INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

MEETING MINUTES

June 21 and 22, 2018

American Institute of Architects
1735 New York Ave., NW, Washington, DC, 20006

Board Members	**Board Secretariat and NIST Staff**
Chris Boyer, AT&T, Chair, ISPAB	Matt Scholl, NIST, DFO
John Centafont, NSA	Jeff Brewer, NIST
Patricia Hatter, Barrick Gold Corporation	Robin Drake, Exeter Government Services, LLC
Marc Groman, Privacy Consulting	Warren Salisbury, Exeter Government Services, LLC
Brett Baker, Nuclear Regulatory Commission, OIG	Andy McConnell, Exeter Government Services, LLC
Jeffrey Greene, Symantec	
Steven Lipner	
Absent with Regrets	

Thursday, June 21, 2018

Mr. Chris Boyer, ISPAB Chair, opened the meeting at 9:02 a.m., Eastern Time.

Welcome and Remarks

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

The Chair welcomed everyone to the meeting and provided an update of his activities since the last Board meeting. He has spent a lot of time on supply chain issues, along with working on the botnet report. Today's presentations on blockchain will be good topics for the Board to consider.

The botnet report is a continuation of what is in the Network of STEM Education Centers (NSEC) report in the fall of 2017. There's a lot of consistency between the NSEC report and the botnet report. It recommends a lot of actions that different sectors in industry should take on botnets. USTelcom, along with the Council to Secure the Digital Economy, which is a joint project between USTelecom and the Information Technology Industry Council (ITI), are looking at different ways to effectuate some of the recommendations that will hold some use. It's been a lot of work to determine how to effectuate change based on the botnet recommendations and how to deal with supply chain.

On behalf of the Board, the Chair welcomed its newest member, Mr. Steven Lipner of SAFECode. Mr. Lipner was a member of the ISPAB Board in the early 2000s.

Mr. Scholl introduced Mr. Jeff Brewer as the ISPAB Designated Federal Officer (DFO) in training. His training will be complete this summer. At that time, he will become the official DFO for ISPAB.

Welcome and Remarks

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

The Chair welcomed Dr. Charles Romine of NIST to the meeting to update the Board on Information Technology Lab (ITL) activities since the last Board meeting. The ITL at NIST has one central purpose, and that is cultivating trust in IT and in metrology. The lab tries to enhance cybersecurity to promote trust in IT and uses measurement science to promote the same trust. A central concern is trying to maintain a balance between fundamental research and applied research to attempt to put things into practice. Research is followed by developing standards and best practices, and then trying to drive adoption of those best practices and those standards.

There are a few high-profile programs run by the lab. The cybersecurity program encompasses a fair amount of that work. Cybersecurity, in its fullest interpretation, includes the privacy work that happens under the umbrella of the cybersecurity program. NIST has been doing risk management for nearly two decades. Work in cryptography has been going on since about 1972 making approximately 46 years and counting of cryptographic research. There is a longstanding program in identity management, and a somewhat newer program in privacy engineering.

There are two programs in cybersecurity that came from administration or congressional mandates. One is the National Cybersecurity Center of Excellence (NCCoE). Funding from Congress started about five or six years ago to establish the NCCoE. It started in a temporary location. The facility moved into a 60,000 square foot building provided by the State of Maryland and Montgomery County. It's located a couple of miles away from the Gaithersburg NIST campus. It's now almost fully populated. NIST works collaboratively with industry, academia, and with other federal agencies to solve practical problems faced by many sectors of the economy.

The other program is the National Initiative for Cybersecurity Education (NICE). This is a program NIST took on in a coordination role. Its function is understanding different roles and responsibilities that cybersecurity professionals can have in the workforce and has been very successful.

NIST has been concerned about the security of the Internet of Things (IoT). The issue is that first-to-market pressures override designing and building in cybersecurity at the outset. NIST has started to work with vendors, software providers and others to try to get cybersecurity as part of the conversation and get more emphasis on the security. NIST has received additional funding to do a little more work in this area.

There have been recent concerns about budget cuts. The current appropriations package saw NIST doing very well. The last time the Board met, the concern was NIST had to ensure that it had preparations in place in case there was a significant cutback in appropriated funds for its activities. The appropriated funding that NIST received, as a whole, turned out

to be a 28 percent increase, the largest increase among all of the scientific agencies. However, the vast majority of that increase went to a construction-specific account. Congress was sympathetic to the reality that NIST's infrastructure, in Boulder and in Gaithersburg, has been crumbling for a number of years. The vast majority of that sizeable increase went to infrastructure repairs. There is additional funding in the appropriations language for the research funding account, which amounts to about a 5 percent increase.

One exciting piece of news is the lab spent a significant amount of time over the last several months preparing for the National Research Council (NRC) external review on the quality of the work it performs. They bring in experts over the course of a couple of days to do an in-depth evaluation of one or more of the laboratories. It was ITL's turn a week or two ago.

The reviewers look to determine what, in addition to the lab's current activities, can be corrected or improved upon. They provide insight on areas of improvement, gaps, and provide other feedback such as from the private sector, other government agencies, and academia.

The NRC is tasked with determining how well the lab is doing what it is tasked to do. A panel reviewed one-half of ITL when Dr. Romine first became the director. He received permission to review half of the lab rather than the entire lab because he wanted a greater level of analysis this time.

The part of the laboratory that was reviewed included the entire cybersecurity program, the Advanced Network Technologies Division, and the Applied and Computational Mathematics Division (ACMD). The results are not available yet. The evaluation went really well. Dr. Romine will receive a formal readout and a formal report. The report tends to happen at the very end of the year.

The lab has ongoing engagement in artificial intelligence (AI). NIST has been looking at artificial intelligence and machine learning for some time. NIST has been privileged to co-chair the Machine Learning and Artificial Intelligence subcommittee of the National Science and Technology Council (NSTC), which is run by the White House Office of Science and Technology Policy (OSTP). Very recently, OSTP elected to form the Select Committee on AI, with representation by the most senior representatives of various departments and agencies. Walt Copan, the Director of NIST, represents NIST on this select committee, along with France Cordova from the National Science Foundation (NSF) and a number of senior leaders from the other agencies.

