Meeting Minutes

Attendees:

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

Others: Kiersten Todt, Kevin Stine, Donna Dodson, Matt Scholl, Rodney Peterson, Kurt Barker, Adam Sedgewick, Amy Mahn, Rob Knake, Karen Scarfone, Robin Drake

Agenda:

I. Timeline Overview for Working Paper Discussions and Follow Up
II. Discussion of the Workforce working paper led by Rodney Peterson
III. Discussion of the Identity Management working paper led by Donna Dodson
IV. Wrap up/Next Steps

Discussion:

I. Timeline Overview for Working Paper Discussions and Follow Up

a. **Ms. Todt:** Starting today, commissioners and staff will address two of the working paper topics over the next five weeks. They are intended to be building blocks for future use. After every call, staff will be taking the input and creating draft report language. The papers and draft are intended to be points for discussion. Commissioners will have the opportunity to provide feedback or additional thoughts on the minutes, and return them following the meeting.

b. Staff are drafting report language that will go to the commission in September.

  i. The commissioners will have a chance to propose recommendations. These will be accumulated into a larger version of the draft report.

  ii. The Commissioners will prioritize the list with their top ten for discussion with the Commission. The recommendations will be finalized in October.

c. The key points include discussion, identification of findings, proposed recommendations, ideas, and concepts to be included in the report and having an inventory of all those ready for deliberations.

d. Today, two papers will be discussed: First, the Workforce paper, led by Rodney Petersen. He leads the National Initiative for Cybersecurity Education (NICE). Following the cybersecurity and workforce discussion will be discussion of the Identity Management paper, led by Donna Dodson.

II. Discussion of the Workforce Working Paper led by Rodney Petersen

a. Will discuss current state of play, and proposed recommendations and findings.

  i. The paper gives the big picture view across the nation. The federal government has some important activities, such as the national centers of excellence and others. There are a lot of plans and activities for the next one to three years, but not much planned for beyond that.

  ii. Activities at the community college level have greatly increased in the last few years. They are working with high schools, middle schools, as well as universities.

  iii. The communication and coordination across these three groups is good and is improving.

iv. There is concern about the efficiency of investments in education.
v. It requires a system approach. It's not just graduating more college students with degrees in these areas, it really starts with younger students, teachers and employers.
vi. The workforce pipeline is not just for traditional age students, but it should also include non-traditional learners, older adults, and those looking for re-training and certifications.
vii. There have been plenty of sprints, but not so much looking forward to ten years from now.
viii. We need to understand who the players are, and their roles and responsibilities. Investments need to be prioritized and coordinated.
ix. It is also important the employers drive changes in the future. It needs to be considered at the state and local levels, and not just at the national level.
x. What is the change in innovation we need to see? We need new ideas and innovations. It is possible that automation will assist in the future
xi. Commission Questions and Discussion –

    1. **Mr. Palmisano:** When viewing cyber education is it a separate discipline, or included in computer education?
        a. **Mr. Petersen:** It is both. There are computer science and technical roles, and certifications and degrees.
    2. The private sector has in the past committed to hiring a specified number of people in order to fill shortages in certain job positions. Has this been considered?
        a. **Mr. Petersen:** We have not looked to make the private sector commit to hiring people in cybersecurity as the need is so great now. We have tried to encourage hiring by other means including promoting awareness that degrees in certain fields will greatly increase the probability of receiving a job offer.
        b. **Mr. Petersen:** We are trying to close the gap that has existed in academia that they have not always provided skills needed for students to be qualified to take jobs in particular fields when they graduate. The private sector in the past has laid out job descriptions.
        c. **Mr. Chabinsky:** Apprenticeships and two-year programs are done in the United Kingdom (UK) and facilitated by the government. It would be nice to know if that approach is working in the UK. More recently a similar program has been going on in VA. There are US-based companies doing in this.
        d. The Department of Labor (DOL) apprenticeship program has given out 165 million dollars so far in this effort. It is a good topic to pursue. Apprenticeship is a good method to develop skills and hire people. There are studies to evaluate return on investment to for apprenticeships.
        e. Is there anything on the law enforcement investigative side? There was work done in the sixties, and the criminal justice degree was developed as a result. It involved an investigative component.
        f. We need to understand what the workforce will look like in five to ten years. Things are now trending toward managed security service providers, and it may not even be managed

in the United States. There is a concern that we may be educating people for a field without a future demand for jobs.

