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 29, 30 and 31, 2017

National Press Club Building, 14th St. NW 13th Floor
Russell Senate Office Building, 1st and Constitution, NE Room R-253
Washington, D.C.

***Please note: Speakers/times are subject to change without notice**.

Board Members Chris Boyer, AT&T, Chair, ISPAB John Centafont, NSA Greg Garcia, Signal Group Patricia Hatter, Intel *(March 29-30)* Toby Levin, Retired Ed Roback, US Department of Treasury *(call-in March 31)* **Remote Participation** David Cullinane, Security Starfish, LLC *(March 29)* Jeffery Greene, Esq., Symantec Corporation Gail Stone, Social Security Administration *(March 29-30)* **Absent with Regrets** Annie Antón, Georgia Institute of Technology J. Daniel Toler, US Department of Homeland Security	Board Secretariat and NIST Staff Matt Scholl, NIST, Acting DFO Robin Drake, Exeter Government Services, LLC Warren Salisbury, Exeter Government Services, LLC

Wednesday, March 29, 2017

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

Welcome and Remarks from the Chair

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

The Board members provided brief updates on their activities since October, 2016.

Mr. Boyer has been involved in quite a bit of activity in the internet of things (IoT) space. AT&T has been deeply concerned about IoT devices as a factor for DDOS attacks. They have been working with the Consumer Technology Association, helping them develop some best practices, or standards, for devices that potentially may be rolled out. The IoT continues to be a primary concern.

On the critical infrastructure side, AT&T is doing a lot of work on integrating with the Automated Information Sharing (AIS) portal. We just published a Federal Communications Commission (FCC) report for the communications industry on information sharing and recommendations on how to do more sharing within the sector and how to possibly implement enhancements to the Communications Information Sharing and Analysis Center (ISAC). That report was published in March. Mr. Boyer was the chair of that effort. It is a 40-page report on what the industry is doing today and what could be done differently.

Improving information sharing and dealing with IoT are two top-of-mind issues we're talking about. The National Security Telecommunications Advisory Committee (NSTAC) is focused on a report for the Emergency Technology Strategic Mission, which is looking at new technologies and equipment directives for National Security Emergency Preparedness (NSEP) – type issues. The group is also trying to work with the new administration. The Board will hear more tomorrow about what they're going to be focusing on.

The new administration is going to launch an initiative concerning botnets and botnet mediation. It's a continuation of some of those efforts, it should be a major initiative once it kicks off, possibly sometime this summer. There are discussions with the electric industry about cross-sector preparedness for cyber incidents. Needless to say, there is a lot of activity going on.

The March report was part of the FCC Communications Security, Reliability and Interoperability Council (CSRIC). There were reports on cyber security, Wi-Fi security, information sharing, supply chain best practices, and a report on cyber security workforce. They're all recommendations for what the industry, the FCC, or government could be doing in these topic areas. Mr. Boyer chaired the group on information sharing. It mainly documented what the industry is doing. The process of actually writing it down was important. The group also identified some areas where the industry could do a better job. The group tried to crystalize current activity and areas to improve.

Welcome and Remarks - NIST

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

The Chair introduced Dr. Charles Romine, Director of the Information Technology Laboratory (ITL) at NIST, which houses all the cybersecurity activities for NIST. Dr. Romine is updating the Board on the ITL's ongoing activities and NIST in the broader sense. Dr. Romine expressed his gratitude to the Board for its work on behalf of NIST, and its input and advice on many topics.

Dr. Romine discussed some recent organizational changes that have happened at NIST and Commerce, as well as some legislation that affects the agencies that was signed into law in January. There is a new Secretary of Commerce, Mr. Wilbur Ross, who was confirmed in February. We've had the opportunity to acquaint Secretary Ross with some of the work that we do at NIST and we expect that engagement to be ongoing. Mr. Adam Sedgewick, a member of Dr. Romine's staff, is the NIST detailee to the new Secretary, advising on technology policy. There are some changes within NIST. Dr. Kent Rochford is the lab programs lead and Acting Director of NIST.

There have been some changes within NIST. Dr. Kent Rochford is the acting Director. His permanent position at NIST is the Associate Director of Laboratory Programs, but he is currently acting as the Director of NIST. Ms. Laurie Locascio, the Material Management Labs Director, is now acting in Mr. Rochford's stead. Mr. Mike Fasolka is now the acting Material Management Labs Director. Ms. Mary Saunders, the Associate Director for Management Resources retired a few weeks ago. The CIO of NIST, Del Brockett, is acting in her area as acting director (AD) of Management Resources until a replacement is found.