Dr. Romine represents NIST on the Machine Language and Artificial Intelligence (MLAI) subcommittee. How that is going to relate to the select committee, which does the broad direction, is yet to be determined. People are paying attention to AI in two ways. One, AI has a lot of potential for improving how we try to secure systems by using machine learning or artificial intelligence to detect anomalies. Sometimes, it is possible to find things in data using automated reasoning that may not be found through human analysis.

Second, there is concern as to how to know whether the data that have been used to train a machine-learning or AI system, has been poisoned or tampered with. How will we know whether bias has been introduced? Every AI that's trained is going to be biased by the data it's exposed to. It's important to ensure that there is no bias that is inequity or iniquity.

There is some internal funding that has been re-committed to support some of these activities, and the hope is that AI and machine learning will become an important part of the overall ITL program and in cybersecurity.

The expectation is that the lab will have a lot of standards development activity. This is a supplement of some of the things the lab already doing. There will be some standards development engagement but there will also be some laboratory fundamental research to understand how the communication takes place, and how to secure systems in a way that still maintains the usability and seamlessness of IoT systems. There's some language in the senate markup that says cybersecurity is still important, and encouraging NIST to keep up its work in cybersecurity. It remains to be seen in 2019 whether the budget actually supports that.

Upcoming events include the NICE conference in November in Miami, and the Cybersecurity Risk Management Conference also in November in Baltimore.

Dr. Romine will be testifying before Congress on June 27th on cell-site simulators, IMSI catchers, Stingrays, and other similar technology. This is some of the work NIST has been doing for the last several years on the security of cellular communications. There seems to be some evidence that these things are prevalent in the DC area, and that's gotten the attention of Congress, and they'd like to hear more about what can be done about it.

US Government Use of Blockchains

Anil John, DHS

Dr. Joanna Chan, Data Scientist, NTIS DOC

Dr. Lauren Neal, Principal, Booz Allen Hamilton

The Chair welcomed Mr. Anil John of DHS, Dr. Joanna Chan of NTIS DOC, and Dr. Lauren Neal of Booz Allen Hamilton to the meeting to update the Board on U.S. government use of blockchain.

There is a lot of hype about government use of blockchain and it has continued to grow. The reality is more prosaic. The government interest in blockchain falls in three areas: security and privacy, integration approaches and gain/pain, and digital currency forensics.

DHS is a law enforcement organization. Research and development is separate, but there is interest in anonymous networks. Mr. John's group has worked on an execution model to support potential DHS blockchain operational deployments. The Science and Technology Division is working on a proof of concept for government use of blockchain using staged data and real use cases. DHS invested in six companies as a pilot to develop a customer driven proof of concept to identify integration points and gain/pain ratio.

A number of lessons learned came from the research. First, many blockchains are not actually blockchains. Next, most organizations do not need blockchains. Personal or private information should NEVER be written to a blockchain. Encryption algorithms have a life span. The chain will outlive the ability of the cryptography to protect the data. This can make sensitive information vulnerable. There are a variety of blockchains with a variety of security levels. Organizations should not start with blockchain, but instead start from

understanding its needs, then go to a blockchain if it is feasible to do so. Architecture and design cannot be side-stepped in the blockchain process. One must consider the integration points with existing environments. Interoperability is the challenge in the solution.

Multi-party distributed key management continues to be a challenge with blockchain. NIST can assist in this area. The proof of concept involves immutable logging to ensure resiliency, integrity, and independent validation of IoT devices and sensor data. One must be able to validate public data without putting it on the chain. The true question is, how to protect against anti-spoofing? The answer is, to have custom and broader protection and testing in a field setting. They used cameras at the U.S. border, but not actual camera data. Instead they used weather data and sensors. The cameras were pointed at non-sensitive areas.

The proof of concept involved streamlining and enhancing international trade facilitation. They want to operate without providing sensitive data in order to be able to release cargo internationally, etc. The proof of concept has applications to improve international passenger processing. Presently, enforcement at American customs abroad, takes place at physical lane controls. The question is how to associate people going through customs with their information that is needed by customs and still respect individual privacy? The goal is to move away from the physical credential to a digital one. Some form of id is needed without information physically leaking as is the case with a driver's license that displays the owner's information.

Interoperability must address architecture, protocol, payload, and policy aspects of any solution. Standards must be developed and informed by business driven proofs of concept. Interoperable decentralized identifiers, data exchanged standards, and distributed key management remain open problems.

The National Technical Information Service (NTIS) process facilitates between the agency and partner. They try to understand data challenges. Then, NTIS provides a problem statement and proposal package. They attempt to find the best solution to the challenges. Blockchain may be problematic, but potential use cases exist. Its advantage is information exchange without changing ownership of data.

IBM blockchain works with healthcare use cases. It facilitates activities between unrelated entities through a ledger. In 2009, during the H1N1 flu epidemic, information on the safety of the drug that was widely prescribed to fight the flu needed to be collected, analyzed and stored. The FDA used a real time app to collect data from hospitals. The FDA is looking at methods to share data rapidly during emergencies. Currently, they are working with 4 hospitals around the country. The hope is to expand partnerships with more hospitals by the end of the year.

Data must be secured, so IBM created off-chain cryptographic components. Access to this data is restricted. Data is never stored on the chain. Hospitals have different IT solutions. Everything is done in open source Ethereum. The app is scalable. File size is limited by disk size.

There were many lessons learned. Micro services architecture was used to avoid certain issues. They use Java, as it is more rigorous. There are a lot of misconceptions about

blockchain. They want a solution to work when time is of the essence. The research group is piloting out data. Blockchain keeps data distributed and more widely available.

Supply Chain Risk Management

Jon Boyens, NIST

The Chair welcomed Jon Boyens of NIST, to the meeting to update the Board on supply chain risk management (SCRM). Technology is interconnected and sophisticated and we are dependent on it. Speed and scale of globalization is increasing exponentially. Risk gets transferred down the supply chain to the end user who ends up owning the risk. The problem involves counterfeit products, hardware and software delivered with malware, vulnerabilities, insider threats, and poor quality.

Mr. Boyens worked to develop a NIST report on supply chain. It took four years. There is some misunderstanding of acquisitions and supply chain. Development of standards and practices has been ongoing since 2008.

