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

August 7 and 8, 2019

1735 New York Ave. NW. Washington, D.C. 20006

Board Members	**Board Secretariat and NIST Staff**
Steve Lipner, SAFECode, Chair, ISPAB	Jeff Brewer, NIST, DFO
Christopher Boyer, AT&T	Evie Petrella, Exeter Government Services, LLC
Janine Pedersen, NSA	Andy McConnell, Exeter Government Services, LLC
Patricia Hatter, Palo Alto	
Marc Groman, Privacy Consulting	
Brett Baker, Nuclear Regulatory Commission, OIG	
Jeffrey Greene, Symantec	
Douglas Maughan, NSF	
Brian Gattoni, DHS	
Greg Garcia, Healthcare Sector Coordinating Council	

Wednesday, August 7, 2019

Welcome and Opening Remarks

Steve Lipner, Chair, ISPAB, Executive Director, SAFECode

The Chair welcomed everyone to the meeting at 9:02 a.m., Eastern Time. Board members were encouraged to be interactive and ask questions on subject matter people find difficult to express. An email went out last week regarding the Moonshot report. The chair would like to review the report during the discussion session in the afternoon and provide a consensus of thought on the record. Brian Gattoni, DHS, and Douglas Maughan, NSF are joining the Board as new members.

Welcome and ITL Update

Dr. Charles H. Romine, Director, Information Technology Laboratory, NIST

The Chair welcomed Dr. Charles H. Romine from the Information Technology Lab (ITL) at NIST (National Institute of Standards and Technology) to the meeting to update the Board on ITL. ITL's purpose is to cultivate trust in information technology and metrology. NIST is the U.S. national metrology institute, the best in the world. NIST guidance must be trustworthy and the process behind it must be trusted.

Maintaining proper balance of processes within the spectrum of fundamental and applied research while taking the result of the research and developing standards and best practices is critical. The challenge is that we are getting more and more recognized and the demands on our cybersecurity program are escalating every day.

There are four priority areas for future growth: quantum science, engineering biology, Artificial Intelligence (AI), and the Internet of Things (IoT).

Quantum science involves working with the fundamental physics lab to understand quantum states of matter. There are serious quantum implications to cryptography and cybersecurity. Engineering biology is a complement to the imagery and statistical analysis activities in ITL. ITL is the lead for NIST AI work. IoT is a booming area with many security requirements.

The President's budget went in on March 18, 2019 and passed the House on June 25, 2019. The Senate has not yet acted and there will be a reconciliation phase once the Senate does act. If the budget does not come through by October, ITL will not be able to function if there has not been some appropriation or continuum resolution. Seven-hundred and fifty-one million dollars have been ear marked for NIST and we are cautiously optimistic on approval.

The legislative bill, H.R. 1668: The IoT (Internet of Things) Cybersecurity Improvement Act of 2019, is currently sitting as pending legislation. Vendors of IoT devices are not where they need to be in terms of building in cybersecurity. In the federal space the Act requires a certain amount involved in the adoption of the IoT. There are no regulatory requirements outside of the federal space compelling people to act.

Dr. Romine testified in front of Congress five times within the calendar year. Most of the testimony was centered on or around cybersecurity, small business cybersecurity, IoT vulnerabilities, facial recognition technology, and election security.

To revisit some of the cybersecurity and privacy objectives outlined during the March ISPAB meeting:

- Develop and issue a privacy and risk management framework by fall, 2019.

- Develop and issue FIPS-140-3, detailing requirements for agencies to employ cryptography. The Cybersecurity Framework is a key portion of this area. It will go into effect in September.
- Completion of round two of the quantum cryptography algorithm selection process.
- Advancement of the Cybersecurity Framework and other cybersecurity, privacy and supply chain risk management practices through a series of workshops.

Work was completed to update NIST 800-53 but the document is still under rigorous review. The document is very large and the review process is very challenging to ensure all stakeholders are comfortable with its release. The final document is imminent.

In the area of cryptography, we have tried to follow the Visiting Committee on Advanced Technology (VCAT) recommendation. We are still pushing on lightweight cryptography which means cryptography for constrained environments. There is a strong push to automate the cryptographic validation protocol systems we have in place so that stakeholders get much more responsiveness.

The Privacy Framework is a complement to the Cybersecurity Framework. It was envisioned to be a voluntary enterprise risk management tool to help organizations manage individual's privacy risk. There has been a lot of activity and discussion on the Privacy Framework. We released a discussion draft in the spring with supplemental materials following in the summer. December 2019 is the targeted release date for the final version 1.0.

The core IoT cybersecurity capabilities were published a couple months ago and received universal approval on the content. A subsequent workshop is slated for next week to discuss the document. Because the IoT legislation that has already passed will likely be reconciled and sent to the President's desk, we will continue to be engaged in IoT.

The National Cybersecurity Center of Excellence (NCCoE) is now in its sixth year. New programs continue to be added. The NCCoE provides practice guides that can walk people through how to secure their IT environments. There are now 26 guides. The National Security Partnership (NSEP) program has expanded to 41 partners located at NCCoE from the original 12 partners. An AI security library has also been established.

NIST is the only agency called out within the Executive Order on Maintaining American Leadership in Artificial Intelligence outside of offices within the White House. The task is to develop a plan for federal engagement in the development of AI standards and tools. The due date was August 10, 2019. The draft was delivered on time and is under review. There are four key pillars that were called out in the plan:

1. Bolstering AI knowledge and coordination among federal agencies.
2. Support and expand public-private partnerships.

3. Plan, support and conduct research and evaluation.
4. Strategically engage with international partners.

NIST is privileged to co-chair the two AI intelligence subcommittees at the NSTIC. NIST is also a member of the AI select committee which is at the cabinet level with the Director of NIST, Walter Copan, sitting on that committee.

NIST initiated, in partnership with the Networking and Information Technology Research and Development (NITRD) program, a workshop on the overlap between AI and cybersecurity. The workshop report will come out in September or October.

NIST will celebrate fifty years of cybersecurity research in 2022. There will likely be a major cybersecurity symposium.

How do you view some of NISTs standards activity and how do you think the government is and is not coordinating or doing well? The U.S. is unique in that it is led by the private sector. The federal government does not control standards development for the purposes of U.S. standards. NIST provides technical expertise and support for the private sector in their engagement in standards development. That does not mean we cannot have leadership roles. NIST favors standards development which is open, transparent, participatory and, to the extent practical, free. Not all standards organizations can function with all free standards. Often Standards Development Organizations (SDOs) will charge for the standards they develop and we try to ensure that they charge as low a price as we can. The standards development in the U.S. and in the IoT space is, broadly speaking, coordinated by ANSI. We are involved with ISO organizations. Standards development is important but also a very arcane process. It requires judgement, political skills, people skills, persuasiveness, and compromise. There is anecdotal evidence that people cite about the potential erosion of U.S. influence in the international standards arena. NIST is still heavily involved in the security standards development for 4G and 5G.

Briefing on Current Threats

Mr. Steve Horvath, Telos
Mr. Brad Schulteis, Rackspace
Mr. Lance Dubsky, Iron Mountain

The Chair welcomed Steve Horvath, Brad Schulteis and Lance Dubsky to the meeting to brief the Board on current threats. Steve is in risk management but is exposed to both mitigations and threats on a minute by minute basis at Telos. Brad Schulites is the Director of Government Solutions at Rackspace. Lance Dubsky is VP of IT Security Technology. His current position is one that buys technology and works on FFIC compliance.

The reality is that threats evolve. The tactics change but the leverage is always the lowest common denominator. The insider threat plays one of the biggest roles and the administrator no longer has the ability to take care of everything on their own. All threats are now taking place in the face of cloud computing. Organizations are operating in a new infrastructure. Most organizations believe their information is safer on the cloud. The cloud can be more secure but it involves a lot more complexity in securing it. The threat landscape continues to hit the top three things: 1.) Social and spear phishing, 2.) Insider threat with sophisticated understanding of the architecture of configurations of the network, and 3.) Spending money in the wrong places on products. Organizations need to start investing in cybersecurity talent.