Dr. Romine had no detailed budget information to present to the board. The current continuing resolution is slated to end on April 28th.

There is also no update on the pending cybersecurity executive order. It's been reported in the press that the White House is working on an executive order for cybersecurity. There is a lot of care and attention to detail that's being put into the executive order. Mr. Rob Joyce is scheduled to speak tomorrow on the executive order.

Every federal agency and private tech organization in the area of cybersecurity is competing for top talent and the best minds that we can find. It becomes particularly challenging at a time when there's a federal hiring freeze. Like every other federal agency, NIST is covered under the hiring freeze. There are exception categories in the executive order. Two of those are hiring for national security and public safety purposes. NIST is seeking clarification from the Department of Commerce on what types of positions are considered exceptions and which are not with regard to national security. It's not known how much flexibility there is for hiring in the area of cybersecurity.

There are a couple of programs that may have statutory or other authorities besides what the executive order explicitly says. Research agencies may have such authorities. Many research agencies have worked with the National Research Council (NRC) that manages the national academics and other programs, to implement a postdoctoral program. In statute, NIST actually has a requirement for having an NRC postdoctoral program. It is one avenue to recruit early career, postdoctoral level staff. NIST seeks ways in which it can ramp up participation. Historically, NIST has not been as vigorous as perhaps it should have been in competing for NRC postdoctoral candidates. We are trying to revitalize this program with a lot of energy since it is carved out that we have authority to do recruiting.

Over the last couple of years, NIST has sought to intensify its engagement with academic institutions, particularly BA and minority served institutions. If nothing else, faculties will continue to be aware of NIST and understand the mission it has. Dr. Romine is still focused on ensuring that the word gets out. These are the two things that NIST can do, even under the hiring freeze.

The legislation signed in early January did a few things for NIST. It called out the NIST director as the President's principle advisor on standards policy. It changed the Hollings Manufacturing Extension (MEP) cost sharing ratio from 2:1 to 1:1. The states and territories establish centers for MEP throughout the country. It calls on NIST to develop a strategic plan that addresses interactions with stakeholders, including academic international researchers and industry. It also addresses the relevance issue with commercial and industrial applications. These areas are related to insuring NIST relevance in the future.

Continuing to raise awareness of the value and importance of industry-led cybersecurity standards and best practices for critical infrastructure is directly relevant to NIST and the Board. It continues the role that started with Executive Order 13636 in the last administration, and was put into legislation thereafter.

It calls on NIST to continue to work on security for the voting systems. There is some discussion later in this meeting on voting as a critical infrastructure. It calls on us to continue to do research in our future of information systems, having to do with cybersecurity needs for quantum information systems, including quantum resistant cryptographic standards. It calls on us to look for gaps in techniques for providing the information security gaps in reviewing the challenges and identifying deficiencies that are unidentified by other agencies or by NIST. And finally, this really interesting one on evaluating the effectiveness and sufficiency of federal agency implementation of standards and guidelines.

NIST is working in collaboration with agencies to identify areas where implementation may be subject to improvement. The dialogue continues with other agencies about the sufficiency of our guidance and how well it's suiting their needs. There's this ongoing dynamic tension for us because NIST is a metrology institute. Measurement is our mission in many ways. But measurement, as it relates to accountability, is different than measurement for scientific purposes. We really think this conversation with the agencies on how they are approaching their risk management should be, from our perspective, "How can we be helpful in helping agencies be more effective in risk management."

We're looking for feedback from agencies on the utility of the guidance we provide and areas where we can work with agencies to help improve that guidance so that it is more actionable, so that they improve their risk management overall. NIST is not the accountability side. NIST is the "work on making risk management across the federal government better" side. The accountability function already exists and is vigorous in the attorneys general (IGs) and in the Government Accountability Office (GAO). It points more toward improving the overall risk management for agencies as an approach.

NIST has also announced an update of the industry cybersecurity framework, now Version 1.1. Areas that were called out originally were included. When we released the first industry framework for critical infrastructures, we also had an ancillary document that detailed some other things that we thought we needed to work on. We've worked on those things in consultation with the private sector and other stakeholders. Version 1.1 was released that includes a section on cyber supply chain risks. We've clarified definitions of key terms, and also introduced a certain level of evaluation methods that organizations can use for their cybersecurity. The draft was released for public comment. The comments are due in the middle of April.

