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

March 20 and 21, 2019

700 13th St. NW, Suite 1150, Washington DC 20005

Board Members
Steve Lipner, SAFECode, Chair, ISPAB
Chris Boyer, AT&T
Janine Pedersen, NSA
Laura Delaney, DHS
Greg Garcia, Healthcare Sector Coordinating Council
Patricia Hatter, Qualys
Marc Groman, Privacy Consulting
Brett Baker, Nuclear Regulatory Commission, OIG
Jeffrey Greene, Symantec

Absent with Regrets

Board Secretariat and NIST Staff
Jeff Brewer, NIST, DFO
Robin Drake, Exeter Government Services, LLC
Warren Salisbury, Exeter Government Services, LLC

Wednesday, March 20, 2019

Welcome and Opening Remarks

Steve Lipner, Chair, ISPAB, Executive Director, SAFECode

The Chair welcomed everyone to the meeting at 9:13 a.m., Eastern Time. The March 2019 meeting is Mr. Lipner's first Board meeting acting as Chair. He encouraged everyone to be more active on agenda items in the course of the meeting. Speakers inform the Board and it is useful for the members to be active in terms of asking questions.

Janine Pedersen, NSA, is joining the Board as a new member.

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. Dr. Romine noted it is an extraordinary privilege to work with ITL.

ITL's purpose is to cultivate trust in information technology and metrology. NIST is the U.S. national metrology institute, and 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 activities, lab standards and their adoption is a critical concern. There are four priority areas: 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 artificial intelligence work. IoT is a booming area with many security requirements.

ITL has significantly larger objectives in cybersecurity and privacy. Goals include:

- Developing and issuing a privacy and risk management framework by fall, 2019.
- The next release of FIPS-140-3, detailing requirements for agencies to employ cryptography. The Cybersecurity Framework is a key portion of this area.
- Completion of round two of the quantum cryptography algorithm process by this time next year. The down-select to 27 algorithms has happened. Mr. Scholl, Chief, Computer Security Division will provide an update to the Board during the NIST update.
- More will be presented on the Privacy Framework. It is a voluntary risk management tool. A summary analysis of the responses to the Request for Information (RFI) emphasizes making sure it's consistent to the Risk Management Framework (RMF). An outline of the Privacy Framework was issued in February. A workshop will be held at Georgia Tech in May 2019 for further discussions.

There are three major focus areas in cryptography: post-quantum cryptography, lightweight cryptography, and automated cryptography. Working with the private sector as a trusted and impartial entity, NIST can change the world for the better. Post-quantum is helping to prepare for the inevitability of quantum systems; lightweight cryptography is intended for smaller systems where chip design and size do not allow for full-sized cryptographic applications; and automated cryptographic validation protocols where there is a need to be more agile.

IoT devices have proliferated, causing issues in trust. NIST needs to be in partnership with vendors as they develop new products. The goal is to maintain the ability to innovate, but with standards for device security.

The National Cybersecurity Center of Excellence (NCCoE) is now in its sixth year. New programs are being added. The NCCoE provides practice guides that can walk people through how to secure their IT environments. The National Security Partnership (NSEP) program has now expanded to 40 partners located at NCCoE from the original 12 partners. The Department of Commerce is the first Federally Funded Research and Development Center (FFRDC). FFRDCs are public-private partnerships that conduct research for the federal government.

Dr. Romine testified to the Small Business and Enterprise Committee last week on how NIST is supporting cybersecurity for small business. This is the 17th time he has testified before Congress.

In standards development for AI, the Fundamental and Applied Research and Standards for AI Technologies (FARSAIT) has two important aspects: applied and fundamental. Fundamental standards measure and enhance the security and trustworthiness of AI systems. Applied standards delve into the use of machine learning and AI within NIST scientific programs. Today, measurements at NIST are augmented by IT across the board. The same thing will be true in the future such that measurements will be augmented by AI. How to instill trust in AI? How do we nurture trust in automated systems? It is ITL's work to accomplish these goals.

The executive order on maintaining American Leadership in AI calls out NIST specifically. NIST must develop a plan for federal engagement and how to engage standards development to support systems in the future within 180 days of the signing date of the order. The report is due August 10, 2019.

The National Science and Technology Council (NSTC) operates the AI select committee. Dr. Romine participates on the MLAI subcommittee. There is a joint NITRD and NSTC workshop on AI and cybersecurity June 3-5th at the University of Maryland, College Park. NIST also partners with the Joint Center for Quantum Information and Computer Science (QuICS) at the University of Maryland at College Park to do quantum research.

ITL was assessed by the National Research Council. There were three takeaways: ITL has areas of national importance; NCCoE has added significant value to ITL; the long-term viability of ITL is derived from its recruiting.

There is legislation pending on IoT security. Will the legislation be consistent with the direction of ITL? One of the outgrowths of building trust over decades is the connections ITL has with congressional staff. They know NIST has no agenda. ITL members often have conversations with House and Senate staff. ITL does not hand them legislation. It's not the role of ITL to do this. NIST will provide commentary on the impact of proposed legislation to ITL, or of other consequences legislation. ITL is reviewing IoT legislation.

NIST UPDATE

Matthew Scholl, NIST

Kevin Stine, NIST

The Chair welcomed Matthew Scholl and Kevin Stine of NIST to the meeting to update the Board on NIST activities. Since the last meeting, the Computer Security Division (CSD) was reviewed by the National Research Council (NRC). They have looked at how to integrate CSD activity with other divisions. Dr. Romine received approval to keep the National Vulnerability Database (NVD) operational during the furlough. It is a critical security function. The database was able to continue to receive vulnerability data during the furlough.