There is greater awareness today than previously. Tools to support risk management activities are being developed. It has often been a circular approach. SCRM gets a lot of attention now. NIST has tried to put it in a technical and risk management perspective. NIST participates in the Committee on National Security Systems (CNSS). Guidance for security system supply chains was recently released. An assessment of IT systems was ordered for multiple agencies and entities that have connections with China. The Circular A-130 was updated. There was a roadmap item in the cybersecurity framework on supply chain risk management.

Currently, supply chain risk management is integrating into existing publications. The 800-161 is the most important publication on supply chain risk management. It places supply chain risk management into controls. Criticality analysis is being incorporated. NIST IR 8179 is the process document for critical analysis processes. It is extremely important as there is no other work on criticality analysis. Research on industry supply chain risk management principles continues. The goal is to make the research more useful across sectors and to the federal government.

NIST continues to look at emerging technologies such as blockchain. A big concern is provenance. There are a lot of tradeoffs. Criticality analysis becomes key in that instance. Public-private partnership is very important. There is a lot of angst in industry. NIST sponsors and co-leads the Software Assurance Forum. They meet three times a year and there are three thousand members currently.

Basic due diligence about organization supply chains is critical to security practices. Ultimately, if there is a reason for a lack of trust, there are no mechanisms to overcome the lack of trust in a potential supplier. Most importantly, there are no silver bullets where supply chain security is concerned. The question becomes, how to determine what's in or out of scope as far as supply chain management is concerned. Some aspect of scope must be part of SCRM. Early on, the intelligence community and defense were focused on the threat. Supply chain is difficult because intent is invisible. Back doors can exist because of poor

coding or malicious intent. Quality management and security were considered separate activities. They need to intersect at some point.

Risk Management Framework Update

Ron Ross, NIST

The Chair welcomed Ron Ross of NIST to the meeting to update the Board on Risk Management Framework activities. When the president signed the modernization strategy about a year ago, the OMB came to NIST to review NIST publications to make sure the content supports modernization. NIST took the task to look at five key publications. Mr. Ross will review the publications they were tasked with. There are a few others being tracked such as the FIPS-200 and FIPS-199. Those documents are going out for public comment. Mr. Ross will review deadlines and the schedule.

The president's modernization strategy consists of three main areas. They include transitioning agencies to shared services, moving to the public cloud, and protecting high value assets. Using shared services up to this point has been an exception rather than the rule. It's changing now because federal agencies must use the capability. Shared services is a great opportunity to save money and do better security. The same applies to the cloud with FedRAMP. The agencies comply with very strict federal security controls that are part of the authorization process in FedRAMP. It's another way for agencies to move some of the IT infrastructure either to a shared service or to the cloud. Agencies are still responsible to protect federal information.

This is all background on how the Risk Management Framework (RMF) is evolving in the context of the modernization strategy of the White House. The attempt is to reduce the level of complexity. It can't be eliminated entirely, but it can be reduced and managed. It goes with security engineering, which is a critical part of building trustworthy secure systems that will evolve over time. "Innovate", "simplify" and "re-automate" characterize how NIST views the regeneration of security standards and guidelines. The goal is to make things easier for customers and agencies to understand, as well as the private sector members that use the standards and guidelines. Every task in the framework is being examined to determine the best way to do that task, measure the output, and look for things that can be done better. Over the last year, they have talked to customers who are implementing the RMF at the working level.

With the Executive Order signed by President Trump in 2017, the Cybersecurity Framework became mandatory for Federal government agencies to implement. FISMA has always required NIST to develop the core set of standards and guidelines. It began with FIPS and the RMF and the security controls in 800-53. That's the foundation that has existed since 2003. Now, there is the Cybersecurity Framework.

The Cybersecurity Framework assists with communications. The functions, categories, and sub-categories work to provide a common dialogue with parties involved at all levels. Federal agencies must use the Cybersecurity Framework and the RMF. Communication is part of the overall decision on how much to protect; how many safeguards, how many security controls, how many privacy controls, and what's it going to cost. These are the

critical areas of risk management. Senior leaders must be involved because they must ensure the mission for the business.

Institutionalizing the core things like selecting common controls that can be applied across the enterprise, making sure there is a risk management strategy, and understanding the risk tolerance across an organization are all fundamental things that system owners can address.

The Cybersecurity Framework was the next big challenge. The Cybersecurity Framework was designed to do certain things. The Risk Management Framework was designed to do other things. The Cybersecurity Framework has risk aspects to it but they're different from the risks in the RMF.

The first task was to take them apart and figure out how they align. There's a strong alignment on the organizational prep-step that aligns with the identified steps in the Cybersecurity Framework. It sets the context of the organization including questions such as, how to manage risk, and what are the core missions and business areas to worry about.

What we're trying to do is allow organizations to execute the Cybersecurity Framework and the RMF at the same time, and get the good things from both frameworks that we can take advantage of. There is an authorization package in the RMF that authorization decision makers use to make that risk based decision. In that package, there is a security client which lists all the controls. IT includes the assessment of all those controls to see what needs to be improved with plan of action milestones. It allows senior leaders to see where certain vulnerabilities are clustering.

The big difficulty is controls in the RMF world are selected based on FIPS 199. Every system and every piece of data was categorized under FIPS 199 as, "high", "moderate", or "low". Those individual data categorizations end up being rolled up into a system level categorization. It's a starting set of controls for federal agencies. From there, they taper low controls, the moderate, and the high. It's done in FedRAMP by every federal agency.

Engineering concepts have come into the control selection world and the Cybersecurity Framework is one of the beneficiaries. Everyone will be able to use the massive control catalogue that's been updated in Rev. 5 and the catalogue of controls for security and privacy. There is no doubt, that privacy has always been important. Security has always dominated conversation, until recently. People realize now that there's a huge digital foot print on them, just because they're interacting with normal technology.

Privacy and security are combined in the 800-37. NIST is starting to integrate privacy into every one of its publications. The partnership with the Office of Information Regulatory Affairs (OIRA) came about because of several things related to privacy. NIST now works with them for all updates that relate to privacy in all of the publications being discussed today.

The 800-37 is the first document in the group. They evaluated every step for how privacy professionals use the same framework to select, implement, and assess privacy controls and came to some sort of an authorization decision. There is input from the security side and privacy side of the house.