The skills gap is the biggest threat and only widening. There are people who understand information security, network security and traditional security paradigms and there are those who understand the cloud. There is virtually no communication between the two groups. No one is speaking the same language and one cannot secure an environment if all of the players speak different languages. We are hiring people out of college who have never practiced in their life, do not know what enterprise IT looks like on the inside, and are charged with securing the entire enterprise. Very few people in the cybersecurity talent pool understand network security concepts. There are thousands of threat actors all over the world. Each threat actor uses a different toolset from the beginning of intrusion to the end. Each threat actor group requires a lot of expertise.

The challenge is convergence. Convergence on the IT side making all the different pieces of IT work well together as a partnership is one thing. One of the challenges for Lance Dubsky at Iron Mountain was to break down the walls of the various IT areas and people to ensure that the partnership worked and people talked. Additionally, he is tasked to make sure they are hiring the right talent as well as reviewing all of the toolsets they have to make sure they are getting value out of what they are paying for. It is hard to hire the right expertise without spending the money. We are spending less than five to ten percent on education and training, as far as cybersecurity, than we really should be.

Do you see specific traits in organizations that are doing a good job? An organization that identifies malicious content within a 24-hour window, quarantines, and does some forensic analysis and then brings back operations in 18-36 hours is good. A major concern is the lack of network visibility in a lot of federal civilian agencies or even the U.S. intelligence community. Tracking down every device that's connected to the network in some way is extremely challenging. It's one of the things that the cloud offers as a tremendous benefit.

How do we make the most of the inexperienced talent coming out as college graduates? We need to get to a point where the developers are the security experts. Everyone in an organization needs to understand their individual responsibility in securing an

organization. Host the right tools in the developer environment and make it common practice for developers to use them and self-police. Hold senior people accountable to hold their people accountable for developing reasonably secure code so that when it does get to the risk organization, you can secure it better and the environment you're putting it in is secure. A secure environment is difficult particularly in light of technical debt. To replace all of the servers and applications of a publicly traded company is a tremendous cost. The CIOs and CTOs in charge of IT infrastructure need to figure out ways to ensure their technical debt is reasonable. Every organization should know its critical systems. Once you know what the critical systems are and what needs to be protected most, you can apply the tools, the manpower, the patching, and the priority to those things that reduce risk to the organization.

Supply chain is getting more attention now than it ever has from a cybersecurity perspective and it's one of the scariest areas most people don't know about. It's not just supply chain of material goods but supply chain from an acquisition perspective. It's not simply about the server and the infrastructure.

There's a dramatic drive to go to pipeline development where you have DevOps. Security professionals are arguing over whether to be SecDevOps, DevSecOps, or SecOpsDev. The arguments about terms are comical when in reality that methodology of development greatly increases cybersecurity technical debt because there is a dramatic focus on capability and the drive to release code. The rush toward capability sometimes sacrifices security.

What is it going to take to make it so security is no longer a bolt-on but rather a part of an integrated, holistic look at what we are doing? It is important from a legal and contracts perspective we're understanding the financial risk we are accepting. It is necessary to qualify the risk. There is an important convergence that's happening right now from a policy perspective. One of the biggest pieces, even for federal agencies, is the NIST 800-37 Revision 2. Everyone is doing compliance management but no one is doing risk management. We focus so much on weakness and vulnerability but we're not looking at the issues from a cost perspective. There is a lot to go into the equation to decide on investment from a cybersecurity perspective.

The challenge is the most common denominator which is almost always people. There needs to be a more blended approach to allowing people to work together to get to common problems because the only way to combat some of the threats is for IT and IP security to work together. There have to be partnerships. The problem is that in a majority of private sector organizations, they look so much at service delivery and how many tickets are being closed. This mentality does not allow for strategic thinking.

Brief on NIST IOT Security Project

Ms. Katerina Megas, NIST

The Chair welcomed Katerina Megas of NIST to brief the Board on the IoT Security Project. The NIST Cybersecurity for IoT Program coordinates across NIST on IoT cybersecurity to include research and reports, special publications and applied sciences. Much of the current discussion around IoT involves the work on the baseline and 8228 that was recently published. IoT is not one size fits all. There is an external facing website with an inventory of all the work being kept.

There are five cybersecurity for IoT Program principles that were created following a conference that included private industry, externals, and academia to discuss where they saw the future issues with IoT cybersecurity. The principles are 1.) Risk-Based Understanding, 2.) Ecosystem of Things, 3.) Outcome-Based Approach, 4.) No One Size Fits All and 5.) Stakeholder Engagement.

The NISTIR 8228 draft was put out in November 2018. The majority of comments pointed to not reinventing the wheel and evaluating how IoT fits into the context of existing work. NIST 8228 final version was published on July 31, 2019 and addresses security and privacy. While writing NISTIR 8228, multiple existing efforts, domestic and international, were analyzed and 15 common capabilities were identified and included in Appendix A. Industry feedback concerning the work within the Appendix was very enthusiastic. There was interest in continued engagement on Appendix A, to develop a cybersecurity and privacy baseline for IoT.

While looking at the methods and methodology used to do analysis on the Appendix we were asked if the work of the Appendix would be turned into its own deliverable? There was no existing body to use to derive and frame the analysis of the work being done. There was the ongoing work on the privacy framework that was starting off at NIST so it was decided to sequence that work. Security should be the focus as it is a far more understood area with existing work to draw on for analysis. On privacy, the prevailing thought was that conversation should be allowed to evolve. The Privacy Framework could be utilized to derive and look at whether a baseline for privacy devices makes sense.

The Botnet Report on enhancing the resilience of the internet against botnets and other automated distributed threats was delivered to the president in May of 2017. In the report, IoT was identified as an area of focus for addressing the issue related to botnets. This was flushed out in what became known as the Botnet Roadmap. The Roadmap charts a path forward and sets a series of tasks and deadlines laid out in the president's report. The Roadmap is a plan for coordinating efforts among government, civil society, technologists,

academics, and industry sectors to develop a comprehensive strategy for fighting these threats.

The Roadmap's IoT line of effort lays out an action plan to establish a robust market for trustworthy devices. The broader picture of the Botnet Roadmap calls for a core baseline, sector specific baselines, transparency schemes, and conformity assessment. Currently the focus of work is on the core security capability baseline.

After feedback was received from the public comment period on the Appendix it was decided that the best way forward would be to come up with criteria about what makes a good capability and what makes a bad capability. Three assessment candidates were created: 1.) Utility, 2.) Verifiability and 3.) Feasibility.

Based on the criteria, eight baseline candidates were then created. NIST published an essay inviting stakeholder feedback to inform development of the Core IoT Baseline in February 2019. The intent was to engage with stakeholders through meetings and webinars. The commentary was heavily used to inform the first draft of the Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers, NISTIR 8259 (Draft). Some of the draft essay feedback included points on the following:

- Elaboration of capabilities and informative references to further inform the meaning of the capabilities
- Include optional capabilities for consideration
- Other considerations for manufactures of devices beyond the baseline items
- Considerations in the baseline for device constraints when adaption may be appropriate

There are four general areas in the way the work is presented based on the feedback. The first is the 'Cybersecurity Feature Identification' which helps walk an organization through things to consider while designing a device. Next, the 'Cybersecurity Feature Implementation' talks about baseline items and understanding architectural considerations. Third is 'Cybersecurity Communication' which is where all the other topics that are more organizational policy discussions are presented. What are the cybersecurity features? Being transparent about what is on the device. What are the sources of the IoT device software on the device? Much of this maps to the discussion being held internationally as well. The final area is the "Secure Development Practices for IoT Devices'.

The focus is communicating that the core baseline is a starting point. There was a lot of concern that people see the baseline as good enough so the messaging has shifted to show that it is only a starting point. The eight baseline candidates have now become six:

1.) Device Identification - the IoT device can be uniquely identified logically and physically

2.) Device Configuration – The IoT device's software and firmware configuration can be changed, and such changes can be performed by authorized entities only.

3.) Data Protection – The IoT device can protect the data it stores and transmits from unauthorized access and modification.

4.) Logical Access to Interfaces – The IoT device can limit logical access to its local and network interfaces to authorized entities only.

5.) Software and Firmware Update - The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.

6.) Cybersecurity Event Logging – The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.

It made more sense to not talk about the core capabilities as separate because doing one implied you had to do the others. All of the capabilities can be mapped to 800-53, as well as the Cybersecurity Framework.