NIST also released SP 800-184, a guide for cybersecurity network coverage. Then, in the NISTIR 7621, Revision 1, guidance was updated for small business information security which is fundamental information people have been looking for. It provides some of the fundamentals for even the smallest of small businesses that can take steps to manage their risk in cybersecurity.

A couple of practice guides have been developed in draft from the National Cybersecurity Center of Excellence (NCCoE): one is based on email security, and the second one on situational awareness of government utilities. Email is such a threat factor constantly across agencies and industry. We have so many tools at our disposal where we have the real protections of many organizations to put these in play. Secure email is one of those.

The leaders of NIST got together periodically over the course of a number of months to try to rededicate and rearticulate what it is that makes us the kind of institution that we are. We settled on four major areas: The first one is Perseverance. We may work on thorny and challenging problems, not just for years, but for decades, without giving up. We strive to make improvements in a variety of different metrology and technology areas. The second is Integrity. It is the idea that we are uncompromising. The word "expedient" doesn't exist in the NIST vocabulary. We don't take shortcuts. We don't compromise our integrity for any reason whatsoever. The third is Inclusivity, which really has a couple of dimensions: a commitment to ensuring that we seek and provide avenues for a diverse work force; it also means ensuring our stakeholders have a voice in the work that we do and that we reflect the needs of the private sector and our government partners. The fourth is Excellence. It's hard to imagine that excellence would be fourth out of four, but these are in no priority order. We strive to do absolutely the best work in whatever area we get involved in. We try to be the best in the world. We don't stop until we've achieved that, and then continue to seek ways in which to get even better.

NIST has also been participating with NTIA on their efforts in IoT. ITL has its own IoT research program that is not solely focused on security, but largely focused on the challenges associated with an infrastructure that is connected everywhere all the time. Some of the risks that are associated with that particularly, where devices are of limited capacity to deploy security technologies. How do we architect the network for the systems in a way that can protect or isolate the risks?

DHS Voting as Critical Infrastructure

Dr. Neil Jenkins, Director, Enterprise Performance Management Office, DHS

The Chair welcomed Dr. Neil Jenkins, Director, Enterprise Performance Management Office, DHS to speak on DHS Voting as Critical Infrastructure. The Board members introduced themselves to Dr. Jenkins.

Dr. Jenkins provided updates to the Board on DHS activity working with state and local election officials on election infrastructure issues. He noted cyber incidents are viewed similarly to "arsons" in that there is a cause for the "fire", or incident, that must be discovered, and other parties assist with "putting the fire out". The FBI's main role in incident response, along with other law enforcement agencies, is to go in and try to figure out who started the fire, and prosecute them for it. Our job from the DHS perspective is to go in and help put out the fire, and then show them and help them get back up to speed.

There are three main areas of effort: protecting federal and civilian networks from malicious actors, supporting state, local tribal, and territories in managing their cybersecurity risk, and providing technical assistance and incident response if requested.

DHS provides risk assessment tools either with tools they provide to system owners so they can do self-assessments, or DHS can assist with a hands on approach. DHS is now working on internet voting. They started examining voting processes from a risk perspective when working with the states with the goal of providing tools. Any work to be done is voluntary. Originally the view was to work with state CIOs, but election infrastructure is much broader than originally thought. They then sought to identify capabilities that would assist with making elections more secure.

Voting infrastructure was designated a subsector of critical infrastructure. The designation allows election officials more access to threat information, and clearances in instances where it is deemed necessary. DHS also offered capabilities that were not dependent on any critical infrastructure designation. Tools offered included scanning an IP space and searching for vulnerabilities. We had 33 states and 36 local entities signed up for the service by Election Day. We were able to mitigate a great number of vulnerabilities. The service is still being offered, and is free of charge. At least five more local jurisdictions have been added since then.

DHS offers risk and vulnerability assessment, both onsite assessment and external, as well as other more onsite in depth assessments. The vulnerabilities discovered were similar to what has been found in other states and jurisdictions. There was nothing that warranted refocusing efforts. In sum, election officials were very prepared, more than most. We're not concerned with voting machines. They are difficult to access. The Voluntary Voting System Guidelines (VVSG) advise against putting them on the internet. This reduces risk and ability to launch attacks. We have not seen actual attacks on voting machines. We worked on voter registration database vulnerabilities and worked with the multi-state (MS) ISAC. They are continuing to encourage conversation with state CIOs. Cybersecurity advisors used to work with states according to FEMA region for a range of purposes. They urged connections be made prior to incidents when they are needed.

