin Drake

Agenda:

I. Discussion of the State, Local, Tribal government working paper led by David Stearn and Kevin Stine
II. Discussion of the Internet of Things working paper led by Matt Scholl
III. Next Steps/Wrap up

Discussion:

I. Discussion of the State, Local, Tribal Government Working Paper led by Kevin Stine and David Stearn

a. State and local government maintain a lot of critical information.
b. There are several equities. Coordinating with states can mean diff things. There is no single point of entry - some of CIO, CISO, fusion center, local government or others.
c. The federal government supports state and local governments through the Multi-State Information Sharing & Analysis Center (MS-ISAC) based in New York, and there are other kinds of funding.
d. Several challenges were identified by DHS, according to the National Association of CIO Officers and other reports.
    i. State authority is often limited leading to fragmentation.
    ii. There is a lack of integration and planning for cyber incidents.
e. Often there is competition for leadership in responses to incidents.
f. Discussion of proposed ecommendations:
    i. First, the Homeland Security Advisory Council sub-committee was set up to advise in this area.
        1. A state cyber framework can resolve issues, provide coordination, roles and responsibilities,
        2. It is extremely important for incident response and informing those involved. The framework may take several forms, but is most useful, when it promotes information sharing. It will allow better alignment, and allow hiring better people.
    ii. Second, take care of networks. Good cyber-hygiene is crucial. We have received feedback to put more emphasis on cyber-hygiene.
        1. More analysis is needed on strategic intelligence.
g. Federal Proposed Recommendations:
    i. First, the federal government should increase awareness for FEMA grants and initiative. It's not widely publicized that these grants are available.
    ii. Second, enhance communication with state governments, on what's available and improve communication in general.

h. State and local governments can have economies of scale in purchasing with assistance from the federal government. It is available to the state and local government, will enable them to save money.
i. Discussion on the State, Local, Tribal Governments working paper
    i. **Mr. Lin:** Likes the paper overall. It is missing a proposed recommendation or finding regarding state, local, and tribal governments learning from each other. There should be horizontal learning.
        1. There are working groups in the state and local that have the opportunity to work together.
        2. There should be a more tactical focus on information sharing.
    ii. **Mr. Stearn:** What mirrors this is the MS-ISAC. There are several working groups focused on key areas like industrial control systems, cyber exercises, business continuity, awareness and outreach, etc. These are opportunities where state and local members can speak with their peers about policy development, some initiatives they have going on, and share best practices.
    iii. **Ms. Murren:** States should have comparative data, and possibly organize basic recommendations. Some states may not know how to do budgets with cybersecurity.
    iv. **Mr. Gallagher:** Need to account for state roles. The paper looks at the protective/preventative side and it looks generic. Have you looked at the areas where states are unique? There are exposure points in state/local that are unique from the federal government. Are there things we should pay attention to?
        1. Those things should be covered in state and local responses.
        2. In terms of voting technology, DHS is following.
        3. The authority for voting is actually a state activity, outside federal authority.
    v. **Mr. Gallagher:** What about grant funding for the states? There are a number of types of funding. Has anyone catalogued the footprints available at the state level?
        1. **Mr. Stearn:** DHS does not handle that. We looked at best practices for voting, etc.
        2. **Mr. Alexander:** I have not heard this in any public sector discussions. Is there any sense of the amount of uptake for the NIST framework?
            a. **Mr. Stine:** There are events that encourage the uptake of the NIST framework. There has been good feedback on these events.
            b. **Mr. Stearn:** When DHS does risk assessments, the questions are aligned to the NIST framework.
            c. We would like to make the framework the common lexicon going forward.
        3. **Mr. Donilon:** The commission should be recommending the states adopt best practices. We should look at and raises up the leading states best practices.
            a. Could suggest states should adopt the NIST Framework.
            b. In general, we should take a harder line on proposed recommendations.
            c. We should emphasize the many good things that are happening in the states.

i. In terms of voting systems, we should define voting systems as critical infrastructure.

d. Make stronger suggested recommendations on workforce. We hope to have a broad spectrum recommendation directed to the next president.

e. **Mr. Chabinsky:** A lot of the areas in the proposed recommendation would benefit from standardization and best practices. We may be able to drive what the standards are. More is needed on the federal fusion level for law enforcement. Can we elevate state and local cyber-crime issues to the federal side in terms of collaboration?
    i. **Mr. Stearn:** DHS works closely with law enforcement partners. DHS assists with incident mitigation, law enforcement goes after the criminals. The FBI and others are represented in NCCIC. This is where collaboration most often happens.

f. **Ms. Murren:** A best practices summary for states would be helpful. States are not always able to do this independently. Providing support with the best practices, will be a big help in allowing states to carry out responses.
    i. State and local governments can also offer scholarship for service with the federal government still paying.

g. **Mr. Donilon:** We should not go through this process without having all states at least adopting some NIST framework practices. There are real vulnerabilities, and information to be protected. Some minimum level should be implemented. Whatever is implemented needs to be achievable.
    i. Staff should develop a paper on state best practices. We should not propose anything unachievable. Some element of support should be available.
    ii. We can also look at roles of non-government entities on these issues.

h. Other reactions:
    i. **Mr. Lin:** A statement on digital elections: We can only offer incentives to promote better security, we cannot require it.
    ii. **Mr. Alexander:** Voting is outside federal regulation. We need due diligence to make sure we are not proposing anything contrary to federal law or the Constitution. The voting laws differ also from district to district. It is complicated.
    iii. **Mr. Gallagher:** The discussion paper seemed to have a very strong federal perspective. There needs to more understanding from the state point of view. States have interactions with other entities. It is very DHS-centric.
    iv. **Mr. Donilon:** We should also try to root our proposed recommendations and practices in the states themselves. The piece needs to be state-

centric, and highlight what has worked and what has not.

v. **Ms. Todt:** We need to move from the federal oversight role.

vi. **Mr. Donilon:** To think about – if a state or locality receives some federal money, what should the minimum requirements be? Possibly we should have staff develop something on this topic.