   g. **Mr. Lin:** There are fundamentals of security that people need know about. There is an argument for a more holistic approach, for identifying the enduring principles. I've sent around a document that speaks to this.

3. If this commission is wildly successful, is the counter balance a reduction in the workforce? It is an interesting question. If a town has a lot of fires, is the answer to hire lots more firemen, or go after the arsonist. There is a big difference between having the right requirements to get a job, and getting offered a job.
4. Universities can identify what specialized areas they offer in security.
5. What will happen in the future, is something the commission can help with.
6. To what extent can we look at undergraduate and K-12, are there ways we can assist or predict people can come out with less student debt if they do something in cybersecurity? Scholarship for service programs are very interesting ways to increase incentive and decrease debt. People who come out with engineering degrees come out with higher repayment rates than liberal arts.
7. **Mr. Lee:** Some of these topics are reminiscent of the software engineering crisis that happened in mid 80s, and 90s. If we don't have a very specific focus, we may end up with a similar sort of crisis now. It ended up harming software engineering education for a time. Noting one of the statements from the paper, "many skills are experiential and not academic."
8. There are programs like Computer Science for all that are gaining traction. We may be in danger in suggesting or creating programs that will create a second class of IT workers.
9. **Mr. Gallagher:** I have very serious doubts on recommendations that push initiatives. I don't know any educational system that will swing 100 percent in four years. I'm not sure if we are focused on the right government role. How can we define the disconnects that exist in the market? We are looking at macro-economic problems.
10. **Mr. Petersen:** CompTIA produces a job market picture. We are trying to get to a more standardized approach.
11. In government hiring, are these new classification standards specific enough to track standards for this workforce. We are attempting to arrive at standards. If the government can't quantify its own workforce, how can it determine anything else? Employers typically add an experience requirement to the skills needed for a job. It seems to be a cover to say other skills are actually needed.
12. Other elements for follow up:
    a. **Mr. Lin:** Would like to know what programs, if any, exist for cybersecurity for managers. There are a lot of people making decisions about it, and there is a big gap. There has to be more than awareness, and second, the question on automation, is there any good work on it? Third, is there

information on the cyber security for the internet of things as opposed ordinary IT?

b. **Ms. Murren:** There is public awareness element. It can be in a number of sections. How will it appear in the report? Will it relate to individual topics in the report or be treated separately?
    i. The sense is, once we have the recommendations and the draft report in September, we may want to categorize these areas into other buckets that make more sense. One of our responsibilities is to identify topic areas that fit together more naturally.

c. **Mr. Alexander:** Is there a way of scrubbing recommendations?
    i. **Ms. Todt:** After each call, we will take stock of recommendations and discussions. In September, we will draft a larger report draft that will include the revised narrative and recommendations, and asking the Commissions to prioritize the top ten. In October we will arrive at consensus on those recommendations.

III. Discussion of the Identity Management Working Paper led by Donna Dodson

a. Identity management is always mentioned as a cyber security challenge. Having confidence in who an individual is, is a very big challenge. Identity management is thought of in the context of killing the password. As we look at the password capability, it was thought to be dead previously, except it is still the basic form of identity used today on the internet.

b. It is more than the credential itself, it reaches into multi-factor capabilities that may include a password or a biometric.

c. As we look at it strategically, it is more than using a credential, it is the proofing behind the credential. It extends through the lifecycle.

d. It includes device identity management, or sensor identification.

e. We look at it from a user and device perspective in the paper. There has not been as much work done in the device identity management area.