In 800-37 Rev. 2, every word in the document was reviewed with the privacy team and with OIRA. The effort is reflected in the initial public draft. The comment period closes tomorrow.

The same thing is happening with the 800-53 Rev. 5. Privacy controls are fully integrated in a consolidated control structure.

Every place in the 800-160 life cycle was tagged with where that activity or task should be happening within the RMF. It is the first step to try to encourage agencies to take a more lifecycle oriented approach to security. OMB is supporting it because they are working on policies and guidance.

The second volume of the engineering series was just released about a month ago. It has to do with cyber-resiliency. It addresses not just the new systems being developed, but also what to do with the installed base that exists today. It provides guidance on how to apply security controls from 800-53 as cyber-resiliency controls. It looks at capability, intent, and who is being targeted. Those are the three characteristics that the intelligence community uses to assess adversaries. Once the determination is made, there is a list of resources to use to try to control damage in that situation.

There is a whole section in 800-53 on supply chain risk management. It's included in the authorization package. There is now a requirement to put that supply chain risk management plan in the authorization package. OMB must be able to put a policy out that controls how these two choices are used.

Privacy and security have a common nexus when it comes to confidentiality of Personally Identifiable Information (PII). Unauthorized disclosure of PII is a security issue, and a privacy issue. Privacy folks also worry about what authorized people can do. The catalogue of controls is not just for unauthorized disclosure for confidentiality, but also about what authorized administrators do with legitimate information they gather. It involves how much information they can collect, how they use it, what they are allowed to do with it, and how long they should keep it. These are all things to think of.

The 800-37 will be finalized in October, with one more draft in August. 800-53, Rev. 5 will be out in December.

National Initiative for Cybersecurity Awareness Update

Danielle Santos, NIST

The Chair welcomed Danielle Santos, Program Manager of NICE to the meeting to update the Board on the National Initiative for Cybersecurity Education (NICE) activities.

Since the last Board meeting, a new working group on apprenticeships has been added to the working group model. There are now six subgroups.

Apprenticeships have been discussed a lot recently in regards to workforce development as a way to get folks into the pipeline more quickly. Apprenticeships are a great way for high school students to get involved, and for college students to get hands-on experience while they're learning. Even transitioning veterans and current professionals who may be in IT but want to get into cybersecurity can consider apprenticeships as a means to achieve that goal. The introduction of the Apprenticeship group has been very timely as the Department of Labor has also been tasked, through an Executive Order, to lead the effort to create apprenticeships in cybersecurity.

NICE goals are intended to support expanding the cybersecurity workforce. There are three goals: to accelerate learning and skills development, nurture a diverse learning community, and, guide career development and workforce planning.

Florida International University (FIU) and New America have been awarded grants to lead the stakeholder engagement program, focusing on the NICE conference in Miami in November, and the K12 conference to be held in San Antonio, TX in December. NICE works across all U.S. states via the Association for Career and Technical Education (ACTE) conference that brings together all U.S. programs. The hope is to have some of those attendees come to the NICE Conference.

NICE has an inter-agency coordinating council that includes the Department of Education. The council worked on the report to the President for Executive Order 13800. NICE and the Department of Commerce were tasked in two areas: assess the scope and sufficiency of efforts, and, make recommendations. Inter–agency groups met over the last year to examine how to expand cybersecurity awareness. A request for information was issued to the public, and a workshop was held last August. The report is posted on the web.

Key messages from the report include: a strong cybersecurity workforce is needed and is critical to current and future national security, and, to be better able to identify, recruit, develop, and retain cybersecurity talent.

Current numbers of open positions show the gap between open jobs and people needed to fill them is getting worse as more jobs are open now in cybersecurity than earlier in the year. It's anticipated the trend will continue for the next few years. The need for people is still increasing faster than the pace of people entering the field. The report provides recommendations that will require commitment and resources from the public and private sectors.

The report contains imperatives, recommendations and actions as well as appendices.

Imperatives include:

- Launch a national call to action to draw attention to, and mobilize public and private sector resources to address cybersecurity workforce needs.
- Transform, elevate, and sustain the learning environment to grow a dynamic and diverse cybersecurity workforce.
- Align education and training with the cybersecurity workforce needs of employers and prepare individuals for life long careers, and,
- Establish and leverage measures that demonstrate the effectiveness and impact of cybersecurity workforce investments.

Recommendations include:

- The Federal government should lead in launching a high profile national call to action.
- The administration should focus on and recommend long term authorization and sufficient appropriations

- Federal agencies must quickly address major needs relating to recruiting, developing, and retaining cybersecurity employees and continue to implement the federal cybersecurity workforce strategy and FCWAA of 2015.
- Recognize and encourage opportunities for re-training. Build on and strengthen experiential and work-based learning approaches.

There is also a deficit of instructors teaching cybersecurity. Increasing the number of instructors who teach cybersecurity will increase the number of students with knowledge who can fill positions.

In the report, recommendations are grouped with corresponding actions. Broader application of the NICE Framework may assist with implementing recommendations. NICE is working with DHS on performance indicators for cybersecurity jobs. Feeder roles, as identified by CyberSeek, can play a greater role in filling jobs by using existing skills. Feeder roles can be used to identify people in the traditional IT workforce who may be able to transition into cybersecurity based on their current roles.

NICE has started to convene the authors and interagency group to review the imperatives and determine who has ownership, identify current progress, and also identify priorities for immediate actions and long term steps.

Social Engineering Awareness and Training

Toney Rogers, HHS
Michelle Stephens, NIST
Mary Theofanos, NIST
Kristen Greene, NIST

The Chair welcomed Toney Rogers of HHS, and Michelle Stephens, Mary Theofanos, and Kristen Greene, all of NIST to the meeting to update the Board on Social Engineering Awareness and Training.

The presenters represent NIST's usability group. The group members are different than most usability groups in the federal government in that they are not all computer scientists and engineers. There is a multidisciplinary aspect of the group that includes social scientists, particularly psychologists, human factors experts, sociologists, and cognitive scientists, who work together daily and bring together these multiple perspectives and disciplines to problems. That combined perspective has allowed the group to reach conclusions that are deeper and have more breadth than what would be possible coming only from a computer science or engineering perspective.