II. Discussion of the Internet of Things Working Paper led by Matt Scholl

a. **Mr. Scholl:** Internet of things is a relatively new technology compared to some of the others being discussed by the commission. There is no unifying definition or description for what it is IoT. Cyber-physical systems is an alternate names for the IoT. IoT is the name that is used by most people.
   i. It usually signifies how state machines (sensor-based), unify with connection technologies, and the backend storage and cloud technologies.

b. It is a sensor gathering data in a physical environment, and storing data in a digital technology.

c. It is a combination of OT and IT technologies, standards are still being worked out.

d. Some combinations of these things become important in this context where they would not otherwise be.

e. Mr. Silvers:
   i. IoT as a topic for commission study is very important. As these techs are designed and deployed, there is a rapidly closing window where it is possible to add security.
   ii. If it's not done now, it will take a generation to add it later.
   iii. The opportunities in the internet of things are unbelievable, but the risks are also very great.
   iv. Ransomware was demonstrated at Black Hat. The attack surface is growing very rapidly.
   v. The imperative here is to include security by design. The government and private sector have roles. There have been good efforts. The U.S. Food and Drug Administration (FDA) published a good paper on security in medical devices.
   vi. There is not an overarching effort that can be referenced. A paper on IoT guiding principles and best practices will be published by DHS in the next few months.
   vii. Guidance from the commission will be welcomed on public and private sector standards. We need to determine what works best. There is an international element as well.
   viii. Inaction will exact a heavy price.

f. **Mr. Greene:** We wanted to convey opportunity and risk. We did not want to convey fear or panic in the report. Time is essential.

g. Ransomware can jump from devices to smart phones and vehicles. Criminals will go **where the money is.**

h. **Mr. Silvers:** Possible metrics or certification on ways to give consumers a way to make informed choices – if they want to buy assured products, they need to have a way of meaningfully doing that. Can drive it through market.

i. In 2012, internet of things was not a common phrase. It's become overused, without a clear definition. There is incredible growth in devices. We are seeing it more and

more in cars. The area of primary concern is installation of sensors without authentication.

j. We may not need to encrypt certain things, but the balance between what's encrypted, and what's not may be important.
k. In terms of risk, there is device and physical security. Machines moving in a way that causes physical harm is a big issue now. Privacy risk is also a critical concern.
l. We have done work showing home health devices can talk to over a dozen domains. Only a fraction of those are encrypted.
m. There is convergence of OT and IT. We looked for programs that will train future experts in OT and IT. Experts are needed who understand both areas. The commission can lend its influence in this area.
n. **Mr. Palmisano:** It is a complex and emerging area. Despite its complexity we can still have influence. Where to start? What area should the commission consider? What should the next president consider?
o. **Mr. Scholl:** One of the critical things is security engineering and security design. Inter-operable standards should be developed across the IoT industry. Unique identification of sensors providing data is crucial. Standards is one area, another is metrics/certifications at the backend for consumers.
p. **Mr. Greene:** Security should be emphasized over getting to market first. The government can lead here by purchasing secure products. Contracts are the fastest way to get the market to respond.
q. **Mr. Lin:** People who make IoT devices may not care about the consumer market. The paper does not include mention of incentives. Also, liability is not mentioned. Having liability for faulty appliances is accepted practice. Liability regimes may assert themselves with more force with the internet of things.
r. **Mr. Donilon:** A built out recommendation on gold certification is key issue for the commission.
s. **Mr. Lee:** Given the ten year view, in ten years the amount of computing power in the internet of things will grow significantly. The threats in the ten-year view are much larger than what the proposals hint at. The potential impact of software updates could be examined more carefully. What about updates in IoT? Also, we have seen explosion in the IoT space, are there things we can physically recommend?
t. **Mr. Gallagher:** We are all zeroing in on the incentive question. A certification regime as a vehicle, it may not have enough agility or speed. We need a bigger set of options. What sorts of things would put the right level of development in this area? A first to market mindset will create an aftermarket of billions of unsecure devices. It may already be too late.
u. **Ms. Todt:** Industries are going to market without device security. We may have missed the first window, but we have second chance.
v. **Mr. Chabinsky:** There needs to be an emphasis on transparency. The first requirement id IoT devices must state intentions in three-five core areas. It at least defines what consumers get. The U.S. standard is to clearly state what key areas are for consumer understanding.
w. **Mr. Lee:** In the 2019-21 time frame, micro-controllers will be fully botnet capable.
x. **Mr. Donilon:** Some of the horses may already be out of the barn. However, we still can lay down some important principles. The issue of liability is very important. Our industrial sector is currently immune to liability. It is constructive to get the debate going for the future.
y. **Ms. Todt:** Staff can develop proposed recommendation on liability. We should make sure the description of the problem is updated.

z. **Ms. Murren:** There should be security guarantees and what's being offered.

III. Next Steps/Wrap up

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