Prior to the election the focus was on cyber-threats. Following the election, they began to look more closely and started dialog with officials on the election infrastructure designation. Voting critical infrastructure includes voting assets such as machines, voting locations, etc.

However, an all-hazard approach was needed. They used the critical infrastructure definition as defined by the Patriot Act. In using that definition, it was clear that there would be an impact on a peaceful transition of power and national security threat if voting systems were attacked.

DHS created a subsector for them, with cybersecurity information relevant to them. Work is being done now with system owners and election system vendors. They have worked with officials to help them to understand the benefits of designation. There are three areas: Helps reduce system vulnerabilities, Work is done through coordinating councils, and participation is voluntary.

There is protection for the Critical Infrastructure Partnership Advisory Council (CIPAC) and the Protected Critical Infrastructure (PCII). Meetings held by these entities normally happen under FACA rules. It becomes difficult when talking about security. Vulnerabilities should not be made public. CPAC is exempt from FACA requirements. Having protection assists with communication with election officials. Information can be shared on incident responses and malicious actors. International norms now apply as attacks on critical infrastructure can be from nation-states. Executive orders can be done in response to attacks on critical infrastructure. It makes it more favorable for the government to use its capabilities to respond.

Are there aggregate findings on vulnerabilities? It may be beneficial to have them, but will need to work with entities to avoid exposing identities, etc. This applies to any election. Robustness of use may vary. Most obvious elections receive the most scrutiny. Local may receive less. DHS is concerned with inherent risk of putting voting systems on the internet. Updating voting system guidelines is ongoing.

Is there assistance to modernize state voting systems? Some of that assessment has been done. Diversity of technology is ok if machines are not on the internet. The scope of diversity is enormous. Many states will need to update their systems. Pieces of systems that touch the internet do have risk.

DHS is working with the vendors first to make sure they are plugged into information sharing in order to be informed about the supply chain. They are also educating election officials. Are there secure systems now in terms of supply chain? Secure systems do exist. There were shared indicators on two states that had voter database breaches. Indicators were shared and out of 20 attempts, two were successful.

L-U-N-C-H

Proposed Draft SP 800-53 revision 5 with Privacy and SP 800-171

Ron Ross; Kelley Dempsey, NIST

The Chair welcomed Mr. Ron Ross and Ms. Kelley Dempsey of NIST to discuss Proposed Draft Special Publication (SP) 800-53 revision 5 with Privacy and SP 800-171. The Board provided introductions for the speakers. Mr. Ross and Ms. Dempsey have two new NIST documents:

the 800-53 with the privacy section and the 800-171.

Ms. Dempsey presented NIST SP 800-171 Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations. CUI regulation was approved in November, 2016. Executive Order 13556 established a government wide CUI program to standardize the way the Executive Branch handles unclassified information that requires protection. The National Archives and Records Administration (NARA) was designated as the Executive Agent to implement the CUI program. A Federal information system is defined as information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency (As defined by FISMA). A non-federal information system is an information system that does not meet the criteria for a federal system.

The special publication describes how to protect the information. SP 800-171 covers only CUI components. The requirements are intended for federal organizations to use for citation to protect that information.

FIPS 200 and SP 800-53 define 14 security control families. That group was tailored to support the baseline for non-federal organizations and protecting CUI. An SP 800-171a will be published which will explain how to assess implementation of requirements. There are tables which map requirements to controls.

Mr. Ross discussed SP 800-53 with the privacy section. A pre-call for comments was sent out on SP 800-53, rev 5. Nearly a thousand comments were received from all sources. Comments were reviewed and fed into the development draft. Formatting and organizational changes were also made. It is intended to be outcome based. Federal focus was reduced because many other organizations also use 800-53. It only uses the term, "system" as opposed to "federal information" systems.

Major changes for the 800-53 Rev 5 included removing lead in entities to each control, focus on outcomes, aligning with security engineering and the cybersecurity framework, reduced the federal focus as well as others. Some appendices were moved into the body of the document. Other portions were moved to the appendices. A new appendix for key words has been added. There was a thorough scrub of related controls. Control references were also reviewed and edited. Front matter was streamlined. Program management controls are now in the main body. Privacy was completely integrated into the body of the publication and the related appendix removed. Two new privacy families were also added. A privacy appendix was added that shows mapping for locations of previous Appendix J material. It was noted that privacy events may or not be connected to breaches.