Twenty-six (26) round-two submissions remain in the quantum algorithm competition. The competition started with 69 submissions. Round 2 will be completed in 2020. Then the standardization phase starts. The focus has been on implementation of cryptography standards. Cryptography transitions in the past have provided lessons learned that are applicable. There is always a need to improve communications with industry and customers on expectations.

NIST had a great session at RSA with industry and infrastructure. NIST is starting preparations to understand the right questions going forward and finding answers for many other questions. There will be a larger discussion on transitions in the future. An August workshop is planned in Florida to talk about transitions and applications.

The FIPS-140 standard has been updated and submitted to Commerce for approval. It will aid in alliance with ISO standards. NIST can then use more automation in testing tools. There is also a workshop in Vancouver, on where we stand on automation going forward.

The deadline for lightweight cryptography submissions has been extended 34 days. Fifty-seven (57) submissions have been received. NIST will be able to move more rapidly in down-selecting submissions in this category. There is a new area of research looking at methods to make encryption stronger by having multiple fail-safes. The research involves establishing the threshold where combining fail-safes does not overwhelm the system. Different threat models are being used in test. It should also handle human error situations.

Level of difficulty is another threshold being considered. The lightweight cryptography team has looked at testing to see what can be automated and whether tools can be used.

The Risk Management Framework (RMF) has an active community and wide use globally. NIST has been very happy with the international uptake. It is available in numerous languages including most recently, Portuguese. International and federal activity will be a key area of focus. The goal is to create greater integration between the various frameworks and guidelines. NIST IR 8170, *The Cybersecurity Framework: Implementation Guidance for Federal Agencies* will be finalized. It came out the day after Executive Order 13800 was signed. There has been much activity in federal risk management in the last year. The first version of the framework was released five years ago, along with a roadmap for covering areas that needed to be enhanced or added in the future. Framework version 1.1 added identity management and supply chain security.

The Privacy Framework roadmap will be updated with the RFI responses. Ms. Lefkovitz and Ms. Nadeau will update the Board on the RFI responses for the Privacy Framework.

In small business cybersecurity activities, the Small Business Cybersecurity Act provided resources to help small businesses manage risk. The NIST Small Business Cybersecurity Corner is now online. It was announced at RSA.

Identity management activity included a PIV user and implementers workshop. The idea was to talk about challenges with the PIV; how is it being used in ways that were not originally anticipated; determining whether changes required to support those new or different uses, and what is needed going forward to stay relevant. Some of the cryptography used in the PIV is public key infrastructure (PKI) and elliptic curve, that will need to be replaced post quantum. Through-put, efficiency, and trust-related items need to be considered going forward, as well as the use of stronger identities and zero-trust networks and implementations. The focus is on protecting the data.

NIST is looking at research issues and foundational security in this area. Ms. Tabassi will be updating the Board on AI on Thursday. The AI lab met with Microsoft and IBM. Industry has been a great resource on challenges and lessons learned.

NIST is working with supply chain management. The goal is to try to understand how to provide better assurances of trustworthiness in supply chain. Mr. Scholl's group is researching best practices. There is a joint partnership with industry working on challenges. There is new legislation on supply chain, including creating a supply chain council. NIST was sought out by OMB and has agreed to serve on the council. The council is looking at specific IT supply chain risk issues. The council had its kickoff, and will be looking at scopes and additional issues.

Dr. Copan is very interested in technology transfer programs. He is working with industry to make sure NIST guidance is implementable. NIST participates in 3GPP, the Internet Engineering Taskforce, ISO, and other organizations.

Cybersecurity workforce development is ongoing with the National Initiative for Cybersecurity Education (NICE). The NICE Strategic Plan has a required five-year update coming up in 2021. NICE will seek feedback on the *NICE Strategic Plan* later this year. Input from the Board on the plan will be welcomed. The *NICE Strategic Plan* may be a future meeting topic. The NICE Workforce Framework will have a refresh in 2020. The process is starting informally, with more to come. We continue outreach with monthly webinars. The annual NICE Conference and National Cybersecurity Career Awareness Week (NCCAW) are coming up in November and the K12 Conference is in early December.

NIST IR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* was issued in draft a few months ago. Feedback has been received and work to incorporate it is ongoing. A discussion paper on a core IoT capabilities baseline is in process. It is a first attempt at capturing capabilities. The paper served as input to meetings at RSA and a webinar today. We anticipate publishing updates to the paper in spring, 2019, followed by workshops and other activities.

New projects, including the healthcare portfolio project involving picture archiving and communications, are in the build phase. For telemedicine and remote patient monitoring, we have received comments on the description, adjudication is ongoing. Greg Garcia with the Healthcare Sector Coordinating Council, and this Board, has been helpful.

Secure domain routing guidance is in the final stage of reviews. It will be finalized soon. There have been additional trusted cloud activities. We have published Volumes A and B. In the Microsoft trusted cloud build, Volumes A and B will be published next quarter, Volume C in October.

There is an IoT project related to the use of Manufacturers Usage Description (MUD). There have been IoT DDOS reports of malware using the manufacturer's universal description (MUD). There is a workshop in April at NCCoE to discuss this malware.

Critical cyber hygiene activity has involved helping organizations to patch their enterprises. Opportunities exist to help make improvements. The project is seeking collaborators. Federal Network Resiliency (FNR) will seek partners to work on this at NCCoE.

