INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Modernization Act of 2014]

MEETING MINUTES

June 28, 29 and 30, 2017

American University, Constitution Hall
4400 Massachusetts Avenue, NW
Washington, DC 20016

Board Members	**Board Secretariat and NIST Staff**
Chris Boyer, AT&T, Chair, ISPAB John Centafont, NSA Laura Delaney, DHS Greg Garcia, Signal Group Patricia Hatter, Intel Toby Levin, Retired Jeffery Greene, Esq., Symantec Corporation Gail Stone, Social Security Administration **Remote Participation** Josh Franklin, Presenter **Absent with Regrets**	Matt Scholl, NIST, DFO Robin Drake, Exeter Government Services, LLC Warren Salisbury, Exeter Government Services, LLC

Wednesday, June 28, 2017

The meeting opened at 9:07 a.m., Eastern Time.

Welcome and Remarks (from the Chair)

Chris Boyer, Chair, ISPAB; Assistant Vice President, Global Public Policy, AT&T

Mr. Boyer opened the meeting and asked the Board members to briefly describe what they're working on and convey any concerns or items for the Board to discuss. He noted the meeting is very timely in regards to walking through components of the recent executive order signed by the Administration.

Many on the private sector side are spending a lot of time dealing with implementations of the executive order. Mr. Boyer is leading a botnet study on "internet and communications technology resilience" with the National Security Telecommunications Advisory Committee (NSTAC). The study is due October 31, 2017. Approximately thirty speakers are due to brief the subcommittee.

The National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA) efforts are ongoing. The NIST workshop is on July 11 - 12. NTIA has a request for comments in process with comments due by the end of July. There are other aspects of the executive order that the Board will be discussing.

The Board will hear about the different components of the cybersecurity executive order in the course of the meeting. The Board was asked to think about particular areas to weigh in on,

including the section on Federal IT in the executive order. The Board has written several letters in the past on things like federal IT modernization.

The Chair tasked the Board to think about topic areas that it believes are particularly relevant and draft feedback on these items to include in another letter to send out at the end of the meeting. Identifying key issues and then offering advice is what the Board is intended to do.

Ms. Levin noted the June, 2017 meeting is her last as a Board member. Mr. Garcia noted one of the more interesting movements is the legislation for cyber grants to the states, and giving DHS that authority. It's a question of where the money is coming from. Some of the more recent attacks on state governments and voting systems have put a punctuation mark on the level of state-cybersecurity expenditures relative to other homeland security and public safety programs.

Welcome and Remarks

Dr. Charles Romine, Director of Information Technology Lab ITL), NIST

The Chair welcomed Dr. Charles Romine, Director of the Information Technology Lab, NIST to the meeting to update the Board on ITL activities. In his update, Dr. Romine presented several key areas, including:

- Actions that have been taken by the Administration since the last time the Board met.
- Highlights of some Congressional actions that affect NIST and may serve to indicate of the kinds of authorities that NIST may exercise in the future, and possible implications.
- An update on some of Dr. Romine's interactions at the Congressional level, and revisit the discussion about ITL's purpose.
- The budget submission to NIST, and discussion of possible future priorities.

Dr. Romine discussed the release of Executive Order 13800, Strengthening the Cybersecurity in Federal Networks and Critical Infrastructure, and the fiscal year (FY)-2018 budget request. There are three main components of the executive order that affect NIST directly. NIST has involvement in areas relating to cybersecurity of federal networks, cybersecurity of critical infrastructure, and cybersecurity for the nation as a whole with a specific emphasis on the area of workforce development.

The President is requiring federal agencies use the NIST cybersecurity framework (CSF) to manage their cybersecurity risk. Secretaries now have a clearer directive from the President that they are the ultimate responsible party for agency cybersecurity, which clarifies accountability for cybersecurity.

NIST now provides an entire suite of risk management documents for federal agencies. The cybersecurity executive order was released on May 11 2017. On May 12, NIST issued draft NIST RIA-170, guidance on how federal agencies can effectively use the cybersecurity framework.

There is also a call for IT modernization and trade, led by the Director of the American Technology Council, a new council set up by the White House. NIST's role is providing input on technical feasibility for modernization and network consolidation for shared services.

Under the heading of cybersecurity critical infrastructure, the main theme is to be more resilient against automated distributed threats, or botnets. The goal is for the Administration to lead a process to reduce threats and promote action by safe course. NIST is part of the lead with NTIA. A preliminary report is due for public comment within nine months. The preliminary report is on schedule. The final report is due one year later, or May 11, 2018.

The last component of the executive order under the heading cybersecurity for the nation involves

workforce development. This is something NIST has been doing for a long time as an interagency lead for activity under the National Initiative for Cybersecurity Education (NICE). The new requirement is to assess the scope and sufficiency of what NIST and others are already doing and provide a report to the President on how to support workforce sustainment.

Since the Board's last meeting, the President's 2018 budget request was submitted. Every year, NIST, as part of the Department of Commerce, has to plan to that budget request. This year, the budget request is a strong reflection of the administrations stated priority to rebuild the military, to make critical investments in the nation's security with a strong emphasis on physical security, and to keep the nation on a responsible physical path.

The lab was given a topline budget number to manage to. The labs were asked to seek activities near the end of their lifecycle, that were less than critical, and/or that were not in the direct core mission of NIST or the inherited mission of the laboratory. The direction received was to propose what should be at least as strong or stronger in the areas that represent the core of NIST's program.

There are four recent actions by Congress that that are relevant to NIST and the Board. Three of them involve introduced legislation. The fourth is a hearing that was held recently. HR-1224, the NIST Cybersecurity Framework Assessment and Auditing Act of 2017 was introduced. The second is HR-2481, Protecting Our Ability to Counter-Hacking, or, the PATCH Act of 2017. On the Senate side, SN-770, the Main Street Cybersecurity Act of 2017 was introduced. Finally, two subcommittees acting jointly under the House Committee on Science, Space and Technology, held a hearing on the implications of the WannaCry ransomware. Dr. Romine appeared before that panel and talked about what NIST has learned and some of the things that NIST is doing to try to prevent those kinds of issues in the future.

HR-1224 seems to provide a new role for NIST. It not only provides guidance for agencies to incorporate the framework into risk management activities, but puts NIST as the chair of a federal working group for developing metrics and tools to understand the effectiveness of the cybersecurity framework. NIST would then use those tools to audit the effectiveness of agency activities in securing their information and information assets. This role gives NIST a completely new auditing capability for auditing responsibility.

The auditing capability in the government rests principally on the Government Accountability Office (GAO) and the Inspectors General (IGs). The bill may be a reaction to a Congressional assessment that the current DHS auditing function is not muscular enough to actually galvanize change in the agencies. NIST is engaged in conversations with Congressional staff on the intent of the bill, and how and whether to assign NIST a role at this time. In the past, the enforcement role fell to the Office of Management and Budget (OMB) in examining Federal Information Security Management Act (FISMA) compliance.

There is no additional funding for NIST to undertake an auditing role, but the bill did ask the Congressional Budget Office (CBO) to assess how much it would take for NIST to acquire a capacity to audit agencies on cybersecurity. The CBO determined it would take 48 million dollars over four years to build and execute the audit capacity.

The Chair noted the Board may consider and weigh in on NIST's role in auditing agency compliance with the framework. There's a fundamental issue that comes in play involving whether acting in an auditing role changes the nature of what NIST does. There's merit in having the audit and enforcement functions separated out. It seems likely NIST's perception will be changed as a result of adding this function. It's an appropriate issue for the Board to consider in its advisory function.

The Department of Commerce would serve as a board member on the PATCH Act (HR-2481), and

coordinate with DHS on the process for DHS to share or release information. This relationship has implications for NIST because its goal lies in ensuring that the infrastructure is as secure as possible. This bill is an attempt to set infrastructure security into legislation so that it's traceable to statute, and governs the process so that authorities or processes cannot be changed without permission of Congress.

The Main Street Act complements some of the things that NIST is already doing in the sense that it specifically asks NIST to do more to help small business understand and work on cybersecurity risk. There is a guide nearly ready to come out for small financial services providers.

Dr. Romine's testimony regarding the WannaCry attack touched on four major things: the cybersecurity framework, the relatively recent guide for cybersecurity event recovery which is SP 184, and the National Software Reference Library (NSRL), and its role in not just law enforcement, but also as support for cybersecurity.

NIST's and ITL's purpose for the statements to the Board is cultivating trust in information technology, and in metrology. The challenge lies in maintaining a balance between fundamental research, applied research and standards to developmental technology transfer.

There are a number of things ITL wants to strengthen over the next couple of years: cybersecurity, along with privacy research and development, and privacy guidance. It permeates many other things, such as the Internet of Things, reliable computing, computing technologies and applications, and a relatively new area, artificial intelligence (AI).

Artificial intelligence is an interesting area because evaluation of AI is a difficult problem. When artificial intelligence exceeds the capacity of human understanding, then how can evaluations be done to understand how the AI operates, or determine the AI has not been tampered with, or the AI is unbiased? The lab is also thinking about data science, and how to support the mission of NIST as a whole. It involves open repositories and providing support for data analytics, understanding the data analytics and doing evaluations and testing of these things.

Software metrology is the great unsolved problem in software. How can software be measured? NIST will have to ultimately tackle this question. There are ideas now, measuring science through statistics and mathematical modeling. It's something that's been worked on for a number of years.

Dr. Romine posed some questions to the Board. What should the lab consider in the area of AI for cybersecurity and privacy? What should the lab consider in the area of future computing technologies when it comes to cybersecurity and privacy? What's missing? What's not missing, but maybe needs a broader dialogue with the experts to help sharpen the focus or clarify the opportunities available.

Executive Order NIST Plans for Standards and Guidance Alignment and Use of Cybersecurity Framework

Dr. Ron Ross, NIST

The Chair welcomed Dr. Ron Ross of NIST to the meeting to update the Board on the executive order and NIST plans for standards and guidance alignment and the use of the cybersecurity framework.

There have been several working groups that NIST has been a part of over the last two months. Two of the groups looked at the Authorization to Operate (ATO) process. The object is to use the risk management framework as the basis for the ATO. The groups are concerned with such questions as, how's it working? How can it be more efficient? How can it be faster? The groups have gone through the entire process and looked at everything, seeking to make it more efficient.

Over the next couple of months, OMB is using the findings to modify several key publications. Dr. Ross briefed the Board previously on NIST publication 800-53, Rev 5, which is in review with OMB. It's one of the three key publications to be modified within the next two to three months. The following documents will become the focal point for making sure that NIST can integrate the cybersecurity framework, and manage risk. Specifically, the documents are the 800-39, the enterprise-wide risk management guideline; the 800- 37, the risk management framework; and the 800-53, security and privacy control catalogue.

The 800-53 has been under a very intense review at the Office of Information and Regulatory Affairs (OIRA). The review is necessary because this is the first time the privacy branch has really had an opportunity to see the document in detail. For the first time, there are joint controls where one control can cover different aspects of security and privacy at the same time. Last Friday, OMB distributed the 800-53, Rev. 5 to all federal agencies for a review on the agency side

The second major document that will be greatly impacted is the risk management framework, publication 800-37. This document has been out since 2006. Privacy is every bit as important as security now as computer capabilities are increasing in everything. The challenge with the 800-37 is the cybersecurity framework and the risk management framework share the word “framework.” The challenge is determining what each framework does well and what things they don't do well. When looking at commonalities, there are opportunities to integrate these concepts. It prompted us to do the NISTIR 8170, which was published a couple of months ago. It’s out for public review with two more days in the comment period.

The idea with the baseline concept was tied to defining low, moderate, and high levels of control was to do a triage. Every organization can examine and categorize the information in their systems by the triage rating; low, moderate or high. In order to meet the general requirements in FIPS 200, they designed a really robust and large catalogue of security and privacy controls.

The total number of all controls is about 826. The low, moderate and high groups range from 150 controls to approximately 250 to 275. There is a hierarchical increase in controls as the level increases. When selecting controls, it represents the level of commitment to what security protections are necessary for that system and the mission being supported. The decision over selecting controls lies within the agencies. A system includes the people, the processes, the technologies, and that’s missed sometimes. A lot of people think security is a technical issue. However, many of the very bad breaches start with people failure.

In risk management, there may be circumstances where an agency or organization is required by their mission to accept a risk. There are means for deciding what methods will best compensate for the risk. An organization must determine what other controls are needed to manage that risk.