In order to not get too prescriptive, but allowing for room to describe what we mean by core capability, the concept of 'Key Elements' was created for each baseline candidate.

The draft will be out for a sixty-day comment period to close on September 30, 2019. A workshop will have been held at NIST on August 13, 2019 which will also be webcast. Once the comment period closes a decision will be made as to whether a final draft can be created or whether a second round is necessary.

Based on the feedback and all of the work done with our partners, there is a desire to see a new natural standard develop in this area around devices. A delegation to the International Conference on Recent Innovation in Computing (ICRIC) put in a proposal for an IoT baseline standard. It's been through a single study period at the most recent meeting in Tel Aviv. It talks about the responsibility of the customer, the network providers, the different infrastructure players, and the device manufactures. Generally, the consensus that having a separate document focusing on the manufacturing of the device would be useful. The plan is to provide the public draft as contribution. We're hoping to work parallel efforts in the U.S.

There will probably be a baseline that will address categories of consumer devices as well as baselines that will be defined for different areas of IoT. For the federal government our responsibility is under FISMA. Part of that is providing guidance to federal agencies that are procuring devices to help understand the minimum security those devices should provide as you bring them into your environment and to look at security controls under 800-53 and other special publications. A workshop will be planned to focus on that. The core baseline

discussion will need to be sufficiently underway before considering the impacts for the federal government. We hope to have a core baseline completed by the end of the year.

How would 8228 or 8259 relate to the emerging IoT Security Act? Would that language be made by the federal profile you referred to or some potential manager or requirements associated with that? It would be based on much of this work. It provides a lot of formality to the work that we are intending to do. There are two parts to the bill as well. The part of the bill that focuses on what we refer to as the core baseline, and the federal profile of the baseline. The second part talks about the vulnerability disclosure coordination. The first part of the bill is very relevant to this work.

Where are the testing organizations that make sure all of these devices get tested? Is that in the picture anywhere where the underwriters of that are equivalent to an IoT? That is not currently in the scope of the baseline. Part of the government profile will be to elaborate on those.

From an industry perspective, one of the biggest issues is ensuring that if a device gets certified it can get certified all over the world in different ways. There is a need to harmonize the standards. Perfect harmony of standards is unlikely but we can work to ensure interoperability so that if you satisfy a baseline in the U.S. you can get credit for that in another country.

Update on NIST Privacy Program

Ms. Naomi Lefkovitz, NIST
Ms. Ellen Nadeau, NIST
Ms. Kaitlin Boeckl, NIST

The Chair welcomed Naomi Lefkovitz, Ellen Nadeau and Kaitlin Boeckl of NIST to brief the Board on the NIST Privacy Program. The Privacy Framework development started during a workshop in Austin, Texas last fall. The RFI on the framework closed in January and received 80 responses. An outline was developed based on the responses and was released in late February. A first draft was issued in April followed by a workshop in Atlanta, Georgia.

The feedback from the workshop in Georgia was used to create supplemental material. Another workshop was held in Boise, Idaho in July. The Boise workshop discussion was centered on the supplemental materials. A second draft is being completed to release at the end of summer with a plan to release version 1.0 by the end of the year. When the RFI was released, a set of attributes was introduced. A tool will be developed to reflect those attributes.

The supplemental materials released prior to the Boise workshop were used to guide the discussion. The desire was to discuss, in depth, the purpose of the framework and how it is being communicated as well as the value and scope. Additionally, discussion was centered on the approach taken to develop a risk-based tool and whether we're achieving the development of something that's flexible for organizations to use. The accessibility of the framework and how effective it is in bridging the gap in the privacy space was a focus as well. There was also focus on the development of a roadmap. Hypothetical use case profiles were created to see how the framework could be used by different parts of an organization. There were a lot of questions about how the profiles of the framework could be developed by organizations. Examples were provided on how the framework could be used in practice.

The draft executive summary was more robust in an effort to obtain great feedback. A request for clarifying individual risk versus organizational risk as well as the relationship between cybersecurity and privacy risk were areas upon which a lot of feedback was received. It was important to have a compelling values statement in the summary. There was a request for plain language through and through so that it could be used by executives. The values statement focused on making ethical decisions when designing or deploying products and services which received some mixed feedback. There was a desire for more positive language around building trust and transparency with consumers to highlight the competitive advantage of using a tool like the Privacy Framework. Future-proofing is also important to organizations which could be a key component for a values statement.

Following came the proposal of two new cores: Integrated Core and Separated Core. The differences are in no way saying that data security is not an important part of privacy. The question was what's the alignment with the Cybersecurity Framework? The lens was shifted slightly to think about it from the standpoint of data and security safeguards to help protect individuals' privacy. The cores allow for flexible implementation. An organization may not need to achieve every outcome or activity reflected in the cores nor are they obligated to achieve an outcome in its entirety. Organizations may need to consider multiple outcomes in combination to appropriately manage privacy risk.

A number of topics were proposed for building out a roadmap to see if people liked the ideas or whether they thought there were areas of priority to work on. The topics include: mechanisms to provide confidence, emerging technologies, privacy risk assessment, privacy workforce, re-identification risk, and technical standards.

The NIST Privacy Engineering Collaboration Space was conceived in the space where people could share tools, solutions, and use cases, and work together to improve those tools and share ideas about what implementations work well as well as what gaps are out

there. Positive feedback was received from private and public sectors as well as advocacy and academia. The collaboration space launched last March. The space involves a growing community of interest where contributions have been received from public and private sector, academia, and advocacy groups. The site is run through GitHub. Contributions cannot be promotion based nor paid-for products. Vendors can contribute and receive feedback but they cannot place their tools into the site for payment. There are three general buckets of what users can share on the space: tools, use cases and feedback. Two of the future focus areas for the collaboration space are de-identification and privacy risk assessment. Both of these future topics appear in the proposed roadmap topic areas. The collaboration space is a place to drive discussions of what belongs in the roadmap for the Privacy Framework. The space is also a staging area for the development of more tools, solutions, etc. to advance the use of domains and provide that toolset organizations need to meet various outcomes that are provided in the Privacy Framework's core.

Brief on the Executive Order on Americas Cybersecurity Workforce

Mr. Rodney Petersen, NICE Director, NIST

The Chair welcomed Rodney Petersen of NIST to brief the Board on the Executive Order on Americas Cybersecurity Workforce. The NICE program is authorized under the Cybersecurity Enhancement Act of 2014. Under the act, the NICE Director is required to submit a strategic plan every five years. On Monday of next week, a workshop will be held at the National Cybersecurity Center of Excellence (NCCoE) to evaluate what the NICE Program has accomplished over the last three years with specific focus on the goals and objectives of the 2016 NICE Strategic Plan: Accelerate Learning and Skills Development, Nurture a Diverse Learning Community and Guide Career Development and Workforce Planning. Mr. Petersen would like to re-engage with the Board in a year to receive input regarding the creation of the next NICE Strategic Plan.

A provision within the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructures (May 2017) relates to supporting the growth and sustainment of the workforce skilled in cybersecurity. It also asked Commerce through NICE and NIST, as well as the Department of Homeland Security, to assess the sufficiency of efforts to train the American cybersecurity workforce and create findings and recommendations.

In June of 2017 an Executive Order Expanding Apprenticeships in America was issued. This order is an effort to reform America's education systems and workforce development programs. The Secretary of Labor and the Secretary of Commerce were asked to promote the development of apprenticeship programs by third parties.

In July of 2018 an Executive Order Establishing the President's National Council for the American Worker was issued. The goal is to develop a national workforce strategy. Mr. Petersen is working with the Office of the Secretary on the launch of the national strategy of the workforce sometime next year. NICE's work in cybersecurity and workforce development is key to this.

The National Cyber Strategy from September 2018 is organized in four pillars. The second pillar is promoting American prosperity as an objective to develop a superior cybersecurity workforce. The actions include building and sustaining the talent pipeline, fixing and reskilling, enhancing the federal cybersecurity workforce, and using executive authority to highlight and reward talents. Reskilling, and reflecting back on the NICE Strategic Goal of Accelerating and Learning, is a good idea because it takes a population of people in their 30s, 40s, 50s, or veterans, or anyone unhappy in their careers, and lets them change careers into cybersecurity.