f. There are good individualized private sector initiatives, where users of a particular service can use more than password.

g. We do not see use of more than passwords in federated models. People now have a choice in what they want to use. There is not much choice in identity management space today. There are usability issues with passwords, and stronger forms of identity. The larger number of passwords we use almost causes sloppy use of passwords, because they are burdensome to deal with. It is an important challenge throughout cybersecurity.

h. Another challenge is identity proofing; associating credentials with individuals. There are challenges in the proofing and strengthening those capabilities.

i. There are different levels of trust required. How do we set it up and convey it so that people can make proper use of the capability?

j. What kinds of attributes are needed for the internet of things? How often do we need that information? How are identities managed, and whose responsibility is it to manage those identities? Is it the manufacturer or the owner of the device?

k. We need to think about the whole life cycle of a device. There are a number of challenges in that space.

l. In our recommendations, we tried to make them fairly detailed. It is really about creating an ecosystem that addresses users and owners of identities. We need to provide capabilities that are actually used on the consumer side, including organizations. It is not enough to provide a stronger credential, but the proofing must be stronger.

m. We must also think about privacy. We may not need names, but we need to protect the characteristics of an individual or entity. There needs to be reliability. NIST has been looking at identities in cyberspace, such as through the National Strategy for Trusted Identities in Cyberspace (NSTIC). We still do not have an identity ecosystem.

  i. **Mr. Palmisano:** You are asking the right questions. Has NIST looked at a digital identity clearing house?

    1. **Ms. Dodson:** There has been some consideration. The U.S. Postal Service (USPS) and the Social Security Administration (SSA) have given that the most thought. Their legal departments did not think they were set up to do it.

  ii. At a human level, is there a secure environment? People can make that choice about security. Is there some innovative way to develop this identity? Can there be a way to do this? Looking for an idea, not a recommendation.

  iii. **Mr. Alexander:** We need to do two things: We need to know people are who they say they are, and there needs to be an ecosystem that does the right things.

  iv. **Ms. Dodson:** One of the topics in the paper is having the different scale and higher level of assurance that originates with public service campaigns, that if you don't do certain things, you won't be safe on the net.

  v. There must be means to assert identity reliably, and protect it reliably. One of the things we learned in Berkeley, was the fact that when services changed the opt-in provisions, there is a very severe drop in the uptake of the service. Market forces may work against the use of multi-factor authentication.

    1. There is a situation here that is similar to the early days of the internet. There are lots of vendors in the world who seek to own identity. The government ended up playing a crucial role to get everyone to work together. Does the government need to play a similar role to get all these identity management systems to work well together? Otherwise companies will fiercely protect their own systems.

  vi. **Mr. Lee:** NIST is trying to create the ecosystem, and help people understand the business models. There are many on the technology side, who are playing, or are ready to play. From Microsoft's perspective, it is acquiring LinkedIn because it is inspired to have a greater role in protecting worker identities. It feels like the early pre-internet days. There is no concrete suggestion. Is it that fundamental, and should we think in those terms?

  vii. **Ms. Dodson:** We have looked at public-private partnerships here. The government getting involved causes concern in certain ways. The Fast Identity Online (FIDO) Alliance is trying to create some of that commonality where things can be shared. As to the government's role, we see the desire to accept identities from multiple organizations and have confidence at different levels. What different agencies need in order to have confidence in an identity may be different for each.

viii. Why has there not been a means for citizens to interact with the government using a single account?

1. There were initiatives ten or fifteen years ago, where banks would provide identity proofing. It could be used across government agencies. The private sector did not buy into that model. There was not a marketplace to provide the service.
2. **Ms. Dodson:** Different agencies collect different information. That complexity has not been sorted out even today. It is something we can think about, based on this conversation and others, and arrive at a proposed recommendation.

IV. Wrap up/Next Steps

a. **Ms. Todt:** Minutes will be sent out as soon as possible for feedback from the commissioners. The feedback will be used for incorporation into staff draft language.