The task is to figure out how to bring these worlds together. The immediate task on modifying the framework is to figure out how agencies can actually execute and use the cybersecurity framework as the overarching piece and yet have that risk management process embedded so they can actually decide what controls they need. That’s where the cybersecurity framework does require a risk management process. The goal is to use the Risk Management Framework (RMF) as the actual control selection process, but it’s going to be informed by many things that the cybersecurity framework brings forth.

NIST identified a new step for the RMF. A "Step zero" was added to the beginning rather than change the existing sequence of steps. There are six steps: categorization, control selection, implementation, assessment authorization, risk acceptance, and continuous monitoring. Organizations can use the RMF and bring the ISO controls in. There are all kinds of combinations of

tools that can be used with the RMF.

Step zero is called the organizational preparation step. If any organization wants to tailor controls, they're often risk-averse to tailoring because there's an inspector General (IG) and a bunch of auditors overseeing the process. Organizations need to feel like it's possible to tailor and actually not get beat up for it. Another problem lies in the guidance. It says, "Select a set of security controls that can satisfy a set of security requirements." The source of the requirements is never stated. Where do those requirements come from? They can come from laws such as FISMA, Health Insurance Portability and Accountability Act (HIPAA), and Gramm-Leach. They can come from OMB policy. They can come from executive orders, or from mission statements. Controls should be traceable back to the requirements. The first step is to develop a set of requirements. Requirements can drive a security and privacy control selection process in the case of an enterprise, or they can build a component or system.

The 800-39 deals with enterprise-wide risk management. It is the document that looks at an enterprise from the perspective of the three areas described here: organization governance level, mission business process layer, and the systems intended to actually execute those mission business processes.

Step zero is intended to raise awareness of risks and managing risks through the whole organization. There are nine tasks now in the organizational preparation process including a risk management survey, figuring out risk tolerance, examining organizational assets, determining where the high-value assets are, do enterprise architecture, develop a set of security requirements, talking to stakeholders to identify their requirements and their protection needs so that security requirements can be created that meet those requirements. All of that package is organizational prep.

A lot of time was spent on security controls and frameworks, but the real issue today is identifying all high-value assets. DHS has been working with the agencies to identify a couple thousand high-value assets. Identification and protection becomes an architectural problem. There are so many systems, and so many different components, and so many applications that the government is drowning in complexity.

It's all about transparency, traceability, and trust. Traceability and transparency won't exist in an architecture that is so complex that no one understands what's there. Security is now tightly coupled to modernization. As the Administration pushes out more modern systems, there will be a big push to go to more shared service systems, and pushing more out to the cloud. Using shared services in the cloud is more of an exception rather than the rule today. The concern has been raised that by consolidating many things in one place, the attack risk seems to increase because it's no longer distributed as in the past.

800-53, Rev 5 will add a new enhancement, a second-level categorization. Seventy percent of federal systems are at the moderate level. In that context, when agencies are asked to move to cloud or shared services, they will probably be risk-averse. In a shared situation where a lot of data originated with different rulesets, data should not be used for a different purpose than it was intended. That architectural piece can be very challenging at the detail level. That's why the privacy team's project was so important.

One of the controls that is now a joint control is called "security attributes." In an access control decision, everything gets adjudicated within a system through access control mechanisms based on the attributes of the data and the user that wants access.

Step zero is a great opportunity to unify the disparate processes that are already on board,

including: lifecycle, engineering, acquisition, and Federal Information Technology Acquisition Reform Act (FITARA) processes. All these processes really start with the enterprise governance level and an understanding of all processes involved with a product in the system.

With Step zero, the working groups hope to strengthen the argument for joint authorization. With approval from OMB, it could change the way agencies look at this problem. Change will not be easy. The Chief Security Officer (CSO) and Chief Information Officer (CIO) role mindset is entrenched today. The system and the process should drive the right information to the right people to make better decisions.

One of the problems with the ATO process is that it's applied uniformly and rigorously across all systems. FIPS 199 was intended to stop that with the triage, but the triage has never been implemented. The ATO process for low, moderate, and high systems are pretty much the same. Allocating resources should be done according to the threat space, and what their adversaries are doing.

The Federal Risk and Authorization Management Program (FedRAMP) is an instance of pre-tailoring. NIST is building overlays with DHS on high value assets (HVAs), for the HVA project. A moderate baseline will be developed initially and additional controls added that are necessary to get to the level of protection needed for HVAs. The government needs to get away from the return on investment question for high-value assets. That's what Step zero is all about. It gives greater visibility, transparency, traceability, and the ability to do different things where it's appropriate.

Executive Order Agency Risk Reporting

Derek Larson, Office of Management and Budget

The Chair welcomed Mr. Derek Larson, OMB to the meeting to update the Board on executive order agency risk reporting. He discussed Memorandum M-17-25 (M-17-25) as it relates to the executive order. It is the only guidance to agencies on implementing the President's executive order. It specifically talks about the risk management assessments being carried out under the executive order. The M-17-25 has set several key deliverables.

The first deliverable came on May 26th, where agencies were to submit the names of senior accountable officials to OMB who will be the primary people in charge of implementing the executive order within the agencies. The next is due July 14th, when agencies will submit responses to the FY-17 FISMA metrics as part of the quarter three reporting process. Large agencies already report on FISMA metrics quarterly. However, small agencies are now also required to report under M-17-25.

The input is designed to provide greater context to agency responses regarding the risks they see themselves as having, their strategies for mitigating those risks, the current capability and resource gaps they're facing, and the involvement of senior leadership in the strategies. OMB and DHS will analyze the information and return risk management assessments to the agencies by the end of July.

Agencies have until August 9th to return responses to OMB on the risk management assessment signed by the senior accountable official. These letters will state how agencies are planning to transfer, mitigate, and decrease the risk that was identified in the risk management assessments.

These assessments will then go on to inform OMB's report to the President and provide recommendations on how to improve federal cybersecurity. The information will be used as an aggregate and will inform the technology requirements that agencies have identified to help mitigate risks. Additionally, the M-17-25 asks the agencies to submit a plan for implementing the

NIST Cybersecurity Framework.

The M-17-25 set out key markers in terms of what agencies should be reporting and how they're implementing the plan including: how they're budgeting against it using the current capital planning process, how they are aligning their capabilities to the FISMA metrics and therefore, to the cybersecurity framework, and timelines for completing that implantation.

Risk assessments had to be done within ninety days from when the Executive Order was issued. In 60 days from August 9th, report recommendations must be turned around to the President. Agencies are also required to submit proposals describing how they will implement the framework. The action plans is due on July 14th, the same day as the FISMA responses. The agencies do not have to implement by July 14th, only submit a plan. Many agencies are already moving in this direction. The plan will show how they will keep the process going forward. There is not an implementation deadline at this time.

Existing oversight processes will track progress on the implementation plans. The EO is to be the first set of benchmarks and then it will be incorporated into the regular OMB process. The report will be submitted in early October. On October 31, the quarter four data comes out and we'll start working on the annual FISMA report.

In terms of the risk management assessments, the FISMA CIO metrics and the FY-16 FISMA IG metrics will demonstrate what capabilities the agencies are putting in place to mitigate and limit risks. The degree to which that becomes public versus part of the classified appendix is still being discussed, but it will be part of what Mr. Larsen presents to give a more complete picture of the risks that agencies are facing.

Agencies are providing questions regarding budget and resource needs as part of responses to one of the narrative questions that are required by M-17-25. It will be a part of the quarter 3 data call. The budget questions are being addressed in the report of recommendations to the President, which is being driven by OMB. Some requirements will eventually be undertaken in other efforts under the government reorganization effort. Some of these activities are going to be longer term.

It is true that budgets for new technology and upgrading databases and all of the legacy systems have been in a short supply in the federal government for decades. Agencies are expected to return input regarding specific gaps they are facing and specific capabilities they're going to need help with. That information will be incorporated into the report of recommendations to the President.

Tight security does have a much bigger play in terms of human capital. It's been an issue raised since cybersecurity's Certified Information Privacy Professional (CIPP) and the Cybersecurity National Action Plan (CNAP). It's a continuing problem, but solutions are being discussed.

Update on NIST Privacy Engineering Program

Naomi Lefkovitz, NIST

Ellen Nadeau, NIST

The Chair welcomed Ms. Naomi Lefkovitz and Ms. Ellen Nadeau of NIST to the meeting to update the Board on the NIST privacy engineering program. Ms. Levkovitz and Ms. Nadeau discussed the work they've done with NIST's privacy engineering program. The program is part of the Applied Cybersecurity Division, and has existed for three years. The lab works with trustworthy systems, and attributes like privacy, security, safety, reliability, are an important part of developing trustworthy systems. There is a host of guidance for engineers to build security into systems, but no similar guidance or tools exist for building in privacy. It is what the privacy engineering program has been working on.

Research collected for NTIA in 2015 states 40 percent of households reported that privacy or security concerns stopped them from doing things like conducting financial transactions or buying goods and services online. One of the primary drivers of the lab's work was the update to Circular A-130 in July, 2016. This update requires federal agencies to move beyond the compliance approach to a more risk-based approach and apply the risk-management framework to their privacy programs. Privacy needs a body of guidance for repeatable and measurable approaches similar to other attributes of trustworthiness.

The Privacy Act of 1974 talks more about a code for fair information practice, meaning more of a requirements-based approach. The question is: how to take this foundational difference and reconcile it with the changes in Circular A-130 that now require agencies to move to a more risk-centric approach. It leads to a document released in January, 2017, the final version of NIST Internal Report (IR) 8062 that introduces concepts for privacy engineering and risk management for federal systems. It is only an introduction at this stage. Workshops continue on these concepts.

NIST SP 800-30 introduces risk models. Risk models define the risk factors that are assessed and the relationships between them. A parallel model was needed that was more specific to privacy inputs. Consequences of adverse privacy events took a lot of discussion to determine the adverse event in terms of privacy. The adverse event is a privacy problem for an individual.

Ms. Levkovitz and Ms. Nadeau introduced a set of privacy engineering objects to bridge the gap between privacy principles like the Fair Information Practice and implementation in a system. The privacy engineering objects express the characteristics or properties of the system and allow users to map capabilities to the system and support control mapping.

The risk objects are being integrated with the risk-management framework. The risk assessment all goes into the privacy impact assessment (PIA) and the controls that were selected to address risk and the requirements. The PIA tells that public story of how all those pieces came together. Ms. Levkovitz and Ms. Nadeau developed a privacy risk assessment methodology that applies the privacy risk model.

The National Strategy for Trusted Identities in Cyberspace transformed into the Trusted Identities Group (TIG). Pilots have been going on with grant awards for a number of years. The pilots are required to demonstrate alliance with the guided principles. There were conversations for months trying to arrive at an agreement on the significant privacy risks.

There were not any tools out there for the pilot programs to demonstrate how they aligned. Ms. Levkovitz and Ms. Nadeau came up with a set of worksheets. They're interested in understanding where privacy risk may exist, so that an optimal solution can be found where function and benefits are preserved while mitigating possible adverse consequences of privacy.

It begins to establish a collaboration between business owners and the privacy engineering team or privacy policy team. There seems to be a sense of antagonism between the privacy team and the rest of the group. By doing this engineering process, the collaboration between teams starts immediately.

The first task is to really understand the system. In cybersecurity framework terms, it is the “identify” function. From the privacy perspective, one of the assets might be personally identifiable information (PII). There's a need to understand what sensitive information exists and where it is. It’s hard to manage information and privacy risk if no one knows where the information is.

Simplification became part of this collaboration effort. Having everybody understand the system provides benefits. When people start to understand the object is to look for problems that

individuals could experience, the engineers can start to become collaborative partners and bring their expertise.

Applying context is really where privacy experts need to come in. When somebody who's really steeped in security but not in privacy issues, they don't really understand the context from a privacy perspective. What they really start adding is data security issues.

There's a variety of factors and the goal is to begin to coalesce them into "summary issues" that can then be further analyzed by privacy experts from a problematic data action standpoint being able to formulate useful analyses is critical.

Assessing privacy risk is the heart of the model. A semi-quantitative analytic approach is used with the goal of prioritizing privacy risks, or a bracket rating from zero to ten. Assessing impact is a lot trickier. People experience privacy problems directly, as opposed to organizations.