Phishing is an ongoing problem in organizations. Context is critical to phishing effectiveness. Usually, if the content is relevant to respondents personally, they may be more likely to click. NIST uses embedded phishing awareness training. Embedded phishing training utilizes simulated emails that mimic real world phishing examples and capture click rates. If someone clicks on one of the simulated emails, they get a screen saying this is not a real phishing attempt and how to distinguish phishing attempts better in the future.

After 4 years of studying click rates, they could not explain why click rates are so variable. It was necessary to collect some additional data to try to make sense of what was going on.

They did three phishing exercises per year with variable timing. They wanted to determine why people click. A survey was done to get people to explain why they click on links in phishing emails. In their responses, users explained what tipped them off to a phishing attempt, or, what made them click a link. Click rates work with reporting rates. Why people click and why they don't click are important. User context is very key in the determination to click or not click. Click rates tend to spike when the emails are targeted.

A voicemail exercise, an unpaid invoice, and an order confirmation were used as tests. The voicemail example spoofed the real voice mail process. The unpaid invoice example mimicked the real world ransomware that was going around at the time. There was a mismatch between the document type mentioned in the email and what was actually attached. The unpaid order came around the time of the holidays when people were doing more online shopping.

They found that the perspective of clickers versus non-clickers varied quite a bit. Non-clickers tended to notice circumstances that did not align with their personal situation, and when that happened they tended not to click on links in those emails. They were suspicious right away. Clickers tended to believe the consequences of clicking would be worse for them if they did not click the link. Clickers focused on what makes the email believable rather than on cues that the email may be false. If a message didn't fit the expected profile for a phishing attempt (it didn't ask for personal information or passwords), it became more believable. The researchers also noted an over-confidence in the NIST firewall to block phishing attempts, meaning, if it came through the firewall, it must be ok.

The research has clarified how important context becomes in the situation where emails are targeted to specific agencies. Click rates can spike to fifty percent because the context in the email is targeted that well. Being a partner with users, raising awareness of the changing nature of phishing attacks, and making sure staff are not overly confident in institutional security, are important ways to prevent real mistakes. Reporting time is important. It shows whether staff is reporting emails sooner.

The group intends to continue expanding its work. This included collect and analyze additional operational data; examine balancing phishing awareness and security fatigue, and collect operational data for a cognitive decision model.

In order to change behavior, they break down emails and point out clues that show it was a phishing attack. There are also lunch sessions where they break down threats to demonstrate clues. The effort to change behavior must be comprehensive. Continuing phishing exercises have been shown to decrease click rates. There are also phishing attempts to high value assets. Senior management is often more concerned with looking bad, and avoiding reporting. The focus should be on better end results such as not clicking on sophisticated attempts.

NIST Update

Matthew Scholl, NIST

The Chair welcomed Mr. Matthew Scholl of NIST to the meeting to update the Board on NIST activities since the last Board meeting. NIST recently underwent the National

Academies of Science review for multiple divisions. They reviewed the Mathematics Division, the Advanced Networks Division, the Applied Cybersecurity Division, and the Computer Security Division. The results of the review are not available yet.

Since the Board last met, work has started in post-quantum cryptography and standards. There was a workshop in Florida where submitters presented work to NIST. The workshop entries are down to sixty-nine submissions in the competition.

Phase 2 is about to start for post quantum cryptography submissions. In Phase 2, evaluators will be looking at the continued cryptanalysis of the submissions, and performance key management. Size, speed, efficiencies of quality and implications will also be evaluated. NIST will work with academic institutions, universities, and some commercial organizations in implementing the submissions in both hardware and software on certain test batches in order to measure these implementations against each other.

Work has started to standardize what's being referred to as lightweight cryptography. It's not as formal as post-quantum but there is great potential. They are looking at very small, power hungry, resource constrained IT devices that need encryption.

They have implemented black box test tools, and put them out as open source to industry. Industry has tested and returned the results back to NIST. This model is different than what has been done in the past, using a third party for testing. It's been much faster and the results have been encouraging. The National Vulnerability Database (NVD) has been identified as a critical national resource by the NRC. Information coming into the database has great value.

The privacy program is growing. Privacy work that's happening in light cryptography is being extended. Privacy is being incorporated into NIST publications. A privacy part to NICE may possibly be developed. There is continuing research on new and emerging technologies. They will be examining what guidance is needed in these new areas. The challenge is to raise the awareness of what's being done in IoT.

A preliminary finding from the review was to communicate NISTs work effectively. The framework has provided ways for people to think of, and communicate about, these issues. There is possible legislation for NIST to develop guidance for agencies.

NIST continues its research into immersion technology areas, 5G technologies, and participates heavily with 5G, 3G, and standards bodies. Virtual reality is being looked at, and how that enhances NIST's capabilities. However, virtual reality has potential security and privacy issues surrounding it as well. Some of these immersion technologies might be important in the future.

There are new builds at the NCCoE. There will be a privacy workshop next month. Cybersecurity Framework 1.1 has been published. A workshop on the 1.1 version will be held in November to find out how it's working. NIST is looking at expanded use of GITHub. The Computer Security Division now has 85 NIST staff and pathways student interns, 15 guest researchers and others. Twenty-seven percent of staff are now eligible for

retirement, with 7 percent more in the next three years. NIST has staff at the University of Maryland, Penn State, UC Berkeley, and the University of Louisville.

Review of Thursday Briefings

The following areas were reviewed by the Board at the end of Thursday's session:

- The Board was interested in a deeper dive on blockchain implementations. An additional presentation is slated for Friday. The Board opted to continue the discussion on blockchain Friday.
- There needs to be some way to organize supply risk management activity. How can the board weigh in? It is very widely discussed right now.
- Is a different approach needed for NICE? There are many events and activities with the same conversation happening, and the gap of people needed for jobs is getting bigger. Is it a problem of scale? The effort is constrained on the budget side. There are a lot of events and promoting security awareness. It needs more funding. The program is doing what it can with what it has. There is a need to increase the number of tech people on boards. The question is how to have a broader culture of cybersecurity.

Public Comments

There were no public comments.