Transportation Layer Security (TLS) 1.3 changes from version TLS 1.2 present challenges to network security. It makes it challenging to go to TLS 1.3. The focus of the center is to understand business challenges. This project is receiving a lot of attention. "Robust" feedback is being received. Does TLS 1.3 fix server vulnerabilities? It does. Security versus visibility are key aspects of that discussion. NIST recommends TLS 1.3, with light use of TLS 1.2.

New projects being considered: moving from IPV4 to IPV 6; zero trust architectures, and 5G security capabilities. A 5G update is being presented March 21st.

Hiring cryptographers is going very well. Dr. Lily Chen and her group have done an outstanding job hiring cryptographers, mathematicians, and others to do research in cryptographic technology. Dr. Chen has worked with universities to identify potential candidates. It means getting a start on the workforce pipeline.

Brief on NIST Privacy Framework Program

Naomi Lefkovitz, NIST

Ellen Nadeau, NIST

The Chair welcomed Naomi Lefkovitz and Ellen Nadeau of NIST to the meeting to brief the Board on the NIST Privacy Framework. The process to develop the Privacy Framework was modelled after the Cybersecurity Framework (CSF). 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 from the RFI was released in late February. Feedback is being received on the outline.

A workshop in Atlanta on the discussion draft is scheduled for May. Challenges arise in privacy compliance. The goal is to have a framework with global standards. The privacy framework team has received lists of standards to consider, and additional information.

Framework attributes have received support. The framework should be a living document that can be paired with existing privacy approaches. There is not a uniform way to define or describe privacy risk. The majority of input wanted the framework to focus on the individual. It is not intended to be a prescriptive document but is intended to represent a discussion. How should the framework be structured? There was a clear interest in aligning it with the CSF. All the possibilities presented received positive feedback. Some said it should be a standalone document. There is alignment with the CSF, but the Privacy Framework also works alone.

The CSF core pillars also apply to privacy. Privacy overlaps with data security. The "Control" and "Inform" areas of the Privacy Framework are new. Privacy core areas include "Identify", "Protect", "Control", "Inform", and "Respond". Any response should be beyond incident-based. It entails coverage of what was done wrong and how to correct it. A section was proposed on how to use with the Risk Management Framework. It will cover how to use other frameworks. Profiles are also used. A user preference category was proposed, with preferences expressed as outcomes.

A lot of work remains. Processing data is not related to controls as yet. Ms. Lefkovitz and Ms. Nadeau are looking for early adopters willing to work on a pilot. The year allowed for completion of the framework will end in October.

The Privacy Framework included CSF tiers. Some organizations like them, others don't. The CSF tiers were adapted to the Privacy Framework. Tiers are intended to be appropriate to the organization and every role can help manage privacy risk. Compatibility can mean "doesn't conflict" with existing laws.

The Privacy Framework roadmap will be a key topic at the May workshop.

Brief on NSTAC Moonshot Report

Thomas Patterson, CTRO, UNISYS

The Chair welcomed Thomas Patterson to the meeting to brief the Board on the National Security Telecommunications Advisory Committee (NSTAC) Moonshot Report. Mr. Patterson was in the intelligence community but left in favor of a career in cybersecurity. The cybersecurity moonshot is in its infancy The moonshot report is an NSTAC product. .

Mr. Patterson feels "Chief Trust Officer" is a more indicative title to represent the needs of a cybersecurity role. Having one voice communicating to management on cybersecurity is where the world is going. Everything boils down to trust. The NIST Cybersecurity Framework had a rough start, but today it anchors organizations all over the world. Infrastructure engineering for most companies looks like a wreck. People don't know what they have on their networks.

The moonshot project must understand the human aspects involved in working with devices. People still don't consider security when they buy things. Industrial Control Systems (ICS) and IoT are still expanding. Lots of people are working on current problems. Is it possible to change the game and get to a more secure tomorrow? There is one chance to recover from the choices that were made in the past. The internet was built by, and for, "good" people and so it was not secured.

Adversaries will soon have the ability to intercept and decrypt all internet traffic; retrain AI to work against good purposes; disrupt real-time communications; create mistrust and masquerade as anyone, anywhere. The identity system is broken. The basics of security hygiene are important, but doing the basics alone will not stop any of the activities described here.

NSTAC is a non-partisan organization that was created in 1982. It advises the President on cybersecurity and other issues. It is made up of private sector executives. The NSTAC report is a draft but is a starting point. The goal of the cybersecurity moonshot is to make the internet safe and secure by 2028.

NSTAC has approximately 20 seated members from American telecommunications and technology companies with Top Secret or higher clearances, along with 30 staff, and invited 30 briefers from multiple disciplines to inform the members on a range of topics. They tried to learn from previous moonshot successes and failures. Privacy was considered from the beginning. The results of the research are in a report available for download.

The report contains a call to action on how to proceed. A full pillar of the report is dedicated to creating something that doesn't exist today. The intent is not to change the nature of the internet. The hope is people will opt in to achieving something better. They noted technologies that could be leveraged for good. The goal is to make the "whole of society" idea real. Everything in the report is deemed to be at least possible.

The report describes six pillars where dramatic action must happen. The six pillars are behavior, ecosystem, education, policy, privacy, and technology. All six pillars must work together for real change to happen. There are not enough PhDs that can get clearances to build what's needed.