Security is ahead of privacy when assessing threats. Privacy risk assessment to date, has been at the level of saying this is an important value. By beginning to illustrate it in a way that people can actually communicate with leadership about some of these problematic data actions, it is possible to act on it and try to address that particular privacy risk.

Privacy risk assessment should occur in system design. Controls can be selected, which could include data access agreements. The result is the ability to make informed risk decisions. The tool doesn't determine any particular outcome. The main point is that it's informed by this reasoning process and it's traceable and adjustable.

In NIST IR 8062, there is a high-level guidance road map and the main documents. There have been a number of workshops on privacy risk management and assessments. Agencies and organizations often request integrated guidance. Integrated privacy guidance came out just last week. It represents a new way of looking at guidance, with completely integrated privacy requirements in with the base functional identity requirements. There is a privacy consideration section along with the security considerations, which gives additional informative guidance. The core requirements were all built in at the appropriate sections.

Ms. Levkovitz and Ms. Nadeau sought input from the Board a about the possibility of developing a privacy engineering toolkit. Anything that can synthesize what is being done, saves companies time and confusion. If there's a resource gap on the security side, there's a much larger resource gap on the privacy side. There will be a need for more people who can do these kind of privacy assessments.

The Chair noted there have always been differences of opinion on privacy. The Board may consider writing a follow-on letter about growth in privacy and the growing need. There are some strategies on how to take a privacy engineering toolkit and work with some universities to incorporate privacy tools into the curriculum. The Board can think about what the government could do in furthering privacy education in system development and have some discussion about that.

NIST Block Chain Research Project

Dylan Yaga, NIST

Andrew Regenscheid, NIST

The Chair welcomed Dylan Yaga and Andrew Regenscheid of NIST to the meeting to update the Board on the NIST Block Chain Research Project. Mr. Regenscheid is with the Cryptographic Technology Group at NIST. Their primary goal is to promote adoption of strong cryptography through research and development of standards, guidelines, tools, and metrics. A blockchain is a

distributed ledger for a particular type of transaction characterized by being decentralized, peer-to-peer, tamper evident/resistant, and synchronized through consensus by the chain members. It can facilitate transactions between entities that do not trust each other without a trusted arbiter. The building block for blockchains is the hash chain.

The blockchain adds a set of rules about what can be included in the chain, and who can propose adding blocks. There are two types of chains: permission-less (public block chains usually tied to a crypto currency), and permissioned blockchains. Permissioned blockchains can be private or controlled. The participants in permissioned blockchains are trusted. Permissioned blockchains are more efficient, and support greater privacy and confidentiality through a governing authority.

Blockchains have many interesting use cases including financial services, data/asset registries, provenance/supply chains, identity management, voting, and others. Work is being done on applying blockchain technology to supply chains. There are pilots working with supply chains. Blockchains can also be used in identity management.

Certificate transparency is a related technology that uses many of the same core concepts as blockchain. The challenge with certificate transparency is scalability. Are there other ways to validate trust on the internet? It is something to be considered. What might blockchain technology mean for business processes? New procedures and policies will be needed.

Areas for further research include security, privacy, scalability, consensus algorithms, and quantum resistance. Active standardization efforts include work in international standards by the International Organization for Standardization (ISO) and the Institute of Electrical and Electronics Engineers (IEEE). National standards work includes the Accredited Standards Committee (ASC) X9 and industry consortia with Hyperledger and the World Wide Web Consortium (W3C). Current and future work items include terminology and taxonomy, use cases, blockchain interoperability, and primitives and building blocks. Potential work areas include ring signatures, threshold signatures, bit commitment signatures, zero knowledge proof signatures, multi-party computation and quantum resistant algorithms.

NIST has established an internal test bed to explore blockchain technologies and use cases. It is also participating in standards activities. NIST co-hosted the "Blockchain and Healthcare Workshop" with the Department of Health and Human Services (HHS) in 2016. The project is now are seeing new types of crypto-primitives, including privacy supporting primitives. Blockchain may be a larger scale use of many new technologies.

Mr. Yaga has worked on the internal NIST blockchain workbench. There is a great deal of interest in blockchain within NIST. The group is dealing with uncertainties in understanding how to proceed with real world blockchains and dealing with purchasing cryptocurrencies for experimentation. It is still under development. Initial blockchains being used are MultiChain, Eternum, and Hyperledger. Each offers different characteristics for use in the internal workbench. Mr. Yaga offered a demonstration of each and some workbench deliverables.

Mr. Yaga and Mr. Regenscheid will be delivering the workbench to NIST. Challenges include a questionable perception of blockchain technology, as bitcoin has been used for illegal activities. There is a lack of interoperability and limited transaction sizes. Blockchains consist of multiple technologies combined together. There are additional challenges such as different consensus mechanisms. There are very few workbenches at this time. The Massachusetts Institute of Technology (MIT) founded the "Be Safe" network. It went public before hearing about NIST's work. The group started in the second quarter of 2016. The report was delivered earlier this year.

There are five types of threats to mobile devices. The Cellular Telecommunications Industry

Association (CTIA) and others raised issues with information not being included in the report as it was submitted. There was a variety of responses from industry on the report. There were 26 responses to the request for information (RFI). DHS conducted one-on-one interviews for some responses. The group also had to settle on a definition of "mobile".

The group sought to identify best practices and standards. The government is very oriented to best practices. There are also legal authority gaps. DHS has no legal authority to require mobile carriers to assess risks relating to the authority of mobile network operators.

DHS Mobility Report

Josh Franklin, NIST (via phone)

The Chair welcomed Josh Franklin of NIST to the meeting to update the Board on the DHS Mobility Report. Mr. Franklin works on electronic voting, telecommunications, mobile security, and public safety at NIST. He is the technical lead for the DHS mobile device security study to Congress.

Mr. Franklin worked on a DHS effort that NIST provided technical assistance for. Mr. Vincent Sritapan of DHS led the effort, which included working with government and industry partners. Mr. Sritapan is on active duty with the Navy, and Mr. Franklin is presenting for him. Mr. Franklin expressed regret to the Board that they were unable to present in person.

The Cybersecurity Act of 2015 mandated a study be conducted on the threats relating to federal mobile devices. DHS was to lead this study in consultation with NIST. DHS and NIST decided to convene a multiagency working group. The working group included the already existing multiagency working group called the Mobile Tiger Team.

DoD handled creating a classified annex to the study. The Cybersecurity Act mandated this report was to have conclusions in the following areas: recommendations for industry standards, efficiencies in DHS authority to address existing mobile security issues, a plan for rapidly adopting mobile technology within DHS, and looking at general techniques for moving from a desktop-centric approach to being primarily mobile-focused.

The multiagency group began convening during the second quarter of 2016, and meeting in earnest during the third quarter. DHS and NIST had one-on-one meetings with industry, while NIST released the Mobile Threat Catalogue in consultation with DHS. The Mobile Threat Catalogue provided the threat model that was primarily used within this study.

Quarter four saw release of the RFI to obtain mobile threat and defense information from industry. Responses were due forty-five days later. The working group organized and analyzed those responses. The report was drafted in the next month. The report was released early this year.

The RFI from the General Services Administration (GSA) closed August 22nd. Two industry dates were held to explain the type of information that DHS was looking for. A number of example clips were identified in these category areas: applications, operating systems (OS), firmware and hardware-based threats, physical device threats, network-based threats, and threat to mobile.

The multi-agency group asked for more information on threat areas and asked for standards and best practices for enabling mobility in the enterprise. There was a large focus on finding worthwhile standards. The information can be used throughout the federal government.

The Chair noted a concern that not all of the industry input submitted into the RFI process ended up in the final version of the report. CTIA put together a response paper that raises some concerns. There was a variety of responses from the industry. There are differences of opinion on completeness of the responses submitted for the RFI. Responses were received from mobile

network operators, mobile OS developers, chipset makers, industry organizations, ENM and NDM providers, and a number of mobile-specific security vendors.

An overwhelming majority of what was received primarily focused on applications and mobile apps. Forty-six organizations provided responses to the RFI. Mr. Franklin also conducted one-on-one interviews to collect responses from a number of respondents. Mr. Franklin conducted meetings with Google, Lookout, MobileIron, Qualcomm, and Samsung among others. The interviews were extremely useful for understanding where to focus efforts for this study.

The scope for the study was fairly large. IoT devices, supervisory control and data acquisition (SCATA), industrial control systems, (ICS), customized tablets for dedicated use or single applications, such as inventory control or electronic flight, devices running mobile operating systems such as those integrated into automobiles, or other pieces of homeware, were specifically excluded.

One of the first items in the study was to settle on the definition of "mobile." The government actually has multiple definitions of mobile. For the sake of the study, the group settled on a simple definition of smartphones and tablets running mobile operating systems.

The study began with some primary mobile threat types including denial of service, geolocation information disclosure, spoofing, and tampering. The group attempted to apply the primary threat types to the mobile ecosystem. The types of attacks would not surprise anyone on this Board. The threats are representative of typical threats, but more mobile-oriented.

One of the main thrusts of the effort was to identify best practices and standards in various areas. It was interesting to find that the federal government significantly outweighs industry in best practices and standards in this domain. There were very few industry-led standards or efforts to secure mobile devices. The government received feedback that it has too many.

For instance, for mobile devices, NIST has publications 800-164, 800-124. The National Information Assurance Program (NIAP) has protection profiles in place. DHS has its own set of standards it uses as well. For mobile enterprise, SP 800-124 also plays a role, as does NIAP. The same can be said for mobile applications. For multi-networks, there was just the 800-187, "Guide to LTE Security". GSM Association (GSMA) has a number of security guidelines relating to Signaling System Number 7 (SS7).

Identifying gaps in DHS's legal authority to address federal mobile security threats was part of the original mandate of this study. DHS identified that it had no authority to require carriers to address risks relating to cellular network infrastructure being used by federal customers. Additionally, DHS cannot compel carriers to allow DHS to assess the security of their networks.

DHS is looking to obtain third-party objective evidence for the security claims made by mobile network operators. DHS proposed the following next steps: FISMA metrics reported by agencies to the Office of Personnel Management (OPM) should include information related to mobile information systems. Providing security information is currently not mandated, and may be missing when reported to OPM. It's not currently clear this information needs to be within those reports.

DHS's continuous diagnostics and monitoring (CDM) should help to encourage network vulnerability scanning tools that have the same capabilities a traditional scanning tools, such as identifying operating system, patch levels, and application versions. DHS is looking to create a new research and development program focused on next-generation mobile network infrastructure, or 5G and beyond. DHS is also looking into revisiting the methods involved with common vulnerability enclosure (CVE) generation for mobile applications, vulnerabilities in mobile systems and how that

information is shared. As of right now, mobile is not a priority for the National Vulnerabilities Database (NVD). New vulnerabilities happen every single day. The group wants to change that perception and make sure that data formats used for threat sharing can accommodate mobile threat information.

The Chair noted it may be worthwhile for the Board to work with CTIA to make mobile information sharing and CVE generation for mobile more of a priority. The communications sector has been doing a pilot of information sharing with Structured Threat Information eXpression (STIX), and Trusted Automated eXchange of Indicator Information (TAXII) for mobile threats with Professor Charles Clancy of Virginia Tech University.

Much of the discussion there has been about whether or not STIX and TAXII, as currently constituted, have the right fields to be able to share mobile threat information, including things like the telephony denial of service (TDoS) attacks that are going on. Professor Clancy may have useful information relating to the study group's work. There were some very specific types of attacks unique to networks where there might need to be some additional field modifications. CTIA's cyber working group includes wire-line carriers and some of the cable companies. There are about eight or nine companies right now. There may be some useful information for Mr. Franklin's effort.

One of the larger concerns that came up in the one-on-one discussions is U.S. government participation in international standard bodies is definitely needed. NIST has been participating in the third generation partnership project (3GPP). The group heard continuously from industry that a more comprehensive approach is needed. For instance, multiple parts of DHS, multiple parts of the FBI, NIST, and the NTIA have all participated in various international areas. Whereas, for other large countries, governments tend to send a single individual that helps to ensure that national interests are taken into account. The group was told that for the U.S., its presentations needed to not only continue, but be more coordinated.

DHS stated that a mobile threat catalogue, created by NIST, should be continued. This is available on GitHub. Mr. Franklin is working with mobile security companies and developers. Adoption is just starting, and DHS wanted that to continue. Finally, updating standards, guidelines, and best practices to mitigate the threats inside this report should be performed, especially when considering taking U.S. government devices overseas.