Automation application to automate updating the 800-53: Automating the comment process to increase updating process speed. Multiple workflows will guide the process. There will be a major update annually, with quarterly minor updates. FIPS is already reviewed on a scheduled basis.

DHS Automated Information Sharing Program

W. Preston Werntz, Chief, Technology Services Section, National Cybersecurity and Communications Integration Center (NCCIC), Department of Homeland Security (DHS)

The Chair welcomed W. Preston Werntz, Chief, Technology Services Section, National Cybersecurity and Communications Integration Center (NCCIC), Department of Homeland Security (DHS) to the meeting to speak on the DHS Automated Information Sharing program.

The Board opened with introductions for the speaker. Mr. Werntz introduced the DHS Automated Indicator Sharing (AIS) and noted it originated from the Cybersecurity Information Sharing Act of 2015. It began with six named entities in the legislation, and has since been working to increase the number of federal agencies involved. The goal has also been to create bi-directional sharing both from the private sector to DHS, but also to increase unclassified, federal government indicators in the best measures that can be shared with the private sector. It will increase value for everyone involved. The program has been running for about a year, and in a week will be going live.

Over two hundred nonfederal entities have signed up to participate, meaning domestic private sector, state and local entities including state governments, local governments, municipal water plants, etc. There are also a number of international certs and companies that have signed up. Anything that's not a federal executive civilian department agency is considered to be nonfederal. There are 93 that are fully connected to our capability. For a nonfederal entity to join AIS, there is paperwork to be completed. We try to make it really simple for folks to sign up.

Once an entity is signed up, there are some technical steps to actually onboard and connect to the server. There's always a lag of people who want to participate, with the time it takes for individual entities to complete the technical steps. Out of those 93 that are connected, 12 of them are either information sharing analysis centers (ISAC), information sharing analysis organizations (ISAOs), or cybersecurity proprietors. ISACs, ISAOs, and these different cyber providers, these commercial companies, they're able to re-share the indicators that we give to them to all their members or customers.

There are 93 direct connections to the server but the reach of the indicators being shared gets into hundreds and thousands of entities. It's even tougher for DHS to figure out how far and wide indicators go. It's a choice we're okay with and we think it strengthens the ecosystem. That 93 gets DHS to several thousand different organizations that can make use of these indicators.

The communications industry has had a pilot for a while now in Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII). It started out as CTIA's pilot but now it's got the cable and CTA and others. AT&T is on and several other carriers are also connected. The pilot was done because some unique issues exist in STIX and TAXII to sort through. We're trying to work with Oasis but that's not necessarily all with AIS.

For the nonfederal side, we've got 34 federal entities connected right now. In some cases, it's multiple with NCI, and JTF out of the FBI. In the 34 there might be two or three per large federal departments, but we're trying to obviously get this spread out to the right places across the federal government.

Once connected to the server, everything is in place to provide directional sharing. As soon as entities receive, they can share back at the rate they want. Once signed up, we're able to share with them very quickly and we're ready to receive from them when they are ready to share with us.

In AIS, the focus is velocity and volume of indicator sharing, not human validation. It is machine speed, machine automation. It's not about putting all this cyber threat data in front of people to look at and validate That's traditionally how it's been done and that's how sharing indicators takes days and weeks and months versus sharing this cyber threat data right now.

When an indicator is pushed to DHS, this is the automated process. If it passes automated processes, it gets re-shared within 30 minutes. It allows content to be shared much faster. It's about velocity and volume, not everything going through human review, but there are places where it does have to go through a human.

Velocity and volume versus retaining context is one of the challenges of the AIS. Contextual information is always a struggle. Some is always lost with automated protocols. Then the question becomes if AIS is a wide open system that's designed around velocity and speed, then the quality of the information at some point gets diluted because it's not necessarily the most contextual. In some cases, it's not as relevant to what they're doing, some of that context gets lost because the focus is elsewhere.

We try to determine technical context in the absence of other context. Developing technical context can mean waiting for metadata, which starts to provide a picture about the information being provided. AIS has some technical context, we are trying to add to it. It leads to a decision about whether an indicator is relevant or not. There is also a cyber threat intelligence context. Some people call it "attribution". "Cyber threat intelligence context" is preferable to "attribution". Saying "DHS" and "attribution" in the same sentence makes people nervous.