There is a lot that is not in the report. Every possible outcome was graded as to the potential to achieve, ranging from ready to do, to at least possible. The outcomes that were deemed at least possible, were assigned grand challenge status. Anything less doable than that was deemed "nice to have", but not included in the report. It is to America's credit, that many people want to help with this effort. Four technology changes will have the biggest impact by 2028: advanced biometrics, 5G, AI, and quantum. Resilience, not perfect security is the goal. The report is on the DHS website.

Why was ten years selected as a timeframe? No one thought they could be successful in five years. The report will be moving out of draft in the next few weeks. Grand challenge workshops are being held at the military academies. The workshops started in February at the Naval Academy in Annapolis, MD. The next will be in April at the Air Force Academy in Colorado Springs, CO. The results of the workshop in Annapolis will feed into the workshop in Colorado Springs.

The Board discussed the moonshot project and determined it should send a letter with the Board's views after allowing the Board members time to download and read the report.

Brief on GPS/PNT Security and Threat Issues, Space-Based Positioning, Navigation and Timing

Harold W. Martin III, SES, Director, National Coordination Office, Space-Based Positioning, Navigation and Timing

The Chair welcomed Harold W. Martin to the meeting to brief the Board on GPS/PNT Security and Threat Issues, Space-Based Positioning, Navigation, and Timing. What happens when systems lose access to time? He is trying to raise awareness of what the authoritative sources of time are, particularly in critical infrastructure, and how to protect them. There are now many more devices that use GPS in use today than previously. However, not many backups exist that keep critical timekeeping functions running and accurate.

GPS is available to everyone and it's cheap. There are approximately 600 million GPS devices in the U.S. today. Most are in private or commercial use, but some are involved with national security, critical infrastructure, and federal systems. GPS uses radio frequencies to send and receive data. Most GPS receivers lack cyber resilience. To compound the issue, very few organizations test their timekeeping functions. Leap seconds, daylight savings time, and other time-related events cause help desk calls to increase. Critical infrastructure is extremely dependent on time. Mr. Martin is trying to raise awareness of the need to do testing with time, particularly in the IT sector. It's recommended that CIOs include GPS-enabled devices in their cybersecurity planning.

Pieces of what became NIST SP 800-183 *Networks of 'Things'* were in different places. The publication brought them all together. The BIOS protection guide was the first guidance in this area. A server-specific guide was next. Knowing where data comes from is important.

A software resilience publication is coming this year. Specifications are needed or not much progress will happen. There is urgency when major vulnerabilities are discovered.

Rather than create more recommendations, how can we pick up things that can be implemented? How is guidance routed to the world at large? Technical due diligence checklists may help. Actions need to be determined. It is a simple mandate, but complex to do. DHS has a task force working these areas.

There is work on a shared lexicon for attribution. Work has been done recently to identify bad actors. The need is to make sure we are talking about it the same way. There is a first attempt with the cyber threat framework to define a common lexicon. The mapping terminology is almost finished. . In this case there has been a lot of work on trusted platform modules (TPM). Some pieces existed in different specifications but the whole did not really exist in one cohesive form.

There is an event March 27th at George Washington University on GPS and cybersecurity for time assessments. GPS.gov has a best practices document that can be downloaded *(Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure*). The event will look at how to add a set of security rules associated with time, to increase cybersecurity. The need is to build more resilience in those systems that are time dependent. The latest GPS Interface Specification (IS-GPS-200) describes valid range checking and other topics.

There is a more focused effort on the presentation aspects of cybersecurity. There is work on getting recommendations implemented, and looking at key technical vulnerabilities that require joint effort.

The Resilient time project is one trying to use cyber resilience for better protection. NIST has led work with other partners on NIST SP 800-193, *Platform Firmware Resiliency Guidelines*. There is a new technical approach that went to final publication in May. Mr. Martin is talking with manufacturers to try to change their specification to use new resilience standards. Multiple ransomware incidents last year promoted the need for resilience. NIST SP 800-193 deals with hardware and firmware. There has been work on GPS processes.

Mr. Martin tries to get CEO-level attention because firmware solutions cost money. If the biggest users choose to only buy resilient firmware it will have an impact. BIOS work started ten years ago has led to most BIOS being protected today. This was a voluntary action. Mandated actions tend not to do as well. Supply chain is a shared problem.

Brief on NSA Public Private Partnerships

Cherylene Caddy, Director, Enduring Security Framework, NSA

The Chair welcomed Cherylene Caddy from NSA to the meeting to brief the Board on NSA public private partnerships. Ms. Caddy has been with a number of cybersecurity organizations over the years, most recently with NSA. Her focus has been on implementation aspects of cybersecurity. There are many advisory committees across the government. Recommendations for needed actions exist, but not necessarily the tasking to accomplish what has been recommended.

A group of agencies are looking at key technical vulnerabilities, intrusions, and things like the recent DNS high jacking and other incidents. These are complex, and longstanding problems. There are not immediate or easy solutions. Industry and government must cooperate to solve these problems. Efforts are being led by NIST in cooperation with others. A new technical approach is needed. Standards will be a critical piece of the implementation of the approach.

As the solution is developed, Ms. Caddy will use the time to look at how to talk to people on how to upgrade their technology. Everything has been accomplished with working through partners and voluntary adoption. The process is a phased roll-out approach and a whole government activity. It means determining what the issues are, what challenges to address, and deciding how to work through them. Present activities are intended to be a discussion starter. It serves to bring things into focus. This project involves more of the technical specifications

The first work that was done were action guides to educate people about firmware. BIOS chips for laptops are different than servers. What matters is that great things are going on as a whole. It's not just NIST. The data now available have will go a long ways to help create understanding of where data is coming from.