Public Comments and Review of Wednesday Items

Mr. Scholl noted there was one email from a member of the public with information they felt might be of interest to the Board. He will forward the email to the members of the Board.

Public Comments from Mr. Mike Nelson, Public Policy for Cloudflare

The Chair then welcomed Mr. Michael Nelson of Cloudflare to the meeting to participate in public comments to the Board.

Mr. Nelson thanked the Board and introduced himself. Cloudflare has operations in San Francisco, London and Singapore. As with his previous testimony before the Commission to Enhance National Cybersecurity, Mr. Nelson spoke about what he didn't hear in the discussions today. He hopes there will be further discussions on in the future.

The first thing to stress is that NIST has an incredibly important role in the international arena, and yet the Board really didn't talk about much of what NIST doing in some of these areas to better educate the government. NIST is involved in the international standards arena very effectively, but there's a whole lot of cluelessness in governments around the world, and some of them are spending a lot of money on technology. Some governments will push companies in directions that

don't make much sense because they don't know any better.

NIST is respected by the technical community worldwide. NIST could have a huge impact on educating governments with enough funding to actually engage in these international discussions. Whether it's the Organisation for Economic Co-operation and Development (OECD), the Internet Governance Forum; even the G-20 is looking at developing structures for international regulation of the internet. A lot of the focus is on hate speech and on content issues, but there's also growing paranoia about cybersecurity. There's nothing worse than high-level government officials who feel they have to do something and don't know what to do.

NIST has the resources and the expertise. However, not all of NIST's technical people are good at communicating with governments. Mr. Nelson hoped there will be more focus on communications even as NIST tries to deal with budget cuts. There are a lot of ways to reach the right people and build a network of clued-in officials.

The other thing there wasn't enough about was the Internet of Things. There's been testimony on the topic, and there are a lot of opportunities. It's at the very early stages, and there are already a lot of fundamental misconceptions. The E.U. in particular has been trying to figure out a way to make sure that every single thing in the Internet of Things is properly regulated, meaning every five-cent or ten-cent device multiple mechanisms for meeting whatever cybersecurity demands are put on it. It makes no sense because those things can be secured much more efficiently by securing the cloud they're embedded in.

Cloudflare released Cloudflare Orbit a month and a half ago. It's a virtual private network for IoT devices. Cloudflare has customers like Lockitron, which is a connected network of locks. Lockitron has a real interest in making sure that these electronic locks are not attacked by a DDoS attack. It would be a very effective way to keep people out of their customers' houses, so they hired Cloudflare to build this service that will protect those devices.

Cloudflare already serves a lot of other device makers who realize that it's much easier to secure the network the devices plug into, than to be ready for every possible attack. The cloud can be updated, but the device can't be updated once it's installed in somebody's door.

The other thing to highlight is something Mr. Nelson announced yesterday, an app store for Cloudflare. Developers will be able to use application programming interfaces (API) to plug into all the features of 115 Cloudflare data centers in 55 countries around the world.

The basic purpose is to filter out botnet traffic. The same network as a content distribution network, and a provider of very strong encryption. A lot of analytics can be done with that network that aren't possible with the regular internet. Developers are now going to be able to tap into the power of this platform. It is a more secure version of the internet with all these added features. The most important thing for these app developers to know is that Cloudflare's first three venture capital investors have put $100 million on the table to invest in app developers developing exciting things that might have commercial potential. It is a different model.

Many people are still working under the old model where there's a server and a customer. They don't understand all the things going on in between the server and the customer, and all the ways Cloudflare, AT&T, Microsoft Azure, Amazon and others can participate in that process. There's a lot of people out there creating structures that could be used to make the whole infrastructure a lot more secure. Yet, it's not being explained. People don't understand it and journalists aren't writing about it. It's fundamentally changing the way traffic flows over the internet. It provides a whole new opportunity to make the network secure.

Mr. Nelson hopes NIST can salvage some of the budget that's been cut. There's a lot of interest in hearings on the Hill where cabinet secretaries have been up there and have been asked, "What would you do with an extra $5 million?" He hoped Commerce's secretary has a good answer.

The Chair thanked Mr. Nelson for participating, and noted it might be worthwhile to have the IoT portion of Mr. Nelson's talk again at one of the future meetings on IoT.

The E.U. is proposing to make device regulation mandatory, to mirror what the Underwriter's Laboratory (UL) and Consumer Reports are doing on device safety. It might be worthwhile to have UL and Consumer Reports come in to talk about what they're doing. There is some merit in beefing up security to the device at some level, but it depends on what the device is.

Different levels of device security are needed but not all devices will be secured. Some kind of cloud mechanism will be needed for devices not otherwise secured. No matter how many standards exist, there will always be a device that's not secured. Determining the role of the device, the role of the network and the cloud, is ultimately what has to be done.

Mr. Nelson has maintained that the "Internet of Things" is an unfortunate term because it focuses all attention on the things. If it were the "Cloud of Things," then focus would be on the cloud and the data in the cloud. The cloud is what needs protection, not necessarily the things.

There is agreement on the international side on IoT, to be discussed tomorrow. There seems to be a lot of anecdotal interest from various companies and various foreign governments in putting this framework as a model for what they'll be doing in regulation abroad. It isn't necessarily a NIST job to do the marketing abroad and the evangelizing. There are other mechanisms for that, including industry partners from global companies in a position of having to reconcile competing overlapping government-mandated standards of practice. There is conversation among large, multinational companies on how to promote the idea of trying to coalesce around the framework. Microsoft has been pushing getting the framework adopted as an ISO standard. There's a lot of discussion going on in this way.

There have been a lot of people who have done a really good job putting the framework out internationally. It's always a challenge to go to countries to ask them to adopt something that was generated in the U.S. The business community and government have both tried to partner in this area. The important thing is the technologist delivers the message ten times more effectively than a lawyer, a diplomat, or a businessperson. A businessperson will be perceived as promoting their own business needs. Whereas, NIST can come in and say this is the best possible framework for technology. It's also important to note that the international community was not silent during the development of the standard as well. There were explicit mechanisms to provide input that were not limited to U.S. enterprise.

Board Items for Discussion

Dr. Romine presented the corrected information for the table in his presentation Wednesday morning. The NIST research budget line in 2017 was overstated. ITL is a subset of NIST research, and cybersecurity is a subset of ITL. The third line is a subset of the second line, which is a subset of the first line. Cybersecurity was at most half of the budget. The question is the trend line, which shows that the budget going down in cybersecurity by 9 percent, but ITL is being asked to do more and more on cybersecurity.

Mr. Boyer noted the question from the Board's perspective, is given the vital role that cybersecurity is playing with all these different areas the Board has discussed, is there an area that should be cut? The Board's should not use its position to weigh in on the broader budget issues that are going on.

The Board can speak specifically to the cybersecurity mission space.

NIST can accept money from other federal agencies when the missions overlap. The other mechanism for possible funding is working with other agencies. There is the federally funded research and development center (FFRDC) that is contained within the National Cybersecurity Center of Excellence (NCCoE). NIST can accept work for other agencies through that mechanism where it's consistent with the mission of the NCCoE. The NCCoE is a particularly streamlined mechanism for other agency funding where the missions overlap.

The Chair wrapped up with noting there are a couple areas that could be flagged for further discussion. The budget issue, the role of NIST, and the legislation on S&T should be flagged for discussion. The framework integration in federal agencies is also something to think further about. Dr. Romine's items to consider should also be included for discussion Friday.

Meeting Recessed

The meeting recessed at 4:03 p.m., Eastern Time.

Thursday, June 29, 2017

The meeting opened at 9:09, Eastern Time.

DDoS Report in EO

Evelyn Remaley, NTIA

Kevin Stine, NIST

The Chair welcomed Evelyn Remaley of NTIA, and Kevin Stine of NIST to the meeting to update the Board on DDOS reporting and the executive order. Mr. Stine provided an overview of the tasking in the executive order relating to distributed denial of service (DDOS) attacks, resiliency, and distributed threats. These items are in executive order Section 2 on cybersecurity for critical infrastructure, with Section (b) covering resilience against automated distributed threats, becoming a report to the President. The report will identify and promote action to improve the resilience of the internet and communications. It seeks to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks. A preliminary report for public review and feedback will be issued in early January 2018. A final report will be delivered to the President early to mid-May next year.

Commerce and DHS, working in conjunction with other agencies, are called on to run an open and transparent process to solicit and identify actionable international recommendations to address threats. They seek to understand the work in past administrations and utilize engagements with industry on botnets to build on that work. The group can get a better sense of not just the past and present, but also emerging ideas, techniques, and capabilities in all these areas. It is a diverse group that includes communications providers, device manufacturers, consumer or user organizations, corporations, government agencies, and end users.

There is a considerable focus on the words and meanings of "open" and "transparent". The words appear frequently in the executive order, particularly relating to this task. There are a number of activities already under way or announced as a request for comments. A public workshop is coming up at the NCCoE in the next couple of weeks.

Ms. Remaley and Mr. Stine noted they are fortunate to work closely with those who drafted and wrote the executive order, and that a year was allotted to complete the task. Many of the other cyber executive order deliverables have a much shorter timeline. It is a representation of how important the Administration thinks it is for stakeholder feedback to be considered in this area.

The request for comment (RFC) is in process. Comments are due July 28th. There has been really good work done in the stakeholder community over the last several years. It is work that the White House helped to host. CSRIC and others in the sector have looked at what barriers have gotten in the way of progress in this area.

The intent is to build on the work that's been done, and receive feedback on what is working well, what's being done, and what gaps still exist. There's a sense that the environment has evolved and there is a need for new ideas and ways to look at how change has happened. The executive order seeks to examine why and where gaps are occurring, which is also the intention of the upcoming workshop at NIST to hear from stakeholders about what those ideas are.

There will be time for industry members to comment on the report they pull together. NSTAC is also working on a piece to be included in the White House report. The report will be posted publicly for stakeholder feedback in January, 2018. The feedback will be used to produce the final report due in May.

The RFC is broken down into seven questions, mostly related to what's happening and what else could be done short-term and long-term. It is also broken down to gather guidance into two particular areas of focus: the network management aspect problem in terms of what additional things can be done, and what impediments are happening.

NTIA has a multi-stakeholder process underway in IoT patching, which is doing some interesting things. The stakeholders are coming up with good ideas that can contribute, but there are other things that need to be done. They're trying to identify areas where, with the right stakeholders and additional dialogue, it would create another incremental step forward in making the environment safer.

In terms of the RFC, there's a sense of how the stakes have changed following the activity in the fall, and this week. There is a definite desire for more progress. In terms of talking with other policy colleagues on the national level, at Commerce there is a strong belief in how industry and stakeholders are the right place for solutions to happen.

As the environment has continued to evolve it's getting harder to keep the stakeholder message going. It is a very important time to hear from stakeholders and for stakeholders to come together. Ms. Remaley hopes to hear from the Board in terms of what it views as the solution space, in order to continue to move the ball forward.

The second significant piece of the stakeholder engagement is coming up in less than two weeks. It's a public workshop at the National Cybersecurity Center of Excellence on July 11-12. The workshop is on enhancing resilience in the internet communications ecosystem. With the RFC extension, the workshop at just about that two-thirds mark in the comment period. It will be a great opportunity to get people together, especially those who haven't had a chance to formulate responses yet.

Ms. Remaley encourages as many folks as possible from a diverse set of stakeholders to submit responses. The purpose of the workshop is to explore the entire landscape of current and future practice and emerging solutions, with an eye toward understanding some the challenges and barriers that have made positive progress difficult in the past.

The workshop will be organized to focus on five main areas. Those areas will have panels to encourage discussion. Facilitated breakout sessions will follow immediately for a more robust discussion on the topic and expand on some of the great ideas that were discussed. The panel focus areas includes infrastructure providers, product development, customers, organizations, individuals; relevant emerging research ideas, and the government role, both domestic, and international. Having international participation to talk about these topics will be key. The panelists will represent a variety of different stakeholders across the different panel discussion areas, from the communication sector to end user organizations to product developers and the research community and government agencies.

The workshop will include many of the agencies that NIST consults with. Following the workshop, a proceedings document will be posted that identifies areas of future discussion, key themes, and key takeaways that were expressed in the community. It will be presented in a way that looks at the potential short and long-term opportunities, barriers, challenges or constraints. The output of the workshop will be the RFC responses and the NSTAC report with other feedback. It will provide significant input into the preliminary and final reports over the next several months.