The America's Cybersecurity Workforce Executive Order of May 2019 has a few policy statements worth highlighting. The first is that a cybersecurity workforce is a strategic asset that protects the American people, the homeland, and the American way of life. The second is the need to enhance workforce mobility. NICE and NIST come heavily into play with respect to these two points. The NICE Cybersecurity Workforce Framework is mentioned nine times in the order. The NICE framework and the efforts of our community help to facilitate that mobility. The framework eases the ability for employers to hire people by standardizing their position descriptions within a company. There is also a great benefit to job seekers. The framework facilitates movement across and within companies, sectors and the government. Another statement is with regard to rotational programs. From both a development and retention standpoint it is a positive action to encourage employees to rotate within or across agencies within the government to develop new skills and competencies. Mr. Petersen pointed to the article 'Wouldn't It Be NICE to Promote a More Mobile Cybersecurity Workforce?'.

There are two main sections of the Executive Order. One is on Strengthening the Federal Cybersecurity Workforce and the second is on Strengthening the Nation's Cybersecurity Workforce. As noted earlier the NICE Framework is mentioned nine times in the America's Cybersecurity Workforce Executive Order. Briefly, four of the references include:

- The Cybersecurity Rotational Assignment Program: the use of the NICE Framework as the basis for cybersecurity skill requirements for program participants.
- Federal Contracts for Information Technology and Cybersecurity Services: Incorporate the NICE Framework lexicon and taxonomy into workforce knowledge

and skill requirements used in contracts for information technology and cybersecurity services.

- Presidents Cup Annual Cybersecurity Competition: the parameters for the competitions, including the development of multiple individual and team events that test cybersecurity skills related to the NICE Framework and other relevant skills, as appropriate.
- Voluntary integration of the NICE Framework into existing education, training, and workforce development.

Another NICE Framework reference is within 'Contracts for IT Cybersecurity Services use NICE Framework' which is being led by the General Services Agency (GSA). The GSA in consultation with the Director of OMB, shall: 1.) Incorporate the NICE Framework lexicon and taxonomy into workforce knowledge and skill requirements used in contracts for information technology and cybersecurity services; 2.) Ensure that contracts for information technology and cybersecurity services include reporting requirements that will enable agencies to evaluate whether personnel have the necessary knowledge and skills to perform the tasks specified in the contract, consistent with the NICE Framework; and 3.) Provide a report to the President, within 1 year of the date of this order that describes how the NICE Framework has been incorporated into contracts for information technology and cybersecurity services, evaluates the effectiveness of this approach in improving services provided to the U.S. Government, and makes recommendations to increase the effective use of the NICE Framework by U.S. Government contractors.

Within the order, the List of Cybersecurity Aptitude Assessments states that the Director of OPM, in consultation with the Secretary of Commerce, the Secretary of Homeland Security, and the heads of other agencies as appropriate, shall within 180 days; 1.) identify a list of cybersecurity aptitude assessments for agencies to use in identifying current employees, with the potential to acquire cybersecurity skills, for placement in reskilling programs to perform cybersecurity work and 2.) Agencies shall incorporate one or more of these assessments into their personnel development programs.

The report to the president following the 2017 Executive Order on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce included four imperatives with multiple recommendations and actions items. The May 2019 order gives permission to move forward with the recommendations. Mr. Petersen pointed to the last priority consideration which is to establish and use measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

NICE will continue to perform it's work in a consultative process in partnership with academia, the private sector and nonprofit organizations. There is the NICE interagency coordinating council in addition to the public working groups established through NICE.

Additionally, there is constant outreach performed by both NICE and NIST. The consultative process also takes place through requests for information and other mechanisms to ensure NICE is getting the most input for future directions for implementing this report.

The Executive Order also includes the encouragement of voluntary integration of the NICE Framework into existing education, training, and workforce development efforts. NICE has been doing this for a long time and will continue with this effort. Additionally, NICE is requested to provide an annual update to the President on effective uses of the NICE Framework by the nonfederal entities and make recommendations for improving it.

NIST Cybersecurity Update

Mr. Matthew Scholl. NIST
Mr. Kevin Stine

The Chair welcomed Matthew Scholl and Kevin Stine of NIST to brief the Board on the NIST Cybersecurity update.

When Executive Order 13800 (May 2017) was issued it doubled down on Enterprise Risk Management (ERM) and stated agency heads would be held accountable for managing cybersecurity risk as part of broader Enterprise Risk Management activities. These activities would be alongside and aligned with strategic risks, operational risks, budgetary planning processes, etc. The Executive Order went on to state that agencies will use the Cybersecurity Framework. There has been a lot of success with the Cybersecurity Framework over the last few years, increasingly in the federal space as well as in industry and internationally. The framework is a useful tool for helping to elevate cybersecurity risk management and discussion into the broader ERM space. There are a lot of great opportunities to bring these different frameworks and approaches, structures and policies together in meaningful ways to help align some of the activities. These are focus areas with respect to the Cybersecurity Framework umbrella within the Enterprise Risk office at NIST. How can the taxonomy that the Cybersecurity Framework provides be more aligned to the language that the broader ERM folks are speaking today?

There continues to be broad adoption of the Cybersecurity Framework which is signaled by the large number of derivative resources produced by industry or other government agencies on how they are using the framework. Some are in the form of cases while others are through mappings. As resources become available that are reasonably correct they are then catalogued. There continues to be tremendous uptake of the Cybersecurity Framework internationally as well the principles that the framework describes. NIST is engaging in international standards and leading a lot of the work on ISO27101.

When NIST initially introduced the Cybersecurity Framework, there was an informative reference column in the actual framework core where there was a handful of highly utilized and well-planned standards as guidelines. They have recently launched an online informative reference, which is a methodology, a process, and ultimately, a repository that will help organizations do the mappings. It provides them with a consistent and machine-readable way to close the gap between the highest order polices, rules, regulations, and principles all the way down through the framework including the controls and specific configuration settings of hardware and software.

The work of the Privacy Framework, the NICE Cybersecurity Framework, as well as the NIST Cybersecurity Framework, are all seeking to provide a common language or taxonomy for a specific discipline in cybersecurity, privacy and the workforce. All of these frameworks have a strong relationship but have their specific purpose. NIST is working internally to clearly establish the relationships between the three frameworks for the benefit of the user community.

Twenty-six (26) round-two submissions remain in the quantum algorithm competition. The competition started with sixty-nine 69 initial submissions to replace both a public encryption as well as a key exchange mechanism that needs to be updated. Seventeen (17) of the twenty-six are to replace the common key encryption piece and nine (9) are candidates to replace the key exchange mechanism. The last twenty-six (26) will be presented at the U.S. Encryption Technology Conference on August 22, 2019. After the conference, an even smaller set of the twenty-six will be selected as candidates for standardization.

Industry is pushing hard on the new standard but it will take time until it is completed. In the interim, NIST will put out some spreadsheet guidance on what both industry and government should be doing. The spreadsheet will ask users to identify where the vulnerable crypto is and what it is and is not protecting. Finally, it will ask users to create a prioritized list so when the standards are done users are set to go.

When the work comes to completion between the 2020 to 2022 timeframe, it will not be adequate to just publish a federal information processing standard and an associated special publication. It will need to be carried through into a standards file. NIST will be working closely with both national and international partners to ensure that the new algorithms are easy to adopt.

NIST received fifty-six (56) lightweight cryptography submissions. A workshop will be held on November 4, 2019 to hold an initial and aggressive down selection. Unlike quantum, NIST is looking at the use cases for the lightweight to be used in a traditional computing environment. Rather than having an internal government standard they will now point to

an ISO standard, NIST is looking to federate more with international partners and accept more testing evidence using the ISO standards. The alignment will allow NIST to accept their test evidence and others to accept NIST validation. The team has been building out the ability to automate much of the testing, especially the algorithms. The Automated Crypto Validation Program (ACVP) is something they are investing heavily in. Therefore, the trust extension and ability to have assurance across labs is ready.

Work continues around block chain. NIST is working with other agencies in the federal government who have done their own R&D that NIST would like to learn from. Additional interest is on the metrics, measurements and security capability that block chains provide and how those security properties change the block chain scope. Research continues into format preserving encryption and extending the algorithm suites, like organization and optimization.