Risk management can make use of these kind of tools to understand what risks exist and where they come from. There is also a supply chain aspect. It can be useful for understanding supply chain. The goal is to figure out how to draw from these strategies for everyone's benefit. There is consideration of attestations on supply chains in contracting or procurement.

Policies can be implemented to describe what purchases are safe. Once that's done, the question is how to arrive at the means to make sure safe purchase levels are maintained in the future. It underscores the need for conversations to determine what should be done. There are other products and services that are high risk. Use cases are needed to determine how to remove those high risk products and software. A best practice approach is needed.

How is information shared about products? How do we manage risks in commercial products? It will be a focus of Ms. Caddy's work in the future. These processes will need to be developed. All of the information that's gathered on supply chains, needs to be translated to actionable form in order to be useful to those who need it. Getting the right information to those who need it, when they need it is key.

Ms. Caddy is also working on a shared lexicon for cybersecurity. We need to be able to discuss cybersecurity across all groups in the same way in order to collectively arrive at a confidence level of attribution of bad actors and activities.

Review of Wednesday Briefings

The Board will consider today's briefings and offer input during tomorrow's review and discussion session.

Public Comments

No requests for public comment were received.

Meeting Recessed

The meeting recessed at 4:04 p.m., Eastern Time.

Thursday, March 21, 2019

The Chair opened the meeting at 9:06 a.m., Eastern Time.

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

Elham Tabassi, Acting Chief of Staff, Information Technology Lab, NIST

The Chair welcomed Elham Tabassi of NIST to the meeting to brief the Board on NIST work in artificial intelligence (AI) and the Executive Order on Maintaining American Leadership in Artificial Intelligence. Most recently, Ms. Tabassi has been the Acting Chief of Staff for ITL.

There are those that think AI is wonderful, while some are more concerned about impacts of letting machines do so many things. This situation became the basis of the NIST AI 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 in the context of AI. The goal was to determine characteristics or attributes for trustworthy AI and focusing on technical requirements and ethics. Important qualities for AI include accuracy, reliability, privacy, robustness, and explain-ability. Researchers asked participants at RSA what they felt trustworthy AI meant.

The next step becomes defining these qualities and defining metrics to measure them. There are several standards activities. Most efforts and activity involve ISO. An AI proposal was first given to ISO in 2017. There are five working groups. Two groups are working with standards, the others are technical in nature.

The NIST AI Visiting Fellow program enables collaboration with the broader AI community and assists with furthering NIST research in AI, including research on terminology and taxonomy of attacks and defenses for adversarial machine learning. There is collaboration with MITRE in an extensive literature survey. A draft for public comment is planned for September 2019.

On Feb 11th this year an executive order was signed to allow the U.S. to maintain its leadership in AI. NIST is cited in a specific task. It 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: determine federal priority needs for standardization of AI systems development and deployment; identification of standards development entities for federal agencies who will be tasked with defining leadership roles in AI; and, opportunities for, and challenges to, U.S. leadership in standardization related to AI technologies. The report is due in 580 days or approximately August 2020. An RFI will be released in March 2019. NIST will analyze the results with a goal to have a workshop in late May 2019. The plan for federal engagement in technical standards development is in August 2019.

A workshop on AI and cybersecurity is scheduled for June 3-5 at the University of Maryland, College Park. Participation is by invitation only. People from industry and academia in AI and cybersecurity will participate. The goal is to create an outline of the report.

Is there a sense or understanding of the various aspects of adversarial AI? The taxonomy and terminology exists to describe attacks on AI. There is a lot of literature on published attacks and many examples. It is best to be proactive. It is not surprising to have a bad response, like attacks, on good advancements.

The community is proactive on talking about attacks but it is a small percentage of the actual attacks. The goal is to be proactive to a greater degree. The document being developed will go more into explain-ability and finding the right balance of the attributes that will increase trustworthiness. There are discussions about a risk management framework for AI. The community concerned with AI is very broad.

Brief on HHS Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Julie Chua, HHS Office of the Secretary, Office of the Chief Information Officer

The Chair welcomed Julie Chua to the meeting to brief the Board on Health and Human Services (HHS) Health Industry Cybersecurity Practices (HICP). HHS recently published its document on managing threats specific to the healthcare sector. It is the result of a public private partnership including healthcare and the public Healthcare Sector Coordinating Council. The government and sector coordinating councils worked together. The final draft was presented across the country. There were participants from all healthcare and cybersecurity portions of the sector.

Section 405(d) of The Cybersecurity Act of 2015 has a section on improving healthcare sector IoT security. The mandate to develop the approach is that use is voluntary, and prohibits any implication that following the guidance it contains is required.

The document was written for multiple audiences. Medical personnel were included in the task group in order to make it usable for them. The requirement was it must be actionable by non-technical healthcare staff. There are not many plain language resources available. The document goes into roles and reasons for healthcare personnel to be concerned with cybersecurity.

It is aligned with the NIST Cybersecurity Framework. The Framework is a good tool to introduce HICP to new people. HICP is not regulatory. This document should not be equated to terms such as "reasonable", or, "recommended", that imply any pressure for the user to adopt the approach or practices in the document. It is not a guide for compliance requirements.