As part of the process, Ms. Remaley is trying meet with folks on a more intimate basis. NTIA and NIST have setup meetings with various sectors and key technologists. The meetings have been very illuminating in terms of some of the challenges that each sector is seeing. The theme that keeps

emerging is everyone recognizes there is a lot of good work that's been done.

It may be there are economic or market pieces as well. Perhaps there is a need to shift what falls into the categories of product manufacturers and government. The President's Commission last year talked about incentives and liability issues. The complexity of the space is going to require multifaceted approaches to managing roles. The other piece is the international aspect, which is significant. There's been close interaction with the White House on progress and meeting the solutions they proposed.

There is a year from May 11th to complete the task set out in the executive order. The problem will not be solved in a year. The plan is to identify a roadmap to making progress. The expectation is to start the work this year, but not to complete all of it. Part of the challenge is putting things in short- and long-term buckets. There are a lot of good ideas, but all are incremental. Is it possible to make things a little bit more difficult for the attackers tomorrow? It is one of the reasons the group has also asked about governance models. The adversary is very agile adversary. How can the U; S. collectively, be agile as well? There has been some good progress but some things have become more complex. There has been talk about the device side and the network layer and different pieces of the network.

Executive Order Agency International Reporting

Jordana Siegel, DHS

Adam Sedgewick, DOC

The Chair welcomed Adam Sedgwick of DOC, and Jordana Siegel of DHS, to the meeting to update the Board on executive order agency international reporting. Mr. Sedgwick presented an overview of the scope of the international component of the executive order. Section (c) speaks to international cooperation and will be discussed today. Commerce, State, Treasury, and Defense are required to submit reports in forty-five days to the President. The State Department will provide a report to the President, documenting an engagement strategy for international cooperation and cybersecurity. All the agencies that wrote reports work with the State Department in determining how to fit those priorities into a broader engagement strategy. The Commerce report has been delivered to the White House, and is being reviewed.

The discussion covered some scope of the international section and the Commerce perspective on the cybersecurity mission. Commerce relied heavily on NTIA in developing the report. The International Trade Association (ITA) and the Bureau of Industry and Security (BIS) have worked closely with Commerce on cybersecurity. Bringing together the bureaus and the diverse mission of those bureaus to have consistent policies has been a multiyear effort.

It's been a means of understanding how to make use of a very diverse workforce with diverse missions and come up with a consistent approach to cybersecurity. For the report itself, the Commerce approach was to think about key priorities from a mission perspective and then highlight programs that support those priorities.

Cybersecurity is needed not just for national security interests, but for continued U.S. economic leadership. If there isn't trust in the internet and confidence in the security and stability of these platforms and services, then all U.S. industry will be in a lot of trouble. Priorities include encouraging and facilitating cybersecurity innovation through the global marketplace, and ensuring that cybersecurity policies are globally relevant. It includes some of the work under the International Cybersecurity Standards Working Group (ICSWG). International successes with the cybersecurity framework have been attributed to the partnership with ITA.

ITA has an interest in insuring that U.S. companies can participate in that global market. Increasingly, they think about things like cybersecurity regulations in other countries and how that might be closing out the marketplace. Things being highlighted now include the cybersecurity framework, multistate voter processes, internet engagement, and standard coordination. Feedback is welcome on these priorities, and if programs are meeting those priorities. We'd also welcome feedback if there are key programs that would be outside of those priorities.

Ms. Siegel discussed the importance of the work that went into the development of the international engagement strategy. The "open" and "operable" and "secure" and "reliable" concepts are reinforced in the executive order. The process provides an opportunity to think about what has changed and those underlying concepts in the context of the development of the international engagement strategy.

At DHS, international engagement happens in the context of its mission. The cybersecurity mission lies in five key areas: leading the federal government efforts to secure networks in federal facilities and executive agencies; working with the public and private sectors to enhance critical infrastructure, cybersecurity, and resilience; utilizing the DHS law enforcement authority to assist law enforcement efforts to prevent, counter, and disrupt cybercriminals; responding as authorized to significant cyber incidents; and strengthen the security, privacy, and reliability of the cyber ecosystem.

The core components that have a cybersecurity mission and some international presence and engagement are the National Protection and Programs Directorate, the Secret Service, Homeland Security Investigations, the Science and Technology Directorate, the Transportation Security Administration, and the Coast Guard.

Internationally, levels of response to issues vary among the range of partners. Some countries follow a model similar to the U.S. They create sectors and have follow-up engagement. In certain regions there are broader policy trends that are influencing the process. The E.U. and the Network Information Service (NIS) have influenced some of their members to consider some cybersecurity policies. Some of those member states have been doing it for a long time. Others may be considering these issues for the first time. When travelling internationally, the emphasis is on the importance of the private sector engagement piece. There is also lot of interest and discussion about how to help small and medium businesses. There have been discussions about how to expand that out and potentially move it to international standards bodies. There was a lot of blowback from small and medium businesses that felt like it might reduce access to their ability to influence the future development of the cybersecurity framework.

Some of the informal pushback that may happen in international discussions will be along the lines of countries having predominantly smaller businesses and the focus should be on them. Businesses have different levels of hygiene.

We've heard very different things from different stakeholders regarding the U.S. origin of the framework and other documents. In some countries, the brand goes a long way and having the U.S. government involved gives it a degree of credibility. In other countries, some steer clear because the U.S. government has its name on the framework.

Executive Order Market Transparency

Lisa Barr, DHS

Evelyn Remaley, NTIA

The Chair welcomed Lisa Barr of the DHS Office of Cyber Policy, and Evelyn Remaley of NTIA to the

meeting to update the Board on the executive order market transparency deliverable. Ms. Barr provided a brief description of their approach to the market transparency deliverable related to the executive order. The executive order transparency report is a deliverable that the administration put forward to DHS in coordination with Commerce to examine sufficiency of existing federal policy practices and the appropriate market transparency of cybersecurity risk management practices, and critical infrastructure. It examines federal policies, and what practices and guidelines should be established through the executive branch and independent regulators.

These cybersecurity measures might include documents focused on cybersecurity management practices, disclosing internal cybersecurity controls, and reporting cybersecurity incidents. The question is, does the federal governments and/or its agencies put out information focused on providing guidance on what to disclose publicly?

The goal is to arrive at market transparency. Does the information that's put out help to inform shareholder and critical infrastructure decisions when it comes to relationships with other publicly traded entities? There is an assumption that shareholders and stakeholders of a critical infrastructure entity have a compelling interest in whether another entity is making appropriate investments in cybersecurity risk management practices. Is there sufficient transparency with those risk management practices? Sufficient transparency about cybersecurity risk management practices is essential for stakeholders to better understand or evaluate the risk of other entities.

The administration directly requested Congress to look at transparency as it currently exists. The approach has been to put out a request for information to the sector-specific agencies who look at critical entities, such as Treasury, DOD, and others to ask what guidance exists for critical structure entities to promote agency cybersecurity risk management practices.

There is consideration of collecting everything that the government puts out on guidance in transparency in cybersecurity. The Securities and Exchange Commission (SEC), the Federal Trade Commission, and the Federal Communications Commission, the sector-specific agencies, and The Federal Energy Regulatory Commission (FERC). The North American Electric Reliability Corporation (NERC) have provided guidance as well. Most of the material deals with guidance on disclosure of incidents and breeches.

Ms. Barr and Ms. Remaley are also conducting a literature review to examine the sufficiency of existing guidance to promote cybersecurity risk management practices. The review attempts to examine what has been written on the sufficiency of those practices published by the federal government. They are also assessing transparency systems to determine their effectiveness in promoting policy goals. It will lead to a report to the administration that focuses on everything the federal government publishes and its sufficiency as well as how transparency systems generally inform policy goals.

The report on transparency is one of the quickest tasks from the cybersecurity executive order. Commerce and DHS are partnering together on the report. Commerce's experience with the cybersecurity framework is why the agency was asked to coordinate with DHS to work with stakeholders on risk management. What has been mapped in the time allotted is a good way to answer the question the task was designed to answer.

There may be a RFC with follow-on questions such as whether the information provided today is adequate from an industry or investor perspective or other things that may also be helpful. The due date for the report is August 9th. It is a very short window. Treasury was very forthcoming in wanting to have Ms. Barr and Ms. Remaley talk with their financial services sector coordinating counselor. They are here to get some thoughts and feedback on the approach to the report, and

what may be missing in terms of sources or additional areas to consider. There has been interest from the Chamber of Commerce to do something through them. Because the activity is so constrained on time, conversations must be meaningful.

When talking to enterprises, it's not the guys in IT that are the transparency concern. They would spend more time on security if they had the money and the people. For public companies, the question becomes is the board paying attention? In most cases, it's not that they wouldn't want to pay attention and be involved, but there's so little understanding of the risk to their companies at the board level. That lack of understanding changes the priorities. Boards tend to take a cursory view of cyber activities. Cybersecurity conversations need to be more on the risk side than merely short operational reviews. Substantive conversations about the risk rarely happen.

The challenge with security transparency issues is how to strike the right balance and provide information that's actually relevant. It has to be meaningful for making investment decisions without making so much information public that it's problematic from the company perspective. It's a balance that's needs to be struck.

There's also an embedded assumption that increased transparency will lead to increased investment which will then lead to more security which, overall, makes entities more secure. More boards pay attention now than they used to. In those situations, boards are getting more sophisticated. A lot of boards pay attention, but most of them have no idea what to ask and they don't understand the answers. The problem used to be, how to get the board to pay attention. Now, it is how to help them to understand what they're hearing.

Cybersecurity insurance has been central to the discussion on assigning values to risk. Last week there was a press release. Insight and Risk Release published standards with the metrics and the measures they will use to rate companies for their cybersecurity hygiene. The standards, in turn will be used by the insurance industry to be able to measure risk in a company for purposes of deciding how much their cyber premium will be, what are they covered for and at what level. It can then start to factor into board level decision making in terms of real costs, and real financial risks that are quantifiable by the insurance sector.

Tom Finen of DHS led a process a few years ago which resulted in the Cyber Incident Data Repository (CDRI). It was the notion that there should be sector-specific anonymized cyber-incident reporting by the private sector or members of the public into this repository in such a way that insurance companies could get a picture of the landscape of risk. The question became, who would own this repository? It should not be government, because companies are going to report to the government in something that could be a slippery slope to regulation.

It may be worth looking at judicial precedents in this area if any exist. The FTC has had some smaller liability cases dealing with the consumer market aspect. Common law, tort law, at the state level might be good sources. A couple of big judgements will impact companies. Lawyers see the judgement, and send out the guidance that companies should do X to avoid situations in the future. The problem is making information that's out there more useful. A SEC action is probably going to lead to companies dumping a lot of information out there so they can say that they've done it.

There was a development of a FAR section requiring notice of an incident. There is a lot of sharing going on from a contractual perspective. There's an expectation and willingness to share when it's a private sharing situation. But within transparency, getting the information out there more broadly is a different calculation that organizations go through in terms of sharing. There are other risks that they would have to work through.

Finally, the Administration has not determined if this will be a public report. There is internal

debate on this question. Ms. Barr and Ms. Remaley are trying to promote the idea that certain aspects of the report should become public. Given the fact the topic is market transparency, they are encouraging making portions of the report public with The White House and the Administration.

Executive Order Workforce Report

Rodney Petersen, NIST

The Chair welcomed Mr. Rodney Petersen of NIST to the meeting to update the Board on the executive order workforce report. Mr. Petersen reviewed the executive order as it relates to workforce and workforce initiatives. There are four major parts of the executive order. The workforce section is the final section of the report but it's foundational. If the right people are not in place, government or critical infrastructure won't be protected. There was evidence of workforce importance when national security positions were exempted from the hiring freeze and cybersecurity was quickly included under the national security umbrella.

It reinforces the efforts to increase the workforce in cybersecurity. The last sentence in the policy statement, later in the executive order starts to talk about cybersecurity for the nation, really says what we're trying to do. "The United States policy is to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields as the foundation for achieving our objectives in cyberspace."

Ultimately, NICE is asked to develop a report with recommendations on the growth and sustainment of the cybersecurity workforce. There are three workforce deliverables. Mr. Petersen will discuss the workforce deliverable and provide details that relates to what NICE is responsible for.