Meeting Recessed

The meeting was recessed at 4:06 p.m., Eastern Time.

Friday, June 22, 2018

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

Legislative Activities in Supply Chain Security

Sean Farrell, House Committee on Energy and Commerce
Tiffany Angulo, Legislative Blockchain Caucus

The Chair welcomed Mr. Sean Farrell from the House Committee on Energy and Commerce, and Ms. Tiffany Angulo from the Legislative Blockchain Caucus to the meeting to update the Board on legislative activities in supply chain security. Supply chain threats and vulnerabilities are a big concern for the government and the private sector. Last year, members of the House and Senate Intelligence Committee sent a letter to FCC Chairman Ajit Pai, highlighting concerns with certain suppliers in the supply chain. A few months later, Chairman Pai issued a notice of proposed rulemaking (NPRM) to examine the issue in more detail.

Initially, the NPRM was to look at telecom providers in the U.S. who use Universal Service Fund (USF) money, to determine whether or not a provider should be denied USF funds if money was being used to purchase from certain suppliers that are deemed to be risky. It became a review of the entire telecom sector. Similar letters went to the Departments of Agriculture and the Federal Trade Commission (FTC).

It's not generally known, but the Department of Agriculture has its own broadband network for rural areas. Agriculture came under pressure to use resources more efficiently. In rural areas, the economics of building broadband and maintaining it in sparsely populated areas is very difficult to meet. There is pressure to have less cost at the tradeoff of using a trusted supplier that may cost more. In addition, military bases often are located in rural areas. Funding these bases brings attention from the Armed Services Committee. It creates some tension in the budget area.

Energy and Commerce recently released a discussion draft for the reauthorization of the National Telecommunications and Information Administration (NTIA) who fall under the jurisdiction of the Department of Commerce. The NTIA goal is to have NTIA play a larger role in dealing with supply chain risks.

Ms. Angulo works with Congressman David Schweikert, Co-Chair of the Congressional Blockchain Caucus. The third blockchain round table was held this week. They discussed uses of blockchain with representatives from industry and government on how government can assist. There were about 50 attendees.

There is a lot of activity on blockchain. The purpose of the caucus has been to educate members on the Hill and their staff about the potential of blockchain, and move beyond talking only about the cryptography, to the technology and potential uses for blockchain. The caucus is taking a lighter touch at present when considering regulation. They want to make sure they're not regulating the technology.

NIST has been trying to develop foundational terminology so that people can have discussions. Privacy and security also need to be considered. There is also a need for standardization of wallets. NIST is also concerned with cryptography, and looking at the

lifecycle of the blocks. Most blocks are not quantum safe. States are very concerned with this area. NIST's work has been more in the area of providing basic descriptions of the technology.

The caucus has become the intermediary in talking with businesses. States have passed laws to encourage use of blockchain technology. The concern is that there will be a patchwork of laws on blockchain across all the states. States are looking for assistance from federal government with the technical aspects of blockchain. NIST publications have some guidance recommending quantum safe solutions, but no standards exist. A document is coming this summer.

When legislation is targeted at particular companies, it is a problem. It can be a lost opportunity to have an influence on the sector. An example is ZTE (phone manufacturer) when it was heavily fined, its board of directors was fired and replaced, and the company essentially ceased sales in the U.S. When these types of events occur, consumers then lose the ability to update their phones.

Congress is trying to deal with making changes more broadly. Software updates are a challenge. Sharing information is a better way to mitigate threats. Government sees threats the private sector does not see, and the private sector may have knowledge of certain types of actions before the government.

OMB Cyber Office Update

Jordan Burris, OMB EOP

The Chair welcomed Jordan Burris, Senior Advisor in the Office of the Federal CIO to the meeting to update the Board on OMB Cyber Office activities over the last year.

In May this year, the Risk Determination Report was published. It provides the OMB assessment of cybersecurity risk management across the federal government along with recommendations or actions to address the most mission-critical cybersecurity gaps. The report highlighted four gaps or areas where work was needed. Those areas are: limited situational awareness, lack of standardized IT capabilities, limited network visibility, and lack of accountability for managing risks.

It was noted in the report that 38 percent of federal cyber incidents did not have an identified attack vector. Only 59 percent of agencies reported having processes in place to communicate cybersecurity risks across their enterprise. While most users have the PIV credential, the report found that not all ICAM programs were at the same level of maturity, and there was a need to make more effective use of the groundwork that has been laid.

Nearly half of agencies had issues with detecting and whitelisting software running on their networks. These visibility issues persist across federal government networks. In addition, only 27 percent of agencies had the ability to detect and investigate attempts to access large volumes of data. Finally, 16 percent of agencies eschew the government-wide targets for encrypting data at risk and highlighted challenges within their enterprise for elevating cybersecurity concerns.

OMB and DHS are working to address gaps. DHS is working on improving GovCAR. OMB, working with GSA, are finalizing requirements related to helping organizations acquire

security operations center as a service. The goal is to have a number of security operations centers that can lead, and have agencies work with those centers. For these efforts, OMB will be working to fund gaps.

They also look to mature the High Value Asset (HVA) program. The HVA program falls under DHS Binding Operational Directive 18-02. DHS, OMB, and GSA are working collaboratively to refine the highly-adaptive cybersecurity services (HACS) special item numbers (SINs) under IT Schedule 70. An RFI was released recently with a June 23rd end date for receiving public feedback. HACS SINs are meant to augment the capabilities that DHS has, and allow agencies to get these assessment services provided by the private sector.

More work is needed in identity management. A draft of the OMB identity credential and access management policy was released for public comment. The public comment period has closed and they received 500 comments. Mr. Burris's team is in the process of reviewing and adjudicating the comments. The new draft policy will address continued expansion of digital services in the federal government and specify protections for digital identities within agencies with additional focus on physical and logical access. There are additional opportunities to further work that is already being done.

NIST, GSA and OPM are core contributors to identity management. We look to increase partnership across agencies. There must be enterprise focus on identity management and other areas. The report notes improvements where they have happened. Metrics are available on performance.gov.

OMB works closely with NIST on standards work and prioritization. There is ongoing dialog. Executive Order 13800 directed agencies to use the framework. It's not a shift but more creating alignment with what has been done and the framework itself.