The task group identified the five most prevalent threats to the healthcare sector today. These are email phishing attacks; ransomware attacks; loss or theft of equipment or data; internal, accidental, or intentional data loss; and, attacks against connected medical devices that may affect patient safety. It also asked security personnel what they were most concerned about. The responses from health sector respondents and security respondents were about the same. It was a good indicator the publication was going the right way. HICP includes four volumes dealing with large institutions, small institutions, and technical information.

The documents identified attributes that include the expected items for a healthcare facility (number of beds, number of providers, etc.). It does not define the entire organization solely based on one of the qualities listed. Organizations can then define what they believe they are.

It identifies ten practices that are important to cybersecurity for healthcare. The task group approved the list of ten by consensus. These ten practices will mitigate the five threats presented in the document. There are many ways to mitigate specific threats. It is not claimed or intended that this list is the complete solution. It is intended to be a good start. The "small" organization technical volume is intended to be a stand-alone volume. The document can be used as a gap analysis tool, but gap analysis is not intended as a primary use. Ms. Chua is the government lead. Cybersecurity is not a one solution process. One needs to adapt as conditions change.

The document went through a rigorous assessment process. Data sensitivity was one area where there was a lot of discussion. The data sensitivity aspect is touched on as far as classification appears in the "large" organization volume. Physicians do not look at data in terms of a classification. Data classification will be a topic in the future.

The idea of sector benefits was important to include. It is the vision or mission for the future. The cybersecurity awareness aspect is important. The hope is to increase awareness among physicians and others in healthcare. Among small providers, cybersecurity awareness is not a priority.

Information sharing is encouraged especially for best practices. Ms. Chua's team was able to get to every region of the U.S. either personally or virtually during the summer of 2018. Information professionals were the largest group of participants in the document pretesting phase. A range of roles participated. Larger organizations were more represented than small organizations in the pretest.

A stronger call to action was needed. Participants said stronger language was needed and it was included. Justifications for the suggested actions were included. Role based resources were requested, and will be included in the future. More aggregated resources are needed. Gathering these resources is in progress.

HHS was lacking data from physicians. It was good for HHS to hear directly from providers. The document is written from a healthcare perspective first, and then a cybersecurity perspective. How to address denial or other issues? Continue raising awareness. Many physicians are aware of the news, but the document made cybersecurity immediate to them. The need is for tailored materials doctors can use.

Staff training is being considered that will offer CAE credits. Offering credit for the training has created more interest. Any government guidelines are welcome resources. Sometimes government resources can be considered mandatory. HHS continues to emphasize the document is not mandatory. Public reaction has been positive. Any future activity will involve a public-private partnership. The hope is to continue to provide resources to the sector.

Within HHS, there is a steering committee that includes NIST. Within those divisions there are regulators. How will success and progress be measured? They make sure any product is the output of the partnership. They ask for information on cybersecurity uptake in the annual survey. The publication has been used for training. There is a weekly series that started March 21st on the five threats and how to mitigate them. The series is not recorded, they are working on remedying that. The Health Resources and Services Administration (HRSA) and others have expressed interest in the HICP document. They are rural and small and provide technical grants and resources.

Brief on DHS Emergency Directive 19-01 Actions to Mitigate DNS Infrastructure Tampering

Michael Duffy, Cybersecurity Division | Federal Network Resilience, Cybersecurity and Infrastructure Security Agency

The Chair welcomed Michael Duffy of DHS to brief the Board on Emergency Directive 19-01 actions to mitigate DNS infrastructure tampering. Mr. Duffy is the Deputy Director of the new DHS Cybersecurity and Infrastructure Security Agency (CISA).

There was an emergency directive during the government shutdown with a ten-day action timeframe. In early January, it became known that some DNS domains were being intercepted by bad actors. Industry began providing reports on analysis and activity. The activity was more global than in the U.S. DHS, ISPs, and industry started working together at that time and came up with basic steps. They utilized previous publications on DNS management and other resources to try to manage the problem. This was the first directive given by CISA, and the first emergency directive during a shutdown. Mr. Duffy has worked with agencies in the past on binding operational directives. This situation called for a more creative approach.

No federal agencies are known to have been directly affected as of the meeting date. The government is much better at DNS management now than it was in December. More continuous monitoring is going on. No organization is on its own. Cooperation across sectors is needed to secure the .gov domain and the American people.

Certificate transparency monitoring gave agencies visibility into their CT logs to be able to determine whether security certificates have changed. This understanding makes it possible to take steps immediately. The team had to come up with things that could be done within the ten-day timeframe.

On Jan 11th, 2019 CISA issued a notice to agencies on the tampering campaign that provided some good practices. Everything went on the public website. A federal participation call with over 500 participants was held the next week. A survey was taken during the call to try to enable people taking the immediate steps that were needed.

On Jan 22nd, 2019 the emergency directive was issued with four actions: Audit DNS records, change the DNS account password, add multi-factor authentication to those accounts, and required use of transparency logs. The January 22nd notice introduced certificate transparency logs to agencies. DHS will review the logs weekly, but the hope is agencies will review logs more frequently.

There were multiple calls with agencies on the four actions. Many agencies implemented within the ten-day timeframe. At this time, a handful have not completed the directive due to external dependencies. By early April, all agencies are expected to have the steps completed.

CISA is looking to sustain the actions taken, continue to monitor logs, and discuss what additional steps can be taken. The hope is to be able to build defenses over time in a methodical way. Interagency working groups are starting in order to continue progress. Agencies have been signing up for the working groups. A plan of action for the next year will be developed.

Emergency directives working with national partners, international partners, and industry have been issued. State governments enacted the directive because they felt it was prudent.