The process of building a machine auto-immune capability to determine trustworthiness of indicators that come in is going on. The context may make things sensitive. There is a TAXI server in Amazon's cloud environment. We evaluated privacy impacts and automated process. The PII is removed. All fields are evaluated, if any fail, those fields are marked and sent for review. CISA has annual reporting to Congress. There are additional DHS reporting priorities. We are trying to determine what quality is available.

A preliminary privacy impact analysis (PIA) was done, and determined a full PIA was needed and done. Some of the information collected was not necessary to track threats. There is a central repository that stores all indicators for the last 3 years. Many non-federal companies are interested in the AIS. Growth is still going on. It is hard to determine actual cost of getting in AIS. Companies can invest heavily or use open source solutions. The PKI cert costs $900. Costs after that very widely.

B-R-E-A-K

Cyber Security Framework 1.1. Changes and comments.

Matthew Barrett, NIST

The Chair welcomed Mr. Mathew Barrett, NIST to the meeting to discuss Cybersecurity Framework 1.1 changes and comments. He provided a brief update on the Baldrige Cybersecurity Excellence Builder. It is a merger of the Baldrige Performance Excellence Program, which is about the integration of quality control and quality assurance into the larger organization with cybersecurity. It falls into the realm of enterprise risk management. A draft of the self-assessment criteria that is the Cybersecurity Excellence Builder was released for a comment period. The final of the 1.0 Cybersecurity Excellence Builder will be released on Sunday, April 2, 2017, in time for the 29th annual Quest for Excellence Conference being held April 2-5, in Baltimore, Maryland. This year there will be a preconference cybersecurity workshop where participants will use the Cybersecurity Excellence Builder as part of a larger session.

Input from various parties are coming in for proposed updates. Cyber supply chain risk management is a major update. There is a basic taxonomy for basic supply chain entities. Supply chain risk management is a fourth property that runs throughout. It makes the twenty-third category to be added to the framework. There is a new section on measuring and demonstrating cybersecurity. Framework flexibility has been a big reason for success. It fits small to large entities.

The FISMA and Framework teams are working together, trying to reconcile these two things with two different lineages. The current permutation has eight use cases. These are things that federal organizations have to do anyway in the realm of cybersecurity. Mr. Barrett's group is trying to demonstrate how to employ the Cybersecurity Framework alongside some of the preexisting FISMA guidance and standards. The bigger point is this intent and plan to unify risk management methodologies and frameworks for federal agencies to use.

The update attempts to refine and clarify what has been done. Feedback came from the December, 2015 request for information, from the April 2016 workshop, and from advances in cybersecurity roadmap topic areas. The dialogues have been about what’s working and what’s not working with the Cybersecurity Framework. The updates are in several topic areas, there is a big, big update in cyber supply chain risk management.

A twenty-third category has been added to the Cybersecurity Framework. It is the only category-add to date. Guidance on metrics and measurement in framework is also an addition. It is a brand new section, Section 4.0, Measuring and Demonstrating Cybersecurity. It may be difficult to measure return on investment for employing cybersecurity measures. Knowing something in advance can clarify potential damages to equipment, damage to reputation for companies, and lost revenue for being offline during an attack.

The access control category for the framework has been improved. The process to finalize the framework is continuing to educate people on the framework and accept comments. Public workshop on the framework is scheduled for mid-May at NIST. The hope is to finalize in late summer. Private citizens and government agencies have responded with comments thus far. Two weeks remain until the end of the comment period.

Security of USG Websites – ITIF Report

Daniel Castro (Remote), Vice President, Information Technology & Innovation Foundation

Alan McQuinn, Research Analyst, Information Technology & Innovation Foundation

The Chair welcomed Daniel Castro (Remote), Vice President, Information Technology & Innovation Foundation, and Alan McQuinn, Research Analyst, Information Technology & Innovation Foundation to the meeting to speak about Security of USG Websites, ITIF Report. The Board members introduced themselves to the speakers.

The Information Technology and Innovation Foundation is a non-profit public policy think tank dedicated to innovation, technology, and public policy. They did a report that looked at federal websites. Federal websites are the primary means of interaction with the federal government. The report looked at the most popular federal websites and evaluated them on a number of factors: federal legislation, federal guidance from the executive branch, and compared federal websites.

Two hundred ninety seven federal websites that ranked in the top million overall were included in the report. Seven tools were used. As an example, page load speed was used as slow loading speed is a major cause for leaving a web page. The report found 78 percent passed for desktop computer scores, but only 36 percent passed for mobile speed scores. A number of very popular federal sites failed. Benchmarks versus non-government websites were determined. They also looked at what would make a load fail from the consumer standpoint. Broadband was excluded from the conditions.