What NICE is focused on is growing and sustaining a workforce. It is the second deliverable in the executive order, due in 120 days. There are two parts of the workforce requirement in the executive order The first requirement is an assessment of the scope and sufficiency of efforts and it uses a few key words: "educate", "train", "cybersecurity-related curriculum", "training', "apprenticeship programs", and emphasizes primary through higher education. It's become the basis for a lot of the work in terms of the approach to the assessment.

The report is about the nation’s cybersecurity workforce, not just federal government cybersecurity workforce. It is really important that the issue is approached by way of process. When talking about private sector needs, NICE needs to be engaging with private sector organizations about the challenges and opportunities.

Who is accomplishing the work? The executive order talks specifically about the Department of Commerce and DHS co-leading the effort. From very early on, the White House was pretty clear that NICE should take the lead in consultation with DHS. NICE has been working in collaboration and partnership with DHS, but really taking the leadership role with a lot of the NICE team directing activities. It also specifically mentions the Department of Defense, Labor, Education, OPM, and other agencies that NICE might identify. The National Science Foundation (NSF) was missing from the list. It has some of the greatest investments in cybersecurity education and workforce development, so they were brought in. They're probably the most active participants in the working group because of the variety of programs and investments they have.

As part of the DOD, the National Security Agency (NSA), co-leads the Centers of Academic Excellence (CAE) who has been an active participant as well. Health and Human Services came forward early on because of some huge programs and concerns they have with the health industry, within the government and outside. A few other agencies join in the effort such as the Department

of Energy. Along with the government stakeholders and utilizing the work NICE already does, NICE sought to include academia as well as the private sector.

Assessment of scope and sufficiency of effort began immediately. A request for information will be released shortly to allow private and academic sector input. Once it's out, there will be a few questions that will allow feedback to this process regarding the assessment, and also with respect to findings, recommendations, and additional things to consider. A workshop is planned in early August after analyzing the results of the R-5, completed the assessment, and tested some of the ideas and learning in order to get some feedback as well.

Science, Technology, Engineering and Math (STEM), IT, cybersecurity and computer science education are clearly related to the work of NICE. The domains listed here are mainly the labels that were in the executive order. NICE is looking at the K- 12 and higher education piece, apprenticeships, and training. A couple of additional focuses have been added, including separating out the public workforce and the private sector workforce because of some different initiatives.

There were other topics either in, or discussed after, the executive order like cybersecurity-related curricula that relates to everything discussed here. We're always asking questions about curricula and guidance that might be related to training and education at various levels. The White House may possibly regret it didn't include competition, challenges and exercises within the executive order. However, the Cybersecurity Enhancement Act of 2014 provides a title on competitions and the role that NIST plays along with NSF, DHS, and competitions. NICE is making sure it talks about competitions as well.

Various types of data exist regarding existing programs. Assessing graduation levels and trends over time is important. A state of continual progress is important to get to. There is not as much output data as there could be. The focus will shift to the types of metrics or measures needed to measure impact or outcomes. It may not be enough to see a student graduate, but also to know if they actually get a good job earning a good salary. Those kinds of outcomes can be used as metrics to some extent.

The apprenticeship executive order is more explicit. It seeks to include people already in IT and possibly transfer them into security. Educationally, there are students of traditional age coming through the pipeline. There are also increasingly middle-aged adults, who already have a bachelor's degree, that go on and change careers. They go back and either get another degree, or get some training at a community college, or a certification. One of the NICE strategic angles is to accelerate learning and skills development. That's a great example where the existing workforce with aptitude or ability can be moved into cybersecurity careers.

For example, in K-12 education, if NSA has gen-cyber camps and hundreds of students and hundreds of teachers attend camps over the summer, how is the effectiveness and sufficiency evaluated? There may be some related threads. Whether it's education or training, the NICE strategic plan talks about performance-based assessments. It is equally applicable in a high school or college or training environment. The Certified Information Systems Security Professional (CISSP) exam, for the most part, is a multiple-choice exam. The International Information System Security Certification Consortium (ISC2) introduced a lab exam with performance requirements as part of the latest certifications. It can be used towards a better measurement of learning and skills than with just the knowledge test.

When trained students get jobs, they often switch to the private sector because it offers substantially more pay. It's not just from the side of the government, it's also industry to industry as well. It is a continual issue. If some of these initiatives are successful, there may not be that kind of

swing in salaries and attrition after reaching the certification or the skill. Things may stabilize a little bit.

The Department of Commerce did a return on investment (ROI) study on apprenticeships and found that employees are more likely to stay with the employers because of the investment in their education. It increased loyalty and commitment to their mission. There is not that same kind of evaluation outside of apprenticeships, but the same argument is made. Companies invest a lot of time and money to put an apprentice in training to developing skills.

The group is looking at apprenticeship from the academic perspective with the National Science Foundation. Students get surveyed on whether they get jobs, where they are working, etc. To date, nobody's been able to answer if the Scholarship for Service (SFS) students ten years ago who've already fulfilled a two or three year commitment, are still with the federal government.

The report is due to the President on September 8th. Internally, it needs about a month for approvals and clearances. The internal deadline is August 11th. NICE held a webinar on June 5th to talk about the executive order, the RFI and the workshop. Three hundred people participated live. Five hundred people listened to the recording. The details about the R-5, the details about the workshop as well as, other information are available online.

Three weeks ago, another executive order was issued on apprenticeships. Apprenticeship is one of the topics NICE was expected to do an assessment on. NICE has been looking at apprenticeships for the last couple years and apprenticeships are in the strategic plan as well. Some pilots and examples are starting to emerge, particularly with employers working with community colleges. Caterpillar has a secure software development program where they're bringing people in as apprentices down in Virginia. They have a cybersecurity analyst role they're trying to build some apprenticeships around.

The executive order on apprenticeship attempts to provide more affordable pathways to secure a high paying job by promoting apprenticeships. The Department of Labor has been doing work in apprenticeships for years. It's almost an executive order within an executive order because it doesn't just talk about apprenticeships, it talks about effective workforce development programs.

Commerce will have a role in promoting to business leaders and cybersecurity is specifically mentioned. This is the first time where cybersecurity has been called out as a type of apprenticeship or a sector where apprenticeship can be useful. There'll be a task force on apprenticeship expansion and Commerce will also have a role as the vice chair of that task force.

The second part of the executive order which relates to the work that we're doing already, talks about improving the effectiveness of workforce development programs. It defines workforce development programs as those designed to promote skills development in workforce readiness. A program like NICE or the Centers of Academic Excellence (CAE), the Scholarship for Service (SFS) and many others loosely define themselves as workforce development programs. This executive order starts to talk about evaluations of effectiveness, employment outcomes, and elimination of programs that are ineffective, redundant or unnecessary.

A whole other area that NICE is working with is looking at credentials with the Lumina Foundation and a lot of non-profit organizations. Whether it's a college degree, a high school diploma, or a certification, the goal is to try and improve the quality of credentials instead of just having the degree or the certification as a demonstration of skills. They're working with the higher education system, taking things like transcripts to make them more than just a course and a grade to have those records more holistically report student experiences. Working with companies and organizations that are committed to rethinking credentials is the framework in which a different

way to report student experience is happening.

The August 2nd workshop in Chicago will be organized differently than has been done in the past, as it is scheduled for only four hours. The earlier plan was to have more than one workshop, possibly with two or three half day workshops. There is still a possibility a second workshop will be offered, depending on how the timing works out. The workshop will cover a few of the most relevant topics on apprenticeships.

Curricula is likely to be another topic because it's included in the Cybersecurity National Action Plan. The plan talked about the lack of agreed upon curricula for cybersecurity. The previous administration funded a lot of efforts. NSA is still giving out grants for curriculum development. There's an Association for Computing (ACM) IEEE project with a curricular framework. The project is going to be hosted by academic institutions as part of the Centers of Academic Excellence and has lots of connections in the community.

Sustainability is another area we're kicking around a lot in terms of what it means. A lot of the federal government programs are not necessarily authorized in law or appropriated through recurring budgets. In the Centers of Academic Excellence in cybersecurity, there are almost 250 universities with that designation. It's dependent on the availability of funds and resources to make that happen. NICE is fortunate that there is an appropriation in addition to the authorization.

As part of the assessment, we're looking at data that's available. We're probably putting a lot of weight and analysis about the number of jobs that are currently open as well as the size and growth of the current workforce. Organizations will be doing annual surveys on what the projected workforce will be in the future and NICE expects growth in cybersecurity jobs to continue. Some pretty significant surge activity will be needed in the coming years. NICE is looking at both current demand as well as future growth.

Ransomware Threat Brief

William Wright, Symantec

Roselie Custodio, FBI

The Chair welcomed Mr. William Wright of Symantec, and Ms. Roselie Custodio from the FBI, to the meeting to update the Board on ransomware threats. Mr. Wright provided an introduction to ransomware. It has been around for a long time, and has continued to evolve during its existence. There has been a big rise in "locker" ransomware. The older type involved the computer screen being locked up. There's an official message apparently from local law enforcement, saying there's some illegal activity. In order to unlock the computer, the owner must pay the fine or the police will come knock the door down. The screen had a little timer counting down the time until the police would come, and it was very effective. This ransomware is still around, although its success is waning somewhat.

Currently, the predominant ransomware type is crypto-ransomware, which encrypts files. The file owner must pay a fee to decrypt the files. Ransoms are taken almost entirely in bitcoin now. It's a big advantage to the cyber-criminals as they can receive money anonymously. There has been a 36-percent increase in the last year alone. The reason is, it's very easy to get in to and it's highly profitable. It's not difficult to figure out how to do it. There is now ransomware-as-a-service. There's competition that's driving prices down for ransomware-as-a-service and the criminals are getting better at it all the time. The free market works in ransomware too. The final stats for 2017 are not available yet, but an equal or greater increase in 2017 compared to 2016 is expected. Much of the information presented here comes from Symantec's annual internet security threat report.

These attacks have spread out across different criminal organizations. The number of ransomware families has tripled. In 2016, Symantec tracked 101 ransomware families. A lot of people are getting into deploying ransomware, and they're doing it because it works.

All countries are victims of ransomware, but the United States is by far the largest. Attacks tend to happen in certain countries that are more likely to pay. Some of it comes down to having internet-connected computers in that country. At present, more consumers are attacked with ransomware but those numbers are changing as more and more organizations are hit with ransomware. The U.S. also has a very distinct characteristic that is driving up ransom costs. In 2015, the demand was $294.00. In 2016, it went to over $1,000.00. Demand amounts are also subject to market forces. If criminals hit the wrong price point, they won't make money. They've honed their skills at finding that exact amount people will pay.

A lot of organizations will look at a demand for $1000 and possibly think it might be worth it. However, the amount really doesn't take into account damage to the brand, the damage from being offline, associated legal costs and the mitigation process. The number is really much, much larger than $1000.

Symantec recommends for people to not pay the ransom. There's a number of reasons not to pay. One big reason is once an individual or organization pays a ransom, they will be targeted repeatedly. They end up on a successful attack list. What's driving malware attacks up? Globally, 34 percent actually pay the ransom. Here in the United States the number is 64 percent. As long as victims are willing to pay, criminals are going to keep pushing the envelope and upping the demand numbers.

WannaCry is one of the worst and most widespread pieces of malware we've ever seen. It had 220,000 victims in 150 countries. In some ways, it is very similar to any other ransomware. It infects a computer. It encrypts files and then it demands a ransom. What made it remarkable was how it propagated and spread. Interestingly, in total the criminals collected approximately $110,000.00 over the course of the attacks. Two of the three bitcoin wallets that were set up to receive ransoms had critical bugs and were unable to receive payments.

A lot of people ask whether the attack was a zero-day. In January, 2017, U.S.-CERT issued an advisory on Server Message Block (SMB) vulnerabilities. In March 2017, Microsoft released a patch on this exact vulnerability. In April 2017, the Shadow Brokers released a large cache of exploits that included EternalBlue, which exploits Microsoft's SMB. The WannaCry outbreak began on May 12, 2017. The initial threat infection vector is still uncertain. Once in a network, it encrypts, self-propagates, and spreads to semi-random domains. It is one reason it spread so quickly. Microsoft also issued a patch for Windows XP.