Blockchain Uses for Government

Victoria Adams, ConsenSys

The Chair welcomed Victoria Adams from ConsenSys to the meeting to brief the Board on blockchain uses for government. ConsenSys is a blockchain software technology company with 1,000 people in 22 different countries with major hubs in London, New York, Dubai, and Singapore. They develop blockchain technologies, and the company emerged from the team that developed Ethereum. ConsenSys is a venture production studio, building decentralized applications and various developer and end-user tools for blockchain ecosystems.

Their work covers five major areas: solutions, infrastructure, capital, products, and education. Ethereum is a social engineering tool. It is a means to accomplishing goals. One of those goals is building blockchains. ConsenSys has a D.C. office to work with government. ConsenSys works to understand government, and to advocate for blockchains with government. The big challenge in government is legacy systems. Legacy systems create substantial inertia in moving to new solutions. There is a lack of understanding of the potential in blockchain.

Blockchain is difficult to explain to people. The basics are just beginning to be understood. There are three types of people interested in blockchain, the "blockchain curious", those

who are mainly interested in the regulatory aspect; the "blockchain enthusiasts", those that have done a bit more, and learned something about it. The third type is the "social engineer". These are the people who want to explore blockchain.

There is a lot of interest in blockchain and its possible use for supply chains. The return on investment for supply chain is low if the suppliers in the chain are trusted. It is ideally suited to consortium situations where there are confidential transactions between purchasers and suppliers. An example of a consortium is Walmart and its suppliers. Walmart may choose to deal with individual suppliers on a confidential basis.

Manufacturer use of blockchains may not have much return on investment. In cases where admission to the supply chain is highly restricted, blockchain may not be worth it. Aircraft manufacture supply chains and pharmaceuticals are examples of highly restricted supply chains. Digital designs may be an area within these realms where it makes sense to have blockchain. Intellectual property and copyright are other areas where it may also make sense.

Incentivized supply chains may work for industry but questions arise for government use. Newcomers buy Ethereum tokens in the chain. The cost for the token is high enough to remove the incentive for any participant to cheat. Fees paid by all entities are escrowed. As shipments clear each stage, and if the shipment is confirmed to be contraband free, then the tokens remain in escrow. At delivery, the tokens are returned. When contraband is found, the finder gets all the tokens put in the chain. It becomes a micro-economy to incentivize good behavior.

There are questions clients need to ask when considering blockchain:

- Will increased security make a difference?
- Do we need transparency, or increased auditability and auditable record?
- Must it be tamper proof?
- Faster order and payment processing needed?
- Greater trust with stakeholders?
- Incentive systems possible?

ConsenSys turns down 90 percent of requests. They spend a great deal of time working with people to identify and understand problems to determine if blockchain is feasible. It is a multi-step process. Users start with a business problem and determine if blockchain will work to solve that problem. Thinking it through ahead of time helps to determine if there is a use case.

Working with incentive systems has been of interest. Some government applications may include voting by mail. Some other interesting government areas include healthcare, medical records, advising, and software licensing. They had discussions with Treasury about reconciling interagency transfers. Currently, there is 1.7 trillion dollars of unreconciled money on the government's books. Blockchain would help with this situation.

Can business processes be re-conceptualized with blockchain? Blockchain can assist with determining ownership of property so that the owner gets paid for their intellectual property. Images are registered on the chain. Contracts are registered on the blockchain. Blockchain is used to track sales, make payments, and trace ownership through the chain.

ConsenSys is working with simpler cases to prove the technology can work in a privacy context. They are working with smart contracts. Public and non-public chains may be replaced by confidential and non-confidential transactions. Confidentiality needs to be built in somehow.

Attestations are a problem when blockchain is used for identity. In Switzerland they are registering identities on the blockchain. Data is not on the chain. Every transaction is on the chain. The chain identity is secure, but it doesn't stop errors by the owner. The individual owns their data, and can see whenever it has been touched. There must be permission to touch data. Owners can stipulate data be managed on blockchains as a condition of use.

Can blockchain improve the underlying security of the internet? The internet was designed as a messaging service between trusted partners. Security architecture must be built on top of the messaging systems. Now, the internet uses communication between untrusted parties. ConsenSys has experts in other areas that may be of interest to the Board.

Supply Chain Risk Threat Briefing

Joyce Corell, Office of the Director of National Intelligence (ODNI)

The Chair welcomed Joyce Corell of ODNI to the meeting to brief the Board on supply chain risk threats. Ms. Corell works in the National Counterintelligence and Security Center. She works with foundational areas rather than day to day research and has government wide authority. ODNI was established by Congress. The National Insider Threat Task Force is part of the organization. They work a number of security issues, such as setting the standards on security practices for companies that do classified work for the government, requirements for cleared defense contractors, and associated security roles. Ms. Corell is the assistant director for the supply chain directorate. They assist the intelligence community with doing supply chain risk management.

A critical infrastructure task force was developed a year ago to work with critical infrastructure sectors. They also collaborate with DHS. Risk management to the government often involves buying goods or services. Acquisition as a process involves cost, schedule, and performance. Performance is about security and integrity. Security needs to become the fourth pillar of acquisition. "Integrated Risk Reduction" must be a team approach.

The government is looking at ways to increase risk management. It is looking at how to mandate better supply chain risk management. Many portions of the government are interested including the armed services and homeland security committees along with the House Science and Technology Committee. Draft legislation has been written to create an acquisition security council. There needs to be a more public discussion on security and what it means.

The supply chain directorate has been trying to have conversations about what is the continuum of examination when dealing with a third party. What information determines

decisions in that context: There can be either a, "yes, we will deal with you", or, "yes, but with conditions", or "no". Some of the reasons why people won't say "no", may be because there is a perception that they can manage their risk through contract language. Some people believe constant monitoring is sufficient. In cases where there is strong evidence of wrongdoing, it can become a matter of the number of people involved for industry to determine they won't deal with a specific organization.

The Department of Defense has moved from a compliance-based mindset to a risk-based mindset. There must be an understanding of risk exposure. The dynamic needs to shift so that companies can create ways for shipments to arrive uncompromised. In that scenario, security moves from the loss column to the profit column. They are working with defense and congressional committees on ideas that represent the right collections of tools that can be used. Is regulation useful? Stability and predictability are desirable qualities. In the next 18 months, regulatory proposals will be coming out. Security must become part of "technically acceptable" acquisitions.

