Meeting Minutes

Attendees:

Commissioners: Pat Gallagher, Annie Anton, Steve Chabinsky, Keith Alexander, Joe Sullivan, Tom Donilon

Others: Kiersten Todt, Matt Scholl, Greg Shannon, Robin Drake, Amy Mahn

Agenda:

I. Opening
II. Research and Development Discussion Led by Matt Scholl and Greg Shannon
III. Questions and Discussion
IV. Next Steps/Wrap-up

Discussion

I. Opening

a. **Ms. Todt:** This call will be a hybrid with discussion of the draft and looking at the proposed recommendations.

II. Research and Development Discussion Led by Matt Scholl and Greg Shannon

a. Mr. Scholl is speaking on the R&D section of the latest draft delivered yesterday.
b. There is a proposed higher level recommendation talking about the need for a government-led effort and creation of a road map in R&D cybersecurity. We should not just look at protection and response, but also develop technologies for the future that are inherently secure, but are simple to recover if breached.
c. The goal is to build a more secure and longer term future.
d. We will talk about each proposed recommendation, with two open items. We hope for general thoughts and prioritization of the proposed recommendations and items.
e. We set the stage with how R&D is looked at today. The sector is growing. The numbers for the government are growing. The numbers from the market are not as clear. Much of the technology is reactive, not as much of the growth is future oriented.
f. There is discussion of the future, and the Office of Science and Technology Policy (OSTP) roadmap for inherently secure products. It includes grand challenges involving many entities. The results must enter the open source arena.
g. It talks about building a better infrastructure for R&D, for an arena and better science for implementation. The question, are we testing tools, or testing models is an issue.
h. We discuss overcoming challenges and technology transfer gaps with government leading and supporting industry.

III. Questions and Discussion

a. Is compliance technology convoluted with security technology? Something to consider
b. OSTP at the WH is looking at priorities in the next ten years, with a view to build partnerships and cooperation. Shifting defensible architectures for the future.
c. Incentivize in the roadmap through grand challenges.
d. **Mr. Donilon:** Would it be useful to have a definition of what a high-assurance defensible system would look like?
    i. It was touched on lightly in the draft, but can be defined more concretely. What things are in the conversation now that would aid in development of this type of system?
    ii. For proposed recommendation 2, do we have the ability to give examples of categories for challenges? It would also add concreteness.
    iii. **Mr. Sullivan:** It would be great to specify what we are talking about. In defining products as inherently secure, can we define what we mean by "products?"
    iv. **Ms. Anton:** Can we add "resilience" to the definition? It also applies to electrical engineering in terms of cyber-physical systems. It applies to the internet of things as well. Not sure where to go, when separating privacy, usability, and related issues. There is concern in separating them that we are not taking a holistic view. We can't continue to do research as technologists in isolation. It is separate from the roadmap, and the challenges.
    v. **Mr. Chabinsky:** How to integrate R&D into other areas as needed? In Europe, in the new data protection regulations, systems are required to be designed with privacy in mind. How to design privacy into products is an R&D issue, but it connects those pieces. Workforce, information sharing, R&D address a larger objective in other sections. It may cover some of the goals we want to address here.
    vi. **Mr. Gallagher:** The proposed recommendations are all various forms of implementing R&D. We have never clearly defined an objective. The big missing piece here is the agenda itself. We should address the motivation for the roadmap, such as a problem with gaps, insufficient scope, etc. We should define an objective first, then the recommendations should come. The roadmap is not an outcome. It's like recommending a recommendation. The section should state what the road map should lead to. A roadmap works when there are well-defined objectives. We can't tell from the definition of the problem, that the roadmap should be first. It would also address Ms. Anton's point. If the problem is well defined, the way becomes clear. It is broader than simply the technology.
    vii. **Mr. Donilon:** There should be some upfront formulation with declarative text on the goal of a research agenda. State the agenda first, followed by proposed recommendations, followed by the roadmap. Include some specific examples of promising areas of research. Lay out what success looks like when they are achieved.

viii. **Mr. Shannon:** We have worked with DOE and NSA. One idea is the notion of unassailable systems. It involves the difficulty to crack these systems. It ensures policies are enforced. Involves formal methods, or proving computational challenges exist to compromising systems. I will provide text **to describe these systems.**

ix. **Mr. Gallagher:** Usually R&D agendas go for a particular question. What could be different about the R&D agenda here, is laying out goal for attributes of the system itself. If we can define high-assurance characteristics of a system, it opens the door for a different R&D agenda than what we have had before. What mix of fields need to be part of the agenda to get to that behavior? What research infrastructure must exist to achieve the goal? Can we define it in an exciting and compelling way for system performance to be the overriding goal, then invite the research community to build it out?

x. **Mr. Donilon:** A report on preparing for the future of artificial intelligence (AI) out last week. Can we cross reference materials in the AI report (offensive and defensive capabilities), and can we talk more about it?