Since the last ISPAB meeting in March, the Office of Management and Budget (OMB) issued their updated federal Identity and Credential Access Management (ICAM) policy. Many agencies are called out in the update and there are a lot of interagency relationships between the requirements in the update. Mr. Stine sees the activities NIST are responsible for addressing in three big buckets. One is additional resources to help agencies with their implementation of 800-63 across the entire body of that work. Second is with respect to developing and issuing guidance to promote deployment of different types of technologies, including open source technologies to help address digital identity needs. The third is on developing criteria for accrediting products and services that meet different assurance levels outlined in 800-63.

The PIV standard will be updated. NIST will look at extending some of the capabilities on CAR as well as ensuring there is a similar level of assurance as other PIV equivalencies. NIST is also looking at the technical capabilities to extend how PIV can be used. A lesson learned after the last couple of iterations is that PIV, as used as a second factor, is not good for many new technologies. NIST is looking at how they can use some of the strong identity vetting of the cryptography in a chip and still be able to extend it to important devices that require strong authentication.

The National Vulnerability Database (NVD), which is the repository of vulnerabilities, has been migrated into an AWS instance and is now mirrored globally. In theory, if there is some kind of disruption, we should be able to continue service. It is experiencing growth at a rate that required them to move into infrastructures that allows them to manage the growth but also extend it into new areas outside of just IT.

On the research side, NIST has been reviewing threat and breach data made available through public sites. They have been scraping and normalizing some of the data and then

overlaying it with some of the vulnerability work into NIST's data visualization tools. This is an emerging research area where they are taking a deeper analysis, not just in vulnerability, but where the least reported threat actions are going on.

The National Cybersecurity Center of Excellence (NCCoE) is a collaborative center of industry and government working together to address business pressing cybersecurity challenges. Partners and other collaborators come to the center to work on daily projects, providing strategic insights and thought leadership in the cybersecurity and technology spaces more broadly. In some cases, partners provide products, services, staff, and engineering time to work with the center to produce example solutions and help create documents. The IoT work, privacy work and the workforce activities all inform and influence the activities of the center.

There has been a lot of attention on the network infrastructure program at the NCCoE. IPv6 is an example of a project they are scoping out zero-trust architecture; which is spearheaded as part of the Federal CIO Council. The Federal CIO Council has expressed and declared an interest in understanding moving more towards a zero-trust architecture. The work at the center through the CIO Council was to help define when we say zero-trust, what do we mean? What are the principles, practices and capabilities? Then, as the project continues to evolve, milling out some example solutions for that.

There has been a lot of work in the IoT program and space. The IoT features baseline was one of the deliverables on the roadmap to the action plan in the BotNet Report which is informing the work at the center as well. Some other activities that fall into the broader IoT bucket is their work on IoT EDOS protections, taking advantage of the MUD protocol out of IoT manufacturing research description and other approaches. The Center is also looking at home IoT devices and understanding the capabilities that those have when they are procured as well as their configuration capabilities. Finally, the center is looking at IoT Sensor Networks.

Data Security is another area of work at the NCCoE. There are two projects in data integrity and two in data confidentiality. Both project areas are broken down by framework functions. All of the projects are in different lifecycle phases or phases of implementation. The projects all include publicly available resources that are either drafts of documents, builds or the project descriptions.

An AI Lab has been set up at the NCCoE focused on securing AI and looking at the use of AI to help benefit security. Sector work continues in energy with some new projects in that area. There is a project focused on privileged access management in financial services. In healthcare, there is work on picture archival communication systems as well as tele talk and remote patient monitoring. Finally, there is continued work on IT. NIST is continuing to

discuss with industry the role NIST can play at the center to understand the security capabilities and prove some of the security capabilities that one can benefit from a 5G environment.

NIST is doing research on security capabilities and on potential issues in security and privacy, in conjunction with the rapid commercialization of low Earth orbit, with a particular focus on what the cybersecurity practices should be. NIST is very interested in time as an aspect of security and how we can potentially provision in the concept of secure or verifiable time for use in everything from ensuring synchronization and 5G communications, automation of vehicle fleets, micro transactions, etc. Thus, work is being done with the Time and Frequency Division to ensure the ability to have the fidelity of measurement in time. Work is being done in partnership with other agencies, like the Department of Transportation, and National Highway Traffic Safety Administration (NHTSA), who will be deploying electric vehicle chargers around the nation which involves calibration.

NIST is very interested in improving cybersecurity development in tools that are being utilized. NIST believes there are opportunities in dev ops when the workflow is considered and how it occurs in some of the virtualized containers that are created to pass workflow down. It is possible to enforce security policies through a less onerous way on the developer and more automated in the tool sets that enforce the process and policy that the developers are working on.

Review of Wednesday Briefings

It was the decision of the Board to discuss the Moonshot report in lieu of the day's briefings. The report was discussed at length but tabled until the following day for further thought.

Public Comments

No requests for public comment were received.

Meeting Recessed

The meeting recessed at 4:51 p.m., Eastern Time.

Thursday, August 8, 2019

The Chair opened the meeting at 9:03 a.m., Eastern Time.

Brief on Federal Contractor Security and 800-171A and B and High Value Asset Protection

Ms. Vicky Pillitteri, NIST
Mr. Alan McClelland, DHS

The Chair welcomed Vicky Pillitteri of NIST and Alan McClelland of DHS to brief the Board on the Federal Contractor Security and 800-171A and B and High Value Asset Protection.

The purpose of NIST Special Publication 800-171 is to provide federal agencies a set of recommended security requirements for protecting the confidentiality of controlled and classified information in non-federal systems and organizations. The most recent revision was published in December 2016. The genesis of the publication began in 2007. The Department of Defense (DoD) received a presidential memo to safeguard DoD data in non-DoD systems in the development of the CUI program. This is the genesis of DFARs (Defense Federal Acquisition Regulation). In 2010, the DoD published notice of the proposed rule-making for DFARs and EO13556. The Control of Unclassified Information was issued. The National Archives and Records Administration (NARA) was designated the CUI Executive agent. In 2011, the DoD published the draft-proposed DFARs Rule which included selecting 850 controls. In 2012, DFARS were re-scoped to protect control of unclassified Controlled technical Information (CTI). In 2013, NARA objected to the DFARs interagency coordination and the safeguarding of unclassified CTI DFARS was published. At this time, NARA, NIST and DoD began work on what would become Special Publication 800-171. Two years later the initial Special Publication 171 was released and the DFARS rule updated and advised to site 171 to apply to DoD's CUI.

NARA and NIST had objected to the DFARs use of selected subsets of Special Publication 800-53 Controls. Essentially, the original draft asserted that the full moderate impact baseline was required for protection of CUI. The 800-53 was originally developed with a focus on federal information systems. With the issuance of DFARS there was no expectation for contractors to go in and build new systems. The DoD wanted to leverage the systems in place but also make sure the appropriate security measures were in place. Another reason the 800-53 moderate baseline was not a good fit for contractor systems was many of the baseline controls were unnecessary, which is why in Special Publication 800-171, the focus is on the confidentiality of CUI.

The solution to the problems was through the development of 800-171. The security requirements were based on FIPS 200. They were performance based to ensure they were adaptable to non-federal systems. The focus was on the essentials of providing protection of confidentiality for CUI. There are 111 security requirements in 800-171. The controls not related to CUI were removed. 800-171 offers a pre-tailored and uniform set of requirements for protecting CUI. This allows non-federal organizations to consistently implement safeguards for protection of CUI while allowing contractors to implement alternative but equally effective security measures to satisfy CUI.

In 2018, NIST Special Publication 800-171A, Assessing Security Requirements for Controlled Unclassified Information, was published. The purpose of 800-171A is to provide federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirement in NIST Special Publication 800-171. The amount of rigor is up to the organization that's doing the assessment. A common feedback point from stakeholders was that they wanted more guidance to 800-171A. When 800-171A was issued it also included draft items on supplemental guidance to further explain and give more context to each security requirement.

The initial public draft of NIST Special Publication 800-171B, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirement for Critical Programs and High Value Assets, was published in June 2019. The comment period closed last Friday. The purpose of 800-171B is for enhanced security requirements for protecting CUI in nonfederal systems and organizations where information runs a higher than usual risk of exposure (e.g., part of a critical program or high value asset (HVA)). The enhanced security requirements; are implemented in addition to the basic and derived requirements in NIST SP 800-171. They apply to components of nonfederal systems that process, store, or transmit CUI, provide protection for such components when the designed CUI is contained in a critical program or HVA and, are only applicable for a nonfederal system or organization when mandated by a federal agency in a contract, grant or other agreement. There were 34 additional enhanced security requirements added to 800-171B. They cover all of the same families as included in 171. Half of the families have additional requirements.