Brief on NTIA Work in Software Bill of Materials (SBOM)

Allan Friedman, NTIA

The chair welcomed Allan Friedman to the meeting to brief the Board on NITA work in software bill of materials. Transparency is not a new concept. Ingredient lists, safety data sheets and other tools all enhance transparency. Having a common frame of reference is critical to transparency.

Modern supply chains are complex. Having visibility into what is produced is helpful, whether for security or other purposes. There are a number of private resources available. There is a need for harmonization, and to bring everyone together. There was a kick off last August to work on SBOM.

NTIA works on an open community concept. Working groups form out of meetings. It is an iterative process, and progress has been made. A consensus was reached at the end of 2018. There are four working groups.

What is a bill of materials? The idea of a bill of materials is not new. Spelling it out takes some work. Defining the bill of materials is an identity problem. There is a core of identity and other characteristics with optional fields for specific elements. The group started with a minimum core of fields. A SBOM has a mandatory minimum of required information with a first level of dependencies that forms a dependency tree. The dependency tree will allow entities to determine their risk tolerance.

One of the obvious benefits is monitoring the supply chain. Security is never static. New vulnerabilities are discovered and vendors need to know about them. One of the largest banks in the world is asking about the software bill of materials. Software costs increase if there are unknowns in the software chain. It is a way to drive innovation and awareness across the supply chain.

Two standards influence innovation and awareness in the software supply chain. They are commercial vs. open source. There are two licensing tools, ISO and the open source tool SPDX. Open source has its own licensing standard. The Linux Foundation and others are concerned that licenses can be mapped in the open source community. For the moment, open source and ISO are in use, but it is not the government's decision to use one or the other.

Tools for risk assessment are needed across the board. GitHub does this today. Software will either come with, or be linked to, a bill of materials that the appropriate people can access. Securing the data can come with the bill of materials identifying each source.

A proof of concept came out of the first meeting. A partnership between the largest medical device manufactures and the best hospitals began to share data. Can SBOM be integrated into the hospital data systems? Healthcare has lagged behind in data security. The medical device community has been active in embracing cybersecurity risk. Medical devices face many challenges. They understand what can happen if flaws are not fixed quickly.
The FDA has indicated it will ask for a software bill of materials starting in 2020 (not requiring but requesting). Healthcare use cases were provided. The group communicates

constantly. It is not integrated into existing tool sets today. Most vulnerability management providers are involved in this process today. What does transparency look like? Public sharing is not ideal. The manufacturer's universal description (MUD) is possible to use for embedded devices. The important part is keeping it up to date.

This topic is not linked to other important discussions going on in government. Once it is done, it will be available to anyone who wants to use it. The next meeting is April 11th , 2019. There will be some new deliverables. A solid first draft of deliverables will be available by early summer. The hope is to get some feedback at that point. It should be more solid by fall.

Brief on 5G/LTE Standards and Security Issues

Michael Bartock, NIST

Jeff Cichonski, NIST

The Chair welcomed Michael Bartok and Jeff Cichonski of NIST to the meeting to brief the Board on 5G/LTE standards and security issues. The First Responder Network Authority was created in 2012. It required NIST to look into next generation standards for first responder network technology. The Public Safety Communications Division (PSCR) within the Communications Technology Lab (CTL) led the research effort.

In the last five years, they have been developing cyber expertise in telecommunications. Identity management for public safety is covered in NIST IR 8014 and covers secure application development for public safety. The division worked with network vendors in the Boulder, CO lab to test security features. Implementations with network venders enable optional security features. SP 800-187 is the LTE Security Guide. LTE is markedly more secure than its predecessors. Strong security mechanisms were integrated from the beginning.

LTE features include hardware security, device and network authentication, air interface security, backhaul security, and core network security. Hardware security includes the SIM and a hardware-backed crypto-module. Credentialed integrity key and confidentiality key are derived from the shared secret key.

The device and network mutually identify themselves. There are new air interface security features. Backhaul protection was not specified as required. There is no core guidance requirements for network security.

LTE threats include bid down attacks where an attacker can interfere with a legitimate connection and downgrade the security. Device and identity tracking means when a phone connects, it must provide its identifiers to the base station. The data provided by the phone has geolocation information. Rogue stations can interfere with emergency calls and might not allow emergency calls to go through. There is no user-plane integrity protection (checking the packets sent are the same as those received).

Many people are talking about 5G. The 3rd Generation Partnership Project (3GPP) is responsible for writing the technical specifications on how the system works. 3GPP writes specifications only, not standards. 3GGP has been around for a while. When 4G came, there were three groups that worked on specifications. One body is working on specifications for 5G.

NIST attends the working groups that work on 5G. The standardization process is iterative, and work is described in a technical specification and technical reports. Specifications are evaluated. It is a consensus-based process for the group. The group must do the analysis and arrive at consensus. Votes are not typically held on technical material, as it is seen as a failure of the consensus action of the group.

5G release 16, in process now, is set to finish in 2020. There are many deployment options. Security in 5G comes with 5G option 4. NIST Security for 5G started being defined two years ago. The group looks to NIST for guidance. It is an industry driven standards body. Advancements are being made. NIST tries to participate where it makes sense and where people will respect NIST's opinion. NIST's job is to support industry standards. Research efforts will inform priorities in standards development and engagement.