    1. **Mr. Shannon:** The report talked about qualities and what is needed for systems to be secure. AI is important, but we didn't want it presented as the answer to today's cybersecurity challenges. If presented with the desired attributes for the system, it may be used in that context. Putting the AI out of business is the ultimate goal, but we're not there.

e. Other comments –

i. **Mr. Gallagher:** The discussion is a key part of it. Trying to create wellness around IT infrastructure is hard. There needs to be a functioning immune system, and AI can play a key role. It will be important going forward for the nearer term.

    1. **Mr. Scholl:** It is one of the examples where market based R&D is actively working. We need to make it clearer on the definitions, and call out challenges for the agenda, and the rest will follow.
    2. **Mr. Donilon:** The capability needed for the journey.
    3. **Mr. Shannon:** AI will augment human systems. Finding pathways into systems. Utility across the whole spectrum.

ii. **Mr. Scholl:** We propose recommendations about transition to practice and technology transfer, and building infrastructure for R&D.

    1. We propose a recommendation that talks about facilitating technology transfer.
    2. We propose recommendations that talk about building infrastructure. The earlier discussion was very helpful.

iii. **Mr. Chabinsky:** Moonshot – We have an opportunity in the discussion tomorrow, on how to position. Start with the moonshot and underlay with objectives and metrics, etc. Will discuss further tomorrow.

iv. Mr. Scholl will consider and restructure the section based on today's comments.

v. What is a good timeframe for achieving the goal (unassailable systems)? It is an infrastructure migration, with possibly a 15-year timeframe. It could be measured in 5-year pieces. It is doable, and has been done elsewhere.

vi. **Mr. Shannon:** Demos would be possible in five years, with further evolution following. The hard part is making it pervasive.

vii. **Mr. Scholl:** With migrating cryptography is not uncommon to see this migration in fifteen years.

viii. **Mr. Donilon:** How will the research community react?

   1. The commission needs to consider how to incentivize the action.
   2. **Mr. Scholl:** Overall, it will be welcomed. There has been some research already. It becomes what the government is willing to invest.
   3. The research community is primed for this research, and creating trust for society.

ix. **Mr. Donilon:** Should we cite a dollar amount for investment, and a timeframe?

   1. **Mr. Shannon:** We have talked about it, but have no real basis for a response. Unclassified research spend is about seven hundred million dollars a year.
   2. Staff will research further.

x. **Ms. Anton:** The National Roadmap for Robotics for 2013 may be an example. They were able to get money from multiple agencies for an initiative that led to the roadmap.

xi. **Mr. Shannon:** There has not been any appreciations in the new budget for what we are considering. Should there be cost estimates?

   1. **Mr. Donilon:** If Tony Scott could provide a number for a six to ten year plan for addressing legacy systems and progress with R&D toward a goal. The numbers are not that large, that we should not suggest some numbers.
   2. **Mr. Shannon:** People may be surprised that a small amount could have such a large impact.
   3. **Mr. Donilon:** Evaluating may better inform the scale.
   4. **Ms. Todt:** We may be able to discuss more tomorrow as well.

xii. **Mr. Gallagher:** What is annual the cyber budget at NIST?

   1. **Mr. Shannon:** It is an order of magnitude less than numbers mentioned here. DARPA has absorbed much of R&D investment in this area. The National Science Foundation (NSF) is around 150 million a year (for security and the trustworthy computing effort) as a comparison, an F-35b fighter costs 105 million.

xiii. **Mr. Gallagher:** Think about whether the translation problem is different here than other R&D areas. Is there a systematic mismatch with the private sector, or translating R&D into product lines?

1. There are more and different challenges in technology transfer. Some mention should be made so that it is paid attention to is important.

IV. Next Steps/Wrap-up

a. **Mr. Donilon:** Everyone should come prepared for the working group meeting tomorrow with ideas, and ready to continue consideration and review of updated materials.