In 2017, the Department of Homeland Security (DHS) High Value Assets (HVA) program created a document called The HVA Control Overlay. The HVA Control Overlay was based off risks that were mined and consolidated as part of their assessments, and identified controls that the agency felt were very important for agencies to apply. There are 93 controls within the HVA Control Overlay, that are above and beyond, or highly recommended. DHS also performs a number of assessments against these HVAs. The assessments include: The Security Architecture Review (SAR), a Risk and Vulnerability Assessment (RVA) and a Federal Incident Response Evaluation Assessment (FIRE).

A 45-day comment period was held for both Draft SP 800-171 Rev 2, as well as, Draft SP 800-171B. Most of the changes to Draft SP 800-171, Rev 2 were cosmetic. The bulk of the comments, 644 in total, were received on SP 800-171B from 46 unique organizations. The team has yet to begin comment adjudication. A number of requests were for access to SP 800-53, Rev 5 because the security requirements in 171B reference 800-53 Rev 5. The final draft of SP 800-53 Rev 5 is at the Office of Information and Regulatory Affairs for internal

review. Ms. Pilliteri reviewed some of the extensive feedback that was received on SP 800-171B. The comments can be found here.

Mr. McClelland of DHS noted that moving forward they will evaluate the HVA controls and align them with some of the risks that they are seeing. Then, pending the release of NIST SP 800-171B and NIST SP 800-53, Rev.5 an update will be made to the DHS HVA Overlay along with the development of resources.

NIST Health Information Technology Program Information Brief

Dr. Ram Sriram, Software and Systems Divisions Chief, NIST

The Chair welcomed Dr. Ram Sriram of NIST to brief the Board on the NIST Health Information Technology Program Information.

Healthcare is over 17% of the U.S. economy. $3.5 trillion dollars were spent on healthcare in 2017. It is estimated that approximately $750 billion is lost due to inefficiencies in the system. An effective use of information technology would likely help reduce cost. Another problem within the healthcare system are the multiple parties that play a role such as patients, doctors, government agencies, and regulators.

Levels of biological information go from the individual to DNA. There are several factors that play into making a future health vision attainable: 1.) Advances in Computing, Imaging, and Information Technology, 2.) Advances in Healthcare Practice, and 3.) Advances in Healthcare Technology.

The P7 Concept of Healthcare includes: 1.) Personalized, 2.) Predictive 3.) Participatory, 4.) Precise (recommendation, decision analytics) 5.) Preventive, 6.) Pervasive (including point of care), and 7.) Protective (Privacy and Security).

NIST enables interoperability and adoption by: 1.) Accelerating standards development and harmonization, 2.) Developing a conformance testing infrastructure, 3.) Expanding R&D and deployment of security protocols, and 4.) Leveraging testing infrastructure to assist with the certification process. These key activities in health IT lead to an emerging network that is correct, complete and secure. Additionally, they are exploring standards and measurements for emerging technologies in healthcare.

The NIST Health Care IT Projects include: 1.) Health Information Technology: Standards and Testing, 2.) Interoperability of Medical Devices, 3.) Biomedical Imaging, 4.) Bioinformatics, 5.) Text Retrieval (Past), 6.) Usability, and 7.) Security.

The HIT Standards and Testing project provides technical expertise to leverage industry-led, consensus-based standards development and harmonization, as well as, develop a conformance testing infrastructure to enable interoperability and adoption. They are

developing conformance test tools for fully integrated health IT systems to assure that the standards are implemented consistently. Collaboration with industry includes Health Level Seven (HL7), IEEE, and integrating the Healthcare Enterprise (IHE).

Looking at the Healthcare ecosystem there are a number of participants including hospitals, medical offices, pharmacies, laboratories, devices, etc. Almost everyone is using an electronic health record (EHR) system. Some key issues under an EHR system include:

- Input (user interfaces)
- Store (representation and persistency)
- Manipulate (search, mining, knowledge creation
- Exchange (syntactic and semantic interoperability)

All of this information must remain secure. EHR interoperability is a fundamental problem. Syntactic and semantic interoperability will have to be considered. All of this must conform to some standard.

Standards are the baseline for technical, syntactic, semantic and organizational interoperability. Some of the challenges with health IT Interoperability Standards include:

- Standards can be non-existent for certain domains
- Existing standards can be poorly defined
- Poorly defined standards can be poorly implemented
- Well-defined standards can be poorly implemented
- Well defined standards can be ignored (i.e., not adopted)
- Standards can compete with each other (too many standards)
- Standards can be complex

Some of the common issues with health IT standards include: under specified, multiple solutions, conflation of requirements, documented current state and not the desired state, not specified enough (code system binding), too specific, poor documentation and typos, lack of consistency, conditions without condition predicates, absence of harmonized requirement specification methodology, insufficient requirement specification mechanisms, lack of reference, pilot implementations, lack of testing, and improper scoping.

In 2009 the American Recovery and Reinvestment Act (ARRA) identified NIST to lead the development of health IT testing infrastructure. ARRA emphasizes the need to move toward electronic health records. The legislation called for NIST to:

- Ensure health IT standards are complete and robust,

- Establish a health IT standards testing infrastructure that supports industry consensus standards development and provides robust conformance and interoperability testing capabilities, and
- Deploy those technologies to promote interoperable health IT adoption.

Three stages were proposed for Meaningful Use (MU) of the EHR. NIST developed the tests for compliance with the MU criteria. Based on the requirements in the Office of the National Coordinator (ONC) Final Rule, NIST published 45 test procedures which are in use by the accredited testing laboratories to test and certify EHR products for the MU Program. NIST's tools are foundations for MU implementations.

In December of 2016 the 21st Century Cures Act Sec. 4003 Interoperability passed. NIST is developing a testing infrastructure to provide a scalable, automated environment for current and future testing needs. NIST will collaborate with health IT stakeholders to harmonize healthcare standards test development and delivery to ensure conformance and interoperability within the healthcare domain.

Medical devices involve interoperability and body area network standards and security. There are two processes with respect to medical devices. One is the patient care health device connectivity and the other is the personal health device connectivity.

Healthcare sector projects at the NCCoE include; Securing Telehealth Remote Patient Monitoring Ecosystem Project Detection, Securing Picture Archiving and Communication Systems Project Description, Securing Wireless Infusion Pumps in Healthcare Delivery Organizations (SP 1800-8) and Securing Electronic Health Records on Mobile Devices (SP 1800-1). Additional work is focused on Biomedical, Bioinformatics and Smart Health Care.

Does the Health IT research go into the question of usability, simplicity, and efficiency of use versus just interoperability and security? A focus is on the usability of the systems. One is the technical aspect and the other is interaction or the ecosystem aspect. In the future, the hope is that a doctor will need to interact less with the computer as video and speech should capture the discussion.

Briefing on DoD Maturity Model for Contractors Using SP 800-171

Ms. Katherine Arrington, DoD

The Chair welcomed Katherine Arrington to brief the Board on the DoD Maturity Model for Contractors using SP 800-171. Ms. Arrington is the newly appointed Certified Information Systems Security Officer (CISSO) with the Acquisition and Sustainment Office at the Department of Defense (DoD).

When Ms. Arrington arrived at DoD she knew something needed to be done fundamentally different. The culture needed to change so that security is foundational. Ms. Arrington was brought in as a highly qualified expert (HQE) to make a change and set up policy. Working with partners at DHS, NSA and DoE, everyone is struggling with the same problem of culturally making a change.

Our adversaries are already behind the walls and in the systems. They are not coming in at the state-of-the-art top-tier prime contractor nuclear level, but rather through the lowest tier of contractors to gain access. The adversary is going through a random supplier who is a third or fourth tier connection.