There has been a lot of discussion about why it didn't hit too hard in the United States. A lot of people say the U.S. has really good patching methods, or that people in the U.S. are a little more sophisticated, with better security software and fewer legacy systems. All that is true but there was another reason. Marcus Hutchins, a security researcher Great Britain unknowingly stopped the malware from spreading by sink-holing the domain that the malware would query. It essentially created a kill switch. He noticed there was a domain within the code, and he registered the domain. It's not known why the domain was in the code. However, it's clear everyone dodged a bullet when Marcus Hutchins registered the domain.

Symantec attributed the attack to the Lazarus Group with a high degree of confidence. There's a lot of shared public code, but the potential attribution lies in the non-public code. That code would be very difficult to get. There are some similarities with Lazarus code. Symantec found earlier versions

of this WannaCry ransomware on computers going back all the way to April (several months prior to the outbreak), that also had Lazarus-specific tools.

Lazarus is the group that's also been associated with the Sony attacks, with a number of attacks on Seoul, Korea's financial district and last year, the SWIFT attacks, which ended up stealing $81 million from the Bank of Bangladesh. It was actually a $1 billion scheme but they only got $81 million. The FBI has attributed the Lazarus Group to the government of North Korea.

In the immediate aftermath of the WannaCry attack, there is a silver lining to the entire event. There was very effective collaboration between the public sector and the private sector, and very quick work on the part of the government; specifically, NCCIC.

They had Symantec on the phone almost immediately, trying to get some ground troops in the very early hours of the outbreak. Then, NCCIC really set up an appropriate cadence for the situation. There were twice-a-day calls with very active participation. More than a dozen other security and IT companies were involved in sharing real-time indicators, mitigation techniques, and information on threat vectors. In addition, NCCIC put out really good written analysis on the attack that was used and initiated a dialogue between security company analysts and DHS analysts. Even after the infection waned, Symantec continued to share details about what findings on the attribution front, the Lazarus connection. It was one of the more successful public-private collaborations that Symantec was a part of. Information from the Cyber Threat Alliance ended up being very helpful as well.

Mr. Wright also talked about the Petya ransomware attack. The attack happened two days prior to the ISPAB Board meeting. It was clearly inspired by WannaCry. Petya hit many sectors across Europe and elsewhere. As of the date of the meeting, it hit about 60 countries. However, it was primarily focused in the Ukraine. Petya used an external group exploit as one of the means to propagate itself. It also spread by acquiring user names and passwords to spread through networks. It was much more effective in spreading within a network. Machines could be patched against EternalBlue and still be infected within that network. It's one big difference.

It differs from typical ransomware in that it doesn't just encrypt files. It also overwrites and encrypts the Master Boot Record (MBR) causing a more destructive attack. It demanded $300.00 worth of bitcoins to be paid to recover the files. To date, there've been a paltry 45 payments to the bitcoin wallet for that attack. It may not have even reached $10,000.00. Now it's not even possible to pay to that wallet. There is no evidence that those that did pay got their data decrypted. In fact, it's been quite the opposite.

It's believed the initial infection vector was a software update to MeDoc. MeDoc is a Ukrainian tax and accounting software package. After gaining an initial foothold, Petya used a variety of methods to spread across corporate networks. There is some indication that Petya was more targeted in this way than WannaCry. Like WannaCry, Petya was not very successful from a purely financial perspective.

Cyber-criminals are always looking for bigger payouts. There might be fewer of these sort of "spray and pray" attacks where they are using spam campaigns and exploit kits, but we're going to see more of these self-propagating, worm-like attacks. The bad guys smelled a little bit of success with WannaCry and Petya, so there could be more worm-like attacks to come.

Targets could also shift. Everything now is a computer: cars, televisions, traffic lights. As these devices are connected to the internet, they have their own vulnerabilities, not just to other malware but also ransomware.

Symantec set up an IoT honeypot right during the height of the Mirai botnet last year. At one point, the devices in the honeypot were being attacked every two minutes. Criminals are only bound by their own imaginations. Symantec believes Petya was not financially motivated. There's a number of reasons to believe this is the case. It was designed to be destructive. The way the code was written suggests there was never any intention to be able to decrypt. It was written in a single language, English. WannaCry was written in multiple languages. Petya was far more targeted than WannaCry and more destructive to networks.

Meeting Recessed

The meeting recessed at 1:46 p.m., Eastern Time.

Friday, June 30, 2017

The meeting opened at 9:04 a.m., Eastern Time.

NIST Update

Kevin Stine, NIST

Matthew Scholl, NIST

Mike Garcia, NIST

Paul Garasi, NIST

The Chair welcomed Kevin Stine and Mr. Matthew Scholl of NIST to the meeting to update the Board on NIST activities. Mr. Scholl provided an update of activities within the Computer Security Division and ITL, as well as activities planned for the future. The Board has had many briefings about cryptography and the lab's work in the past. NIST and the lab are conducting internal research on existing algorithms and modes that will be quantum-resistant. The research will finish in November, 2017. Then two new phases will begin. One phase entails looking the research, and determining if it's good enough to be appointed to a standard or a NIST reference. The second is to determine what's missing and develop and conduct research to close gaps.

The research on cryptography is conducted very openly, jointly, and on a large scale. There are participants from the NSA, Treasury, Fraunhofer Institute in Germany, and Catholic University of Leuven in Belgium. NIST is continuing relationships with like-minded industry and NIST-like associations with governments in the Asia-Pacific and the E.U.

The goal is to have standards and guidelines that are quantum-resistant by 2020, and then start working with industry to get standards and guidelines into products. NIST is communicating aggressively with industry concerning concepts of agility. New products and concepts should be modular so they can be pulled and replaced easily. NIST likes having two block ciphers in case one becomes broken, but there is a lot of confidence in AES at this point.

It might be news to the Board but NIST now has a joint quantum institute with the University of Maryland at College Park. The joint quantum institute is a separate but affiliated component; the Quantum Information and Computer Science Center, or QUICS. NIST is looking at the concept of trust roots, a significant level of confidence in a technology to be used for trust extensions and looking at trust roots in a couple of different ways. Everyone trusts certificates. It's a ubiquitous trust root, either machine-to-machine or between individuals.

Recently, pilot programs have started deploying software test tools to industry, and if industry has met a certain level of proficiency and discipline in development processes, NIST will allow them to self-test and self-attest that their cryptography is well-formed, and then send NIST the test results. Currently, NIST uses independent laboratories to conduct all of that work. NIST continues to work in national and international standards bodies. The focus remains on work with the International Organization for Standardization (ISO), in software assurance, cryptography, and hash functions. ISO ensures that our requirements are being put into those national and international bodies.

NIST is very interested in AI from a research perspective. There are two parts of AI: securing AI and AI for security. Some pilot projects are starting to look at how commercially available AI can be used to help with big-data complex security problems, and see how well that works. NIST is looking at models to standardize how metrics are applied to vulnerabilities to allow for machine-generation auto check-in. DHS is very interested in starting to incorporate STIX into NVD as a reference feed for cyber-threat indicators.

While blockchain is very capable technology, it's horrible for usability. If the usability issues are dealt with, then commoditization may happen. We're interested in new forms of high-performance computing, and whether or not that will come to commoditization or not including mixtures of high performance computers and clouds, and peer-to-peer which will allow massive compute capabilities that weren't possible before.

Voice seems to be the way human/computer interfaces are going. A lot of this high-performance computing, voice, and AI all rely on being able to have good, reliable bandwidth. We're very interested in 5G and beyond, its design, and whether there are standards to ensure some security to what's being designed there. NIST is participating in Long Term Evolution (LTE), 3GPP, and 5G standards bodies on the international scale as well.

The NCCoE is also very excited to be hosting the July Web Expo workshop, "Enhancing Resilience of the Internet and Communications Ecosystem". It is a good opportunity to highlight some of the NCCoE's capabilities, particularly as the focus on internet infrastructure use cases increases. The document on malware has been reprioritized to have it come out in the next couple of months.

Healthcare is another important sector focus at the NCCoE. In May, NIST issued a draft 1800 series special publication on securing wireless infusion pumps in healthcare delivery organizations. This area attracts a lot of attention because there is a lot of focus on medical device cybersecurity. As the 1800 series is finalized, there may be movement onto additional types of medical devices. There is a publication in the works that focuses on imaging systems in healthcare organizations.

There was an extremely successful workshop in May, with close to 800 in-person attendees at NIST. One of the big takeaways from the workshop was there's an opportunity to provide to be a little bit more specific in the language used in talking about the framework.

An annual workshop provides a tremendous check-in with industry and other organizations, including government agencies that are now increasing their use of the framework because of the latest executive order. NIST continues to ramp up the small business cybersecurity engagement broadly, but also in context with the framework. An internal effort recently started to develop small business cybersecurity profiles in the framework.

Significant outreach to European nations continues. The European Cybersecurity Conference in Krakow is scheduled for early October. That particular event is very appealing because there's going to be a number of E.U. member nations and European industry represented. That particular event, and future ones like it, are great opportunities to join with industry groups, and be efficient with use of resources. Some of the topic areas of interest include multinational use of the framework, discussing opportunities that other countries may have, sharing the process that was used to develop the framework, and seeing how other nations use the framework.

The K-12 Cybersecurity Education Conference is December 4th - 5th in Nashville, TN. NIST is looking at introducing cybersecurity much earlier in the education lifecycle for kids in K-12. The lab supports this event. Mr. Scholl will send information on the event to the Board.

The 800-63-3 was updated last week. It is the digital identity guideline. It involved significant interaction with all different parts of the identity ecosystem. Mr. Mike Garcia and Mr. Paul Garasi will run through some of the big changes to the 800-63.

Mr. Garcia noted four documents were released last Thursday. The 800-63 was originally released in June, 2004. There was one major update in 2011, and a very minor update in 2013. Since 2011, identity has changed in how it's thought of and treated. The new revision is a complete overhaul of the document which used to be called, "Electronic Authentication Guidelines," and is now called

"Digital Identity Guidelines". The title change encapsulates the new state of identity management, which shows how much it has changed.

The document was split from one special publication into four. New sub-volumes are the 800-63-3, 800-63A, 800-643B, and 800-63C. That model allows new volumes to be added in the future as digital identity matures. Volume D Is already in internal draft. Volume A is about identity proofing, Volume B is about authentication, and Volume C is about federation. With "Dash-3", one of the significant changes from a federal agency perspective is that it adds most of the risk assessment language from OMB M04-04. One of the things that fundamentally drove this change is there is no difference in the way a final risk determination is done for identity-proofing versus identification.

When 800-53 Rev. 5 is released, it will have a much stronger alignment between 800-63-3 and Revision 5 of 800-53 than existed before. The language is compatible with the Cybersecurity Framework (CSF), and the CSF is much more strongly aligned with the RMF in general as well. With the privacy engineering work presented by Ms. Levkovitz, NIST has moved privacy requirements and considerations directly into the document, as well as feasibility considerations. The intent was to make this document something agencies could pick up and use to take care of digital identity without having to go to different sources.

Additionally, NIST spent a lot of time making sure that what was available on the market fully described the characteristics of seven different types of generic authenticators, and described how to determine where each mitigates risk. Biometrics was included in this process. Through this process, NIST formed security requirements for biometrics.

In this version of the 800-53, performance-matching was not enough to provide proof of identity. Adding presentation attack requirements plugs biometric presentation holes from a security perspective. There's also a companion framework being built that gives agencies and the private sector a methodology that can calculate how well their system is resistant to presentation attacks.

Within the identity proofing, authentication and federation sections, the trust level is 1, 2, or 3. If someone is approved at level 3, their next authentication can't be through an authentication level 1 proof because the binding between the two gets lost.

One would use the level to provide to the Federal Privacy Council that all privacy requirements were met. A lot of this privacy risk language from Ms. Levkovitz and Ms. Nadeau leads into the document. This is the first major document that was developed on a platform called “Pin Up,” which is used for open development. It’s extraordinarily popular worldwide for developers.

NIST put together a first working draft and published it for comment. It was called a “public preview,” because calling it a “public comment period” triggers certain requirements within agencies. It was online for about five months, with active updates every day.

This method afforded NIST the opportunity to respond to people directly. The issue number was tagged in the document, as individual "X" from the community that’s supplying a public comment. Contributors can click on it and go right to the document. It allows for other commenters to comment on each other’s comments.

The Board is aware that one of the things NIST prides itself on is its responsiveness to the private sector. NIST recognized this through the development of the cybersecurity framework. There is a certain amount of surprise, particularly for people who were relatively new to engaging with NIST. That responsiveness and the evidence that we’re listening and heeding the input, is much more immediate.