For testing security, they used a tool that looked at SSL connections based on four conditions: 78 percent passed for the desktop scores, but only 36 percent passed for mobile speed scores. Two thirds of the websites passed the test but did not enable https. We noticed that while going through a lot of the tests, non-executive federal websites tended to fail worse than executive federal websites, perhaps because they don't follow the same best practices or the same guidance, but they should absolutely have security.

The test also looked at vulnerabilities and two of those found were both man-in-the-middle attacks: the POODLE attack, and the DROWN attack. The POODLE attack takes advantage of outdated protocols. It lowers encryption and steals information. The DROWN attack poses as web site and intercepts information. DNNSSEC was not enabled in 10 percent. Since the report has been released, there has been good feedback. Feedback on metrics has been received and is being reviewed.

Following the report, the following recommendations were made. First, we recommended that the White House launch a series of sprints to address the most pressing problems. We haven't seen the new administration necessarily take that on as a White House public recommendation. The second recommendation involved standard testing against guidelines or standards. GSA should examine this issue, also shared web services for smaller agencies who have challenges meeting standards. There is a government wide website consolidation initiative. The number of government websites is very high. One of the recommendations is to have strategic thinking about how to bring the other branches of government and these independent agencies on board with following these same type of requirements if we agree that these are best practices. There must be more transparency and accountability.

Modernization and configuration continue to be challenges. How is the problem fixed? Funding or sprints need to happen. Keeping policies updated will also assist with bringing ongoing change as agencies must comply.

Meeting Recess

The meeting recessed at 4:48 p.m., Eastern Time.

Thursday, March 30, 2017

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

Bug Bounties and the United States Government (USG)

Eric Mill, Senior Advisor on Technology Transformation Service, GSA

Hunter Price, Department of Defense (DoD)

The Chair welcomed Eric Mill, Senior Advisor on Technology Transformation Service, GSA; and Hunter Price, Department of Defense to the meeting to discuss Bug Bounties and the USG. The Board members introduced themselves to the speakers.

Mr. Hunter sought to update the Board on recent and future activities at the Department of Defense. Last spring, the DoD and Digital Defense Service launched a pilot bug bounty program called "Hack the Pentagon". For four weeks, about 1,400 hackers and former testers had access to five public-facing community websites, in order to test their security.

These five sites had finished in-testing from a professional in-testing firm before the Hack the Pentagon program started. In total, ten vulnerabilities were found by the in-testing firm. NIST would characterize all of them as low risk vulnerabilities. The first vulnerability report in the Hack the Pentagon program, came within five minutes after the program started. It was what NIST would consider a high risk vulnerability. In total, over the course of four weeks, over 165 unique vulnerabilities were reported. A number of those were what NIST would characterize as high risk vulnerabilities.

The program cost DoD something over $150,000. That meant 15 percent of the cost produced a thousand percent of the return. There was some initial concern on how the program would go. The pilot helped to allay those fears. Last year, an IDIQ was awarded to two different bug bounty listening companies.

One of those companies launched a "Hack the Army" program to test eight public Army sites that were part of the recruiting network. These sites had a lot of personally identifiable information (PII). Prior to the program, about 16 vulnerabilities were found. When the program opened, the first vulnerability was reported in thirteen minutes. It was considered a high risk vulnerability.

The return on the bug bounty investments has been unparalleled. It has given the government access to talent it would not otherwise get. Should the Board encourage the government to pursue bug bounty programs? The answer is yes. There is potential to make people uncomfortable. The perception is that secrecy is part of security. It is a myth. Secrecy is not security. DoD has worked to increase understanding of that principle. There were background checks for Hack the Pentagon. Hack the Army had background checks for those who wanted to be paid bounties. There are gray hat hackers among the pool.

The total cost of the program was 150k. 75k was for bug bounties. Hack the Army launched a vulnerability disclosure policy. It essentially is see something, say something for vulnerabilities. No bounties are paid in that situation. The contractor works with the content owner to remediate vulnerabilities. Are the rules of engagement public? DOD encourages people to talk to them. The contractor decides who participates, and the rules of engagement. Boundaries are clearly defined, and the law enforced appropriately.

They are engaged in making agencies and offices understand that secrecy is not security. If it ever was true, it no longer is today. Entities often want to defer vulnerability searches until they are "ready" under the guise of not having funds. However, attackers don't wait until we are ready.