There are three-hundred thousand (300,000) suppliers within the defense industrial base. Ms. Arrington is not concerned with the top ten but rather the two-hundred and ninety thousand (290,000) that self identify as being NIST 171 compliant, but are not. Ms. Arrington knows because in the past she herself unwittingly conducted work in an unsecure manner. As an example, she would utilize public Wi-Fi at a coffee shop to VPN into a secure system. The moment she utilized the public Wi-Fi the system was no longer secure. We are all human and we all make mistakes. No one is intentionally trying to not do the right thing. Our contractors and vendors want to do the absolute right thing, and when they say they are NIST compliant, they think they are. The problem is we no longer teach critical thinking. The people who created the NIST 800-171 are brilliant but those utilizing it do not have the same cyber and IT degree of critical thinking and it does not convey.

How do we get everyone on the same level? The Cybersecurity Maturity Model Certification (CMMC) was created by the DoD. The CMMC will become a go/no-go decision. They are flipping the requirements so that critical thinking is behind what needs to be done. Every single supplier in the three-hundred thousand (300,000) company supply chain will have to get certified to some level of CMMC. For maturity level one, there are seventeen (17) controls that are equal to FAR 52. Everyone will be required to do the bare minimum. Maturity level two on CMMC is the seventeen (17) controls plus forty-six (46) additional controls. Here a company is starting to build critical thinking about cybersecurity and security. Maturity level three is good cyber hygiene. It is also where CUI is introduced into contracts. Therefore, the full instantiation of NIST 800-171 includes one-hundred and ten (110) controls. If you take forty-six (46), seventeen (17), and the twenty-seven (27) controls, that is compliance to NIST 800-171 in totality. The CMMC also maps to similar controls that can get to the same requirement in ISO 27000, in GDPR, and in the AIA NAS 9933 Standard, etc.

We envision maturity levels four and five to be what is happening in NIST 800-171 Revision B. Revision B is what we are looking at to add our specialized protection of critical technologies and protecting critical infrastructure. It is expensive. The incentive to get

industry to acquiesce is to make security an allowable cost by giving it value. Ms. Arrington sits on the Federal Acquisition Supply Chain Council (FASCC) that was set up as part of Secure Technology 2018. Making it a financial incentive that contractors cannot do the work unless you are right when you are certified will drive the contractors there.

The Revision 4 of the CMMR will be available at the end of August for review. Broad feedback is welcome to include industry, institutions and academia. The work has always been collaborative and will continue to be. The plan is to turn it over to the consortium of non-profits to set up the certification in January of 2020. Between January and June of 2020, they will prepare to train the trainers and certify the individuals or companies who will be redoing the third-party certifications. We are simultaneously in the process of re-writing DoD instruction 5000. They are taking that robust document and adding a cybersecurity and security enclosure. With a cybersecurity enclosure in 5000, it will mirror the CMMC levels. In the re-write, it will not be a one-size fits all with special consideration of the participation levels. In the Fall of 2020 it will be in RFPs.

If we do this as the largest buyer in the U.S, Government, the DoD and other agencies should follow suit. Ms. Arrington hopes to get other agencies interested early should the FASCC say this should be the standard for the Federal Government.

Mr. Lipner noted that the history of CMM goes back to the 90s. We have had a few maturity models for other DoD purposes but it has not been a pretty story. Are tests being conducted to verify that a CMMC level 5 enterprise is really a hard target and that a level 1 is harder than a kid sitting in his basement and so on? When Revision 4 is released on August 30th the path finders start the following Monday. We are taking actual contracts. We are taking contracts that are currently active in the Department of Defense and would be a level 5. The companies have volunteered to come in and do the certification with us. We have Johns Hopkins and Carnegie Mellon coming in to validate. The other part is bringing in other people to do the audit on what we're looking at. So, we're bringing in the intel community in, USDIs, DCSA, DCMA, and NSA.

Mr. Lipner commented that it is very important that, 1), they build 'honest-to-God' what the requirements say they have to do, and 2), get an adversarial test 'honest-to-God' of a system that claims to have done those requirements and then take the feedback from those results before they roll it out. Ms. Arrington commented that they have taken a war game effort, not done by the DoD, but a war game effort that we paid for an entity to do on systems, and overlaying that into what the maturity model looks like where we're seeing the exfills and the capability of our adversaries to penetrate outside of 'a NIST' and incorporating that into it as well. The consortium that holds the CMMC certification will be a bunch of non-profits. The consortium will have voting members and the capability to meet quarterly, to bring in the scientists, the data scientists, the government and industry

partners together to look at threat vectors that have come up and what can be put into the next yearly iteration to ex-fill the threat.

Ms. Arrington wants the CMMC to be used as a capability to communicate, to maintain awareness of our adversaries, and keep them at bay. It will be an education tool to communicate to supply chains as threats arise.

Brief on NIST Work in Artificial Intelligence and EO Maintaining American Leadership in Artificial Intelligence

Ms. Elham Tabassi, Acting Chief of Staff, Information Technology Laboratory, NIST

The Chair welcomed Elham Tabassi of NIST to brief the Board on NIST work in Artificial Intelligence and the EO Maintaining American Leadership in Artificial Intelligence.

On Feb 11th an executive order was signed to allow the U.S. to maintain its leadership in Artificial Intelligence (AI). NIST is cited in a specific task. The EO calls out in Section 6(d) to work on AI standardization and develop a plan to achieve this goal. It asks for a plan to address three things: 1.) Determine federal priority needs for standardization of AI systems development and deployment, 2.) Identification of standards development entities for federal agencies who will be tasked with defining leadership roles in AI; and, 3.) Opportunities for, and challenges to, U.S. leadership in standardization related to AI technologies. It gives 180 days from February 11th, which is August 10th, and they are on track to do that.

A Request for Information (RFI) was released on May 1st. It had 18 questions categorized in three topics. The first topic was on current status and plans. The second topic was around needs and challenges and the third was the role of federal agencies. The RFI was out until June 10th. A workshop was held on May 30, 2019. The purpose of the workshop was to engage the broader community to discuss their questions, the RFI, and what they want to see.

A draft was put out for public comment on July 2nd until July 19th. The plan has three sections and six appendices. There were 43 sets of comments. Many of the comments were on additional confirmation for the plan and others were suggestions for improvement.

Section one of the plan is on needs and challenges. What are the AI technical standards and why they are needed? What type of standards are needed, such as horizontal versus vertical, or cross-sector versus sector-specific standards, and the importance of both of them? All of the relevant standards listed in the appendices have been compiled from inputs from the community and responses to the RFI or public comment.

The second section is on USGAI standards. How federal government can engage in development of standards, what type of standard development organization they should be

engaged with, and what type of standards should be developed are included. It tries to answer the question or the task of the EO that identifies Standard Development Organizations that the federal government should prioritize to participate in. A list of characteristics and attributes was created that a good standard development organization should have. It also discusses the different levels of U.S. government engagement.

The last section includes recommendations for moving forward. There are four recommendations: 1.) Coordination and bolstering AI knowledge and coordination of federal agencies, 2.) Research and promoting focused research to accelerate broader exploration and understanding of how aspects of trustworthiness can be practically incorporated within standards, 3.) Recommendations about partnerships which include supporting and expanding public -private partnership to develop and use AI standards and related tools to advance trustworthy AI, and 4.) International engagement on strategic partnerships and work with partners and countries and maintaining awareness of standard development.

There are six appendices as noted earlier. Approximately half of the report is appendices. The message of the plan is short and concise with the bulk of the information being held in the appendices. The appendices cover, 1.) Definitions, 2.) AI Standards, 3.) Related Tools for AI Standards, 4.) Assignment and Approach, 5.) Request for Information, and 6.) Workshop Agenda.

For August activities, two documents will be put out. The first is the plan as requested by the EO which has a deadline of August 10th. The second includes a more detailed analysis of the RFI and public comments received.

Ms. Tabassi provided a short brief on the NIST AI Research Program. NIST's fundamental research in AI is concerned with how to increase trust in AI. The first question is to determine what "trustworthy" means. The goal was to determine characteristics or attributes for trustworthy AI and focus on technical requirements and ethics. Important qualities for AI include accuracy, reliability, security, robustness, objectiveness, privacy, and explain-ability.

The next step is to come up with a way to measure the attributes. How much accuracy or security does one need? This goes to identifying the risk and what is acceptable for a particular use case and what is the right combination of each of them. There will be a more detailed discussion about this in the document analysis of the RFI public comments.