NIST also documented these items into a best practices document for OMB to use and promulgate.

Board Work and Consensus Decisions

Members of the Information Security and Privacy Advisory Board

The Chair and the Board took time to re-assess thoughts on discussions held Wednesday and Thursday.

The following topics were brought forward:

- Current S&T legislation and the role of NIST.
- NIST budgeting challenges - NIST is being asked to do more with less funding
- Privacy Engineering: the Board should encourage NIST's role in this area. NIST has a unique placement. It is pivotal to the privacy framework and accompanying activities. Privacy engineering work is a letter topic. Ms. Levin will provide language on the privacy portion and overall NIST role.
- Board thoughts on DDoS activities
- Market repository
- International activities
- Letter on the potential NIST audit capacity, touching on budget (letters to OMB, Director of NIST, with copies to Commerce and DHS). It should emphasize situational awareness, and recognition of the inherent challenge. The Board will attempt to offer considerations without getting involved in politics. Mr. Garcia will do the first draft. Whatever Congress does, it must be mindful of NIST's role, and how a change in NIST capacity would impact what has been its traditional role. The letter should stick to a policy perspective. It should tie language to the executive order.
- Next meeting topics for the Board: The Chair would like one day of the next meeting to be focused on one topic area. Suggesting federal modernization activity for the next meeting: Plans, federal cybersecurity, etc., acquisition and IT modernization related to federal cybersecurity, discussion on the shared services model, and an update on botnet activities, cyber incident repository, and encryption. Also:
    - Update from the IG community on their recent activities.
    - Ransomware – follow events until the meeting in the fall.
    - Baseline hygiene on ransomware announced yesterday (framework announced for future development).
    - Legislative update for the next meeting.
- NICE workforce sufficiency for the executive order: Closing the gap between supply and demand, and noting the circular poaching issue with trained cybersecurity staff (Possible letter) Mr. Boyer may have some advice on that topic from his task force. An RFI is coming out shortly with a 21-day comment period. There is the workshop in Chicago in August. Mr. Boyer will provide his report as a reference.
- Next meeting location with dates October18-20 (tentatively). Considering meeting at the NIST Boulder, CO office. Topics relevant to the NIST CO location (Boulder): 5G, first responders. Build an agenda relevant to that facility. Also considering DC locations to accommodate White House staffers for legislative updates.

Executive Order – NSS Implementation and Cybersecurity Strategy

Heather King, NSS

The Chair welcomed Ms. Heather King, NSS, to the meeting to update the Board on national security strategy implementation and cybersecurity strategy. Ms. King thanked the Board for the invitation to present and American University for hosting the Board meeting.

Cyber threats continue to grow. The cybersecurity community must act together to reverse the trend. The cybersecurity executive order signed in May is the Administration's initial action in this area. It sets in motion a series of near term actions to improve the nation's cybersecurity, and establishes a strong foundation for game changing improvements in the long-term. It builds on the last 12 years of work and sets activities in motion for the next 8-10 years. President Trump has said, "To truly make America safe, we have to make cybersecurity a major priority." With this executive order, the President acted to ensure the safety of the American people in cyberspace with initiatives in four priority areas.

The first initiative is securing federal networks. The second is working with industry to protect critical infrastructure. The third is strengthening America's deterrence posture and building international coalitions. A focus on America's cybersecurity workforce underpins all these initiatives.

The President knows how challenging it is to ensure that hundreds of departments and agencies are all protecting taxpayers' information and addressing the national security implications of missteps. There are three key efforts covered within the task of securing federal networks. The first is enterprise risk management. The President believes leadership and accountability go hand in hand. Consequently, he intends to hold his cabinet secretaries and agency directors accountable in their statutory responsibilities for managing the cyber-risk of their enterprises.

Cybersecurity is not simply the domain of IT managers or even chief information officers. Frankly, the responsibility falls with the most senior official at the perimeter agency. The risk management decisions made by agency heads can affect the risk to the Executive Branch as a whole and to national security. NSS views the current day-to-day, agency-by-agency approach as inadequate. Cybersecurity must be managed as an Executive Branch enterprise, so the President can evaluate risk as a whole for the government. This approach will be used for civilian agency systems as well as national security systems.

The second key effort is IT modernization. The federal government has a massive legacy IT problem evidenced in old and often outdated technology that is expensive to maintain. It's no secret that this legacy IT makes the federal workforce less productive than it could be if it had the same IT tools and capabilities that much of the private sector employs.

Legacy systems are also a fundamental barrier to cybersecurity. Legacy IT is extremely difficult to secure. The current approach to IT, which incentivizes agencies to spend disproportionately more on maintaining legacy IT than on purchasing updated, modern IT needs to be re-thought. It puts each agency in an untenable position of defending these antiquated networks in isolation from other agencies. In other words, IT modernization is fundamental to improving cybersecurity.

It is why the executive order includes a process for deliberate modernization of federal IT. It's a vital step toward improved cybersecurity that will enable the government to deploy and operate a more resilient IT infrastructure using fewer resources. The recent executive order to the American Technology Council taps the cybersecurity expertise of the Administration, departments, and agencies as it innovates.

The main focus of the Modernization Act is to re-orient federal IT policy toward shared services for things like internet connectivity, email, cloud, and other commoditized services. The Office of American Innovation is studying how the government could best modernize federal IT systems, retire outdated systems, and move to shared services to achieve cost efficiencies and significant operational improvements. It is not only good government, but good cybersecurity as well.

Consolidating service delivery in these areas will enable agencies to benefit from economies of scale

for both service delivery and cybersecurity protections. Consolidation will save taxpayer dollars and enable agencies to focus their cybersecurity workforce on more specialized IT operations that support the agencies' specific missions.

Cybersecurity and innovation are interlinked. Innovating and improving federal IT must be done with deliberate consideration of cybersecurity. At the same time, cybersecurity can't be the all-consuming focus that locks out innovation from the beginning. Considering cybersecurity at the beginning of the modernization process is better because of innovation for modernization, and re-design of the nation's digital services and federal IT.

The second key effort is critical infrastructure. The work with industry to strengthen critical infrastructure involves three important policy themes. The first theme is comprehensive support. Critical infrastructure provides and enables essential services that underpin society. This infrastructure is vulnerable to an ever-evolving range of threats. The electric grid is an example. Infrastructure serves as both a vital function of society and an essential aspect of national security. Prolonged power outages could have severe consequences for national defense, communications, water, waste water, healthcare, emergency management, and transportation and other critical services.

The government needs to be in a position to use its authority and capabilities to support cybersecurity risk management efforts of owners and operators of the nation's most critical infrastructure. There is a need for deeper and more collaborative partnerships to respond to the threat. In contrast to the federal government, the private sector owns the vast majority of the critical infrastructure that supplies electricity, communications, connectivity, water, and other vital services.

The President's EO sets in motion a series of actions to forge deeper, more collaborative relationships with owners and operators to support efforts to identify, detect, protect, respond, and recover from catastrophic cyber incidents. The government has great value to offer in critical infrastructure defense. That positioning requires a thorough and comprehensive understanding of what the federal government can offer by way of support. Through intensive engagement with infrastructure owners and operators, their needs can be better understood. Currently, gaps exist in government authorities and capabilities that require work with Congress to fill.

NSS needs to utilize our intelligence enterprise on advanced persistent threats in defense of the American people's way of life while assuring it protects sources and methods. Resilience must continue to improve. Determined adversaries will continue to infiltrate past defenses. Damage must be contained and critical capabilities rapidly restored. Resiliency means working through contingency plans. The best way to do this is through exercises and working together to be better prepared to respond, as is already done for natural disasters.

Validating voluntary approaches also plays into supporting and protecting critical infrastructure. The success of efforts to support critical infrastructure and cybersecurity depends on having willing partners because supporting infrastructure primarily involves voluntary collaboration. It's hoped the voluntary approach to managing cybersecurity risk is up to the task.

The third priority area centers on deterrents, international cooperation, and workforce development. The United States must ensure the internet remains open, interoperable, reliable, and globally secure to benefit the United States and the rest of the world.

The U.S. is committed to freedom, productivity, and stability in cyberspace, but other nations might not support these objectives. Options are being developed for deterring these adversaries and reducing the risk to the American people from malicious state-sponsored cyber-activity. The

internet has been a revolutionary driver of economic growth, as well as developing prosperity. There is a duty to protect and preserve it.

The U.S. deterrence posture is a critical element to achieving these objectives. Therefore, the President is calling on his national security team to recommend strategic options for deterring adversaries and reducing risk from cyber-threats.

The EO asks the State Department to draft an international engagement strategy for cybersecurity. The strategy will outline how the United States will take the initiative, working with partners and allies, to defend against and deter malicious actors in order to promote an international framework for cybersecurity and safeguard an open and secure Internet. It pushes back against forces seeking to fragment or wall off the internet, depriving its users of the unparalleled benefits of the free flow of information.

The final area involves workforce. Workforce development underpins all three priority efforts. It is indisputable that there's a global shortage of highly skilled cybersecurity professionals. People are the principle strategic capability that distinguishes one nation's cybersecurity capabilities from another's.

This EO launches the Administration's action in developing the workforce, ideally working with industry and its partners. It sets in motion a series of near-term actions to improve the nation's cybersecurity. The Board has heard the cybersecurity industry needs this talent just as the government needs this talent. To develop those talented individuals, cybersecurity education, training programs, and exploring best practices from countries around the world will be reviewed in order to evaluate the best means of identifying, developing, and retaining world-leading cybersecurity talent.

Cyber-threats are among the most serious national security dangers facing the nation. There are nation states, terrorists, and criminal hackers who are seeking to threaten critical infrastructure, damage computer systems, perpetrate fraud, and steal sensitive information. These actions threaten national security and the economy. Hardly a day goes by without another report of a cyber-incident affecting a U.S. business or consumer.

Meanwhile, America's adversaries are constantly probing U.S. government and critical infrastructure networks for vulnerabilities and taking action to exploit those vulnerabilities when found. The risk for cyber-incidents remains. Response to any significant incident that arises must be coordinated and timely.

DHS established the National Cyber Incident Response Plan, which was released in December, 2016, with incident response in mind. It draws from lessons learned from real-world incidents, policy and statutory updates. The plan includes the National Cybersecurity Protection Act of 2014 as well as Presidential Policy Directive 41 on U.S. cyber-incident coordination.

The various groups working on the executive order have made a great deal of progress. The progress is greatest when collaborating with industry. Government cannot succeed in this task without industry. Ms. King noted that she or someone else on her team would be happy to provide a further update in the fall. The Chair expressed interest in additional updates on modernization.

The Chair noted the information presented was very valuable. The Board intends to have a whole-day session delving into modernization during the next meeting in October. In closing, Ms. King thanked the Board.

Meeting Recessed

The meeting adjourned at 11:34 a.m., Eastern Time.

List of Attendees

Last Name	First Name	Affiliation	Role
Scholl	Matt	NIST	DFO / Presenter
Barr	Lisa	DHS	Presenter
Custodio	Rosalie	FBI	Presenter
Dodson	Donna	NIST	Presenter
Franklin	Josh	NIST	Presenter
Garasi	Paul	NIST	Presenter
Garcia	Mike	NIST	Presenter
King	Heather	NSS	Presenter
Larson	Derek	OMB	Presenter
Lefkivitz	Naomi	NIST	Presenter
Nadeau	Ellen	NIST	Presenter
Petersen	Rodney	NIST	Presenter
Regenscheid	Andrew	NIST	Presenter
Remaley	Evelyn	NTIA	Presenter
Romine	Chuck	NIST	Presenter
Ross	Ron	NIST	Presenter
Stine	Kevin	NIST	Presenter
Wright	William	Symantec	Presenter
Yaga	Dylan	NIST	Presenter
Drake	Robin	Exeter Government Services	Staff
Salisbury	Warren	Exeter Government Services	Staff
Barker	Curt	Dakota	Visitor
Nelson	Michael	Cloudflare	Visitor
Newton	Elaine	Oracle	Visitor
Shockey	Kelton	Cable Labs	Visitor
Starzak	Alissa	Cloudflare	Visitor

Last Name	First Name	Affiliation	Role
Carberry	Sean	Federal Computer Week	Visitor/Media
Geller	Eric	Politico	Visitor/Media
Morris	Joseph	NextGov	Visitor/Media
Weber	Rick	Inside Cybersecurity	Visitor/Media