Brief on NIST Secure Software Initiative

Donna Dodson, Chief Cybersecurity Advisor, NIST

Murugiah Souppaya, Computer Scientist, NIST

The Chair welcomed Donna Dodson and Murugiah Souppaya of NIST to the meeting to brief the Board on the NIST Secure Software Initiative. Mr. Souppaya helped kick off the idea of examining what software is produced and minimizing vulnerabilities in software. There was a recommendation to possibly use the Cybersecurity Framework structure to help shape a secure software initiative. The idea was to go back to the Framework it was designed for. It is a set of comprehensive practices, not programming language specific, and not operating system or environment specific. An approach similar to the Cybersecurity Framework was used with four working groups:

- Preparing organizations – getting a commitment from organizations that produce software that their software engineers are committed to including security at the development stage; keeping security in mind when writing code;
- Preventing vulnerabilities – enabling developers to be able to do root cause analysis;
- Responding to vulnerability reports - identify and patch vulnerabilities; have a team to triage and find root causes to vulnerabilities; avoiding multiple mistakes; and,
- Protecting the software.

Developers can be very opinionated on software. NIST tried to find a different way to explain the desired outcome. The outcome based approach is helpful, instead of telling people how to do something.

Last year at RSA, NIST and SAFEcode presented the original approach. They received a lot of feedback. Some felt the terminology was too "waterfall-centric". The next version of the document was a white paper that was shared with industry. It was still considered too waterfall-centric and some components were missing. Has NIST considered using the Framework approach for this subject to make it more approachable rather than writing specific for software? The goal was to produce something actionable.

The hope is not to create a new set of standards, but to point out what already exists. "Framework" was recommended as a word to use to describe the material, rather than to imitate the CSF. It points to classes of tools that provide desired outcomes.

There is a draft of the white paper. The draft has become more outcome based. NIST received feedback from both types of developers. Major updates have happened since returning from RSA. The updates mainly involve presentation more than content. The draft is coming out in April. Mr. Souppaya and Ms. Dodson will send the white paper to the Board members for them to distribute. They would like to receive feedback.

Ms. Dodson is interested in any comments, but wants focus on the overall approach and usability. It is an opportunity for showing when a piece of software is ready. It also means bringing security to the security team at the beginning. It is key to get the security team to understand what developers use. Integration within existing tools is very important. They would like the paper to be out for the government so they can value the secure software process. Government purchasing may not be made in a way that includes secure software.

Board Review and Discussion

Chair and Members of the ISPAB Board

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

Letters: Dr. Romine expressed concern for losing funding on foundational research during Wednesday's update. More feedback from Dr. Romine is desired. It is something to track for the next meeting.

Additional Items:

1. Moonshot report:
    a. The board can provide feedback on the project. Recommendations are often made and then there are no other activities.
    b. The Board can pass the message not to ignore what's being said on this topic. A lot of great research sits on the shelf until it is too late.
        i. The challenge problems are an important component. They should be cast with the notion of making a contribution.
        ii. What happens can be indicative of the stakeholders involved. Without real accountability, the decade timeframe of the report may go by without real progress happening.
        iii. Program management, accountability and mobilizations are important. The Board should have the opportunity to look at the report. Is a conference call possible before the next meeting? Yes, it can be done. There is a short period before the President approves. Mr. Scholl will arrange the call.
2. During the next meeting, bring in someone to discuss the state of privacy legislation-federal, international and state. It seems like an emerging issue where multiple legal views may clash and where technology must accommodate all. Possibly federal policy makers should step up and create a meaningful standard. This board could recommend this sort of action.
3. Next meeting topics:
    a. Cyber workforce education update.
    b. Briefings – Legislative update on the internet of things and other topics.
    c. NICE Strategic Plan review
4. NASA briefing: It is useful to understand how agencies are implementing or not implementing what they are being asked to do. The NASA IG assigns a maturity level 2 out of 5 to the agency. It may be worth having the board examine what is occurring.
5. The Director of NIST would like to do a short brief for the Board.
6. Cisco-Telos threat block specific to the DNS issue. Have Telos come for a briefing.
7. Some initial work on supply chain legislation. Have someone come to the next meeting.
8. GAO brief- The government is still failing to manage cybersecurity acquisitions.
9. July 31- Aug 1, 2019 - potential next meeting dates. Location TBD. The date may shift if needed.

Meeting Recessed

The meeting adjourned at 3:09 p.m., Eastern Time.

List of Attendees

Last Name	First Name	Affiliation	Role
Brewer	Jeff	NIST	DFO
Bartock	Michael	NIST	Presenter
Caddy	Cherylene	NSA	Presenter
Chua	Julie	HHS	Presenter
Cichonski	Jeff	NIST	Presenter
Dodson	Donna	NIST	Presenter
Duffy	Michael	CISA	Presenter
Friedman	Allan	NTIA	Presenter
Lefkowitz	Naomi	NIST	Presenter
Martin	Harold W.	SES	Presenter
Nadeau	Ellen	NIST	Presenter
Patterson	Thomas	CTRO, Unisys	Presenter
Scholl	Matt	NIST	Presenter
Souppaya	Murugiah	NIST	Presenter
Stine	Kevin	NIST	Presenter
Tabassi	Elham	NIST	Presenter
Drake	Robin	Exeter Government Services	Staff
Salisbury	Warren	Exeter Government Services	Staff
Grossman	David	GPS Innovation Alliance	Visitor
Heyman	Mat	Impresa Solutions	Visitor
Longhitano	Douglas	American Honda	Visitor
Mahn	Amy	NIST	Visitor
Park	James	Wilkenson, Barker, Knarer, LLP	Visitor
Geller	Eric	Politico	Visitor/Media