Two projects coming out of the attribute work include one on Secure AI and another on Explainable AI. For Secure AI, they started by developing terminology and taxonomy of attacks and defenses for Adversarial Machine Learning. NIST has been working in collaboration with MITRE. An extensive literature survey was sent out through both NIST

and MITRE for input. A draft for public comment is planned for September 2019. The second project is Explainable AI. Explainable AI forms the basis of addressing fairness, bias, transparency, security, safety, and ultimately trust in AI systems. They have developed a paper on the Principles of Explainable AI and will have a draft for public comment planned for January 2020.

DHS Supply Chain Risk Task Force Briefing

Mr. Robert Kolasky, Assistant Director, DHS Cybersecurity and Infrastructure Security Agency, National Risk Management Center

The Chair welcomed Robert Kolasky to brief the Board on the DHS Supply Chain Risk Task Force. Mr. Kolasky is in charge of the National Risk Management Center with the Cybersecurity Infrastructure Security Agency.

The National Risk Management Center is a planning analysis and collaboration center where they work on the biggest strategic risks to the nation's critical infrastructure. They are steeped in the analysis of understanding critical infrastructure, trends related to critical infrastructure and how those trends lead to creating changes and evolving risks. In partnership with the analysis is convening groups of people who have the authorities, capability, knowledge, and ability to make progress and to make the country and infrastructure more secure. Strategic risks include threat actors, digitization-connectivity through digitization, changing and emerging technologies, market forces, and governmental gaps.

Mr. Kolasky is here to specifically discuss the effort the center is taking around Information Communications Technologies (ICT) Supply Chain Risk Management, the sources of strategic risk and the policy imperative and opportunity for the government to be better. The Information Communication Technology Supply Chain Risk Management Task Force was established last year as a governance body for a joint effort to reduce risk, build up capability and ultimately reduce risk across the ICT supply chain. It is represented by 20 federal agencies with 20 members of the communications sector picked through the Communication Sector Coordinating Council and 20 members of the IT sector picked through the IT Sector Coordinating Council. The Sector Coordinating Councils are the governance bodies of industry that were established through the Critical Infrastructure Partnership Advisory Council (CIPAC) through the Homeland Security Act going back to 2003.

The CIPAC structures allow for a focused, fair and transparent way to bring industry to the table around critical infrastructure issues and work with them through task forces that are governed by CIPAC authorities. The CIPAC structures sit across all of the 16 critical infrastructure sectors. There is a one-to-one representation of the agencies that are

identified through the Secure Technologies Act to sit on the Federal Acquisition Security Council (FASC).

The task force is now working on three principal activities. The first is creating an inventory of significant supply chain activities, capabilities and processes that are in place across the federal government, the IT sector and communication sectors. The inventory will help put together a greater landscape of what's going on across the community.

The second activity is being primarily conducted through four working groups. The first working group is focused on improving information sharing. The second group is working on threat evaluations and understanding and prioritizing supply chain threats and supply chain cybersecurity threats in particular. The third and fourth working groups are more focused on the incentive or business decision side.

The third activity is focused on the source of interagency and industry input into supply chain practicalities risk assessment that was done per the Executive Order that the president signed in the Spring of 2019. The order directed the Secretary of Commerce, in the face of the national ICT supply chain emergency, to put IEEPA (International Emergency Economic Powers Act) authority to implement rules to ICT companies to not take certain levels of risk or put certain things into their systems. In the assessment we created a taxonomy of the ICT supply chain grouped into five elements: local user access, transmission, storage, processing, and system management. 100 sub-elements were ultimately identified through those five categories of the ICT supply chain. They worked with industry to judge whether those elements were critical sources of risk, had manageably critical sources of risk or were not critical in terms of risk. The assessment has been completed and sent to the Secretary of Commerce for review. How the Secretary of Commerce and the Commerce Department ultimately uses the assessment is to their discretion.

The work of the assessment was built through a framework and they will continue to dig deeper into their understanding of some of the elements. It is intended to be an enduring frame to look at supply chain risk. The work is in process. A task force meeting will be held in a couple of weeks where they will brief the first round of findings.

The aim is for the task force to publish an interim report by September that lays out some of the things they have accomplished to date as well as proposed next steps.

Talk from Greg Garcia, Health Sector ISAC

The Chair recognized Greg Garcia to provide his parting thoughts upon exiting his post on the ISPAB.

Greg noted that it has been a privilege to serve on the ISPAB. The Computer Security Act of 1987 started the ISPAB with a clear and compelling mission. It is difficult to keep the focus on any board. The ISPAB can build and re-build its influence and visibility.

The format of these meetings is one we have come to expect. If change is good then what could we do differently? What if, for every tri-annual meeting, there is a theme for everybody to speak to in order to derive an assessment? The Board gets little snippets of information at every meeting. Greg suggests doing a deeper dive that is focused on a theme over the three meetings in a year. A year's focus would allow the Board to derive expertise and subsequently provide advice. The Board has not been writing a lot of letters because they don't have enough to comment on.

Another suggestion Greg imparted was with respect to a ten-year report. Review the archives and the letters and write up a report concerning what the Board has recommended and what has been implemented. ISPAB is an influential group that is held to a high standard. The people who brief the board are technical experts.

Final Board Reviews and Discussions

The following areas were discussed by the Board in its review:

Letters:

Letter 1: Marc Groman proposed a letter concerning 800-53 (Security and Privacy Controls) be sent to OMB regarding where it stands in review. Marc will draft an initial letter and send to Matt Scholl for dissemination to the Board for review.
Letter 2: Chris Boyer to draft letter on IOT to be sent to OMB (harmonizing interoperability between US and other countries). Draft letter will be provided to Matt Scholl and sent to the Board for review.

1. Moonshot report:
    a. The board will hold on any decisions until feedback is provided from the Workshop planned to take place at Auburn in August.
    b. By next meeting it might be possible to write something about making this work more of a national priority.
2. Next meeting we should have someone come in to discuss the Solarium report.
    a. It will be interesting to see the how the work of both the Moonshot Report and the Solarium report are converging.
3. Next meeting topics:
    a. No topics were officially proposed.
4. December 3rd and 4th is the potential next meeting date. Location: AIA. The date may shift if needed.

Meeting Recessed

The meeting adjourned at 4:32 p.m., Eastern Time.

List of Attendees

Last Name	First Name	Affiliation	Role
Brewer	Jeff	NIST	DFO
Arrington	Katherine	DOD	Presenter
Boeckl	Kailin	NIST	Presenter
Dubsky	Lance	Iron Mountain	Presenter
Horvath	Steve	Telos Corporation	Presenter
Lefkowitz	Naomi	NIST	Presenter
McClelland	Alan	DHS	Presenter
Megas	Katerina	NIST	Presenter
Nadeau	Ellen	NIST	Presenter
Petersen	Rodney	NIST	Presenter
Pillitteri	Vicki	NIST	Presenter
Romine	Charles	NIST	Presenter
Scholl	Matt	NIST	Presenter
Schulties	Brad	Rackspace	Presenter
Sriram	Ram	NIST	Presenter
Stine	Kevin	NIST	Presenter
Tabassi	Elham	NIST	Presenter
Petrella	Evie	Exeter Government Services	Staff
McConnell	Andy	Exeter Government Services	Staff
Belluche	Wayne	Elbit Systems of America	Visitor
Bolin	Elizabeth	NC5	Visitor
Daily	Kathryn	BA1	Visitor
Dodson	Donna	NIST	Visitor
Galvin	James	Atwork Systems	Visitor
Geopel	James	Fathom Cyber LLC	Visitor

Last Name	First Name	Affiliation	Role
Gibbons	Jeremy	General Dynamics	Visitor
Hebert	Terry	Centurum	Visitor
Heyman	Mat	Impresa Management Solutions	Visitor
Johnson	Derek	FCW	Visitor
Park	James	Wilkinson Barker Krauer, LLP	Visitor
Price	Gianna	Telos	Visitor
Rogers	Susan	FS-ISAE	Visitor
Ruhnke	Jay	Suprtek	Visitor
Sommese	Scott	Centurum	Visitor
Tupitza	Charlie	Americas SBDC	Visitor
Wallace	Mark	DHS	Visitor
Walther	Cornett	Elbit Systems of America	Visitor
Wise	Rob	DHS	Visitor
Wootton	Bill	CS Integrated Solutions	Visitor