Increased risk and increased attention from authorities has resulted in being much better at hardening the perimeter. Bad actors will find and take other ways. From a cybersecurity adversary perspective, there are still many people in the government who will click on anything. The tools that improve people, are people. The risk continues to increase.

Robust commercial due diligence needs to be encouraged. Many organizations do not have healthy risk management actions. The threat landscape changes over time. The Communications Security, Reliability and Interoperability Council (CSRIC) report focuses on processes. It recommends institutionalized processes that account for risk and support improved security in the face of those risks.

Small Business Cybersecurity Programs

Rosario Mendez, FTC
Andrea Arias, FTC
Nelson Hastings, NIST

The Chair welcomed Ms. Rosario Mendez and Ms. Andrea Arias of the Federal Trade Commission, and Mr. Nelson Hastings of NIST to the meeting to update the Board on small business cybersecurity programs. The Consumer and Business Innovation division at FTC publishes consumer education materials. Ms. Arias is an attorney working in the Division of Privacy and Identity Protection. They work with the Division of Consumer Education to raise awareness about privacy and data security. The FTC's mission is to protect consumers and promote competition. Law enforcement, consumer education, and policy are the main tools to promote the mission of the FTC.

Ms. Mendez's division is working on developing visual materials for small businesses. There are a variety of tools to educate small businesses including free print publications, business blogs, a special blog series, website, webinars, outreach, partnerships, presentations, and regional offices.

"Start with Security" is the centerpiece of small business education on data security. It gathers the top ten lessons learned from the more than 50 data security cases brought by the FTC over the years. It breaks down what businesses need to do to improve their data

security in a basic way. There are ten actionable steps in the guidance, and videos with guidance on the website. They did workshops around the country on the guidance, which was well received. Four hundred thousand publications were distributed to small businesses in 2017.

There is a data breach response guide for business. The guide includes sample letters and steps for that situation. The framework was mapped to the fifty steps in the guidance and lessons learned. The "Stick with Security" series goes into more detail, focusing on lessons learned from recent cases.

The website Busness.ftc.gov has literature online. It is free to order. Ftc.gov/small business also has information on scams that target small businesses as well as cybersecurity tips. The FTC partnered with the National Cyber Security Alliance (NCSA) and the Small Business Administration (SBA).

Small business is defined as companies with less than 500 employees. The goal was to work with the smallest businesses, meaning 10 people or less. Small businesses are concerned about cybersecurity but don't know how to address the issue. They are concerned about human error. Small businesses need help training employees, and want one unified message from the government.

The FTC has developed a draft small business fact sheet. It is a new cybersecurity for small business education campaign with 12 topics. The topics represent the most common concerns of small business including such areas as, phishing, ransomware, questions about the NIST Cybersecurity Framework, and Wi-Fi security. Mobile security was also important. They created twelve topics, each with a one-page, two-sided fact sheet. The hope is other agencies will decide to co-brand the fact sheet in order to present a unified message from the government on cybersecurity. The FTC is also partnering with the insurance industry to develop a fact sheet on cybersecurity insurance with guidance for small business.

NIST has focused on small business for many years. It starts with partnerships. NIST is partnering with the Small Business Association (SBA) and the FBI InfraGard program to look at different ways to provide educational materials, and looking at self-service methods of providing materials. FTC is also creating starter profiles for small businesses, with common business practices and objectives for small businesses. Work in this area will continue during 2018.

Board Review and Discussion

Chair and members of the Information Security and Privacy Advisory Board

The Board reviewed and discussed the following items:

1. Meeting dates for the fall Board meeting were proposed for November 1-2 at American University in Washington, D.C.
2. Chris Boyer will draft a letter on standards for the Board to review.
3. A new national initiative related to privacy. Put privacy into the NICE effort. Privacy is now in publications, but there is a shortage of people who can implement privacy. Marc Groman will start a draft.

4. Need for leadership in the area of the Internet of Things. The challenge is how to demonstrate progress on standards and assist leadership internationally.

Meeting Recessed

The meeting recessed at 4:30 p.m., Eastern Time.

List of Attendees

Last Name	First Name	Affiliation	Role
Scholl	Matt	NIST	DFO / Presenter
Brewer	Jeff	NIST	Assistant DFO
Adams	Victoria	Consensys	Presenter
Angulo	Tiffany	Legislative Blockchain Caucus	Presenter
Arias	Andreas	FTC	Presenter
Boyens	Jon	NIST	Presenter
Chan	Johanna	NTIS DOC	Presenter
Corell	Joyce	ODNI	Presenter
Dodson	Donna	NIST	Presenter
Farrell	Sean	Committee on Energy and Finance	Presenter
Greene	Kristen	NIST	Presenter
Hastings	Nelson	NIST	Presenter
John	Anil	DHS	Presenter
Mendez	Rosario	FTC	Presenter
Neal	Lauren, Dr.	Booz Allen Hamilton	Presenter
Rogers	Toney	HHS	Presenter
Romine	Charles, Dr.	NIST	Presenter
Santos	Danielle	NIST	Presenter
Stephens	Michelle	NIST	Presenter
Theofanis	Mary	NIST	Presenter
Dhanoa	Harsimar	AT&T	Visitor
Evans	Alison	Lewis-Burke Associates, LLC	Visitor
Heyman	Matt	Impresa Management Solutions	Visitor
Klaassen	Lindsey	US Chamber of Commerce	Visitor
Suh	Paul	USPS OIG	Visitor

Last Name	First Name	Affiliation	Role
Tupitza	Charlie	Right Exposure	Visitor
Wright	Bill	Symantec	Visitor
Baksch	Mariam	Inside Cyber	Visitor/Media
Franco	Joseph	MeriTalk	Visitor/Media
Friedman	Sara	GCN	Visitor/Media
Geller	Eric	Politico	Visitor/Media
Sobczak	Blake	E&E News	Visitor/Media
Drake	Robin	Exeter Government Services	Staff
McConnell	Andy	Exeter Government Services	Staff
Salisbury	Warren	Exeter Government Services	Staff