It gets to the broader question of acquisitions. Contractors tend to sell what they think the government wants. There is discomfort with the government proscribing tools. It has not worked well in the past. The government could consult the community, based on bug bounty results, about what is secure.

The Technology Transformation Service is an umbrella for various technology programs at GSA. GSA has a vulnerability policy, and is about to launch a bug bounty program for a number of their projects. GSA is attempting to bring its risk posture up to match the level of scrutiny it receives. They started with the agency vulnerability disclosure policy because it describes the internal consensus that should become the norm. The GSA technology transformation service is running the bug bounty for GSA. It is not government-wide. Things are less secret than they used to be. "Defense in depth" may be cover for inconvenience in changing difficult things. It is not a reason to defer change.

DDoS Threat Activity

Ari Schwartz, Venable LLC

Arabella Hallawell, Arbor Networks

The Chair welcomed Ari Schwartz, Venable, LLC, and Arabella Hallawell, Arbor Networks to the meeting to update the Board on DDoS Threat Activity. The Board members introduced themselves to the speakers.

The speakers have been active on internet of things and DDoS issues, in working with several different groups across different states. They have been taken aback by the scale of some recent cases. There were some discussions about measures to take against what became the Dyn attack, but it happened too quickly.

Arbor surveys member networks anonymously to track activity. It publishes an annual report on DDoS attack trends. There has been an acceleration in attacks in 2015-16. Most attacks are small. Large attacks are more becoming more frequent. The Mirai botnet was used in Dyn attacks. Dyn was attacked globally. Weaponization and ease of attack is increasing. Availability of tools has increased greatly in the last five years.

Prior to Dyn, sophistication increased in the Krebs attack. The advent of IoT devices has changed the DDoS game. Driving factors include nearly every device on the market now connected. DDoS attacks cost attackers $5 per minute. Cost victims can be $500,000 or more per minute. Attribution is not always disclosed. The volume has increased quite a bit.

Attack sizes started at a low bandwidth volume and have increased to a peak. The largest attack volume until recently was 800 gigabytes per second. There have since been some billion plus per second attacks. Frequency has increased across the board. Some sectors are seeing over five hundred attacks a month. Multi-pronged attacks are common today. Mirai is everywhere across the globe now.

DDoS attacks have become weaponized. It's much easier for attackers to wage DDoS attacks today than it was five or ten years ago. Attackers today are also more technically skilled today than in the past. The internet of things changes the game because of the speed of acquiring traffic using IoT devices.

Net Service Providers have put out a set of best practices for network operators and shared them with all the ISACs. Arbor and others have been a part of that for a good while. Sectors have been hit with large attacks, and it has served as a wakeup call. Attackers are getting smarter about determining whose expertise and protection may be lower. Attacks now involve forming metrics, stage exhaustion, and application layer attacks.

A recent *Wall Street Journal* article on one botnet infected security camera describes attacks with a typical IoT device. It leads into discussions on securing IoT devices, and regulations on that topic. International norms are needed in this area. There are ways to cut some of the traffic unilaterally, but the ultimate solution has to be international rather than domestic.

We need to be prepared for the complexity of a DDoS attack, in order to rapidly detect and respond. On the framework, develop a threat profile to underlie the framework. Arbor is working on such a document and will be happy to share with the Board when it comes out. Underwriter's Lab (UL) has been focused on medical devices and cars. That conversation will continue. There is work on the MUD standard, which examines devices to identify the device type and the port it communicates on. If something happens outside those parameters, the device can be shut down.

BREAK

IOT Security and Privacy – NTIA Report

Dr. Travis Hall, Telecommunications Policy Analyst, National Telecommunications and Information Administration

Evelyn Remaley, Deputy Associate Administrator for NTIA

The Chair welcomed Dr. Travis Hall, Telecommunications Policy Analyst, National Telecommunications and Information Administration and Evelyn Remaley, Deputy Associate Administrator for NTIA to the meeting to update the Board on IOT Security and Privacy – NTIA Report. The Board members introduced themselves to the speakers.

Ms. Remaley will provide an update to the NTIA green paper on the internet of things. Things at Commerce are getting under way with the new administration. NTIA is still awaiting for its new agency head to be nominated. They are moving ahead in the interim.

What the paper did was provide a possible approach based on four principles that IOT is inclusive and accessible to support a stable, secure, and trustworthy IOT environment. We advocate for a globally connected internet of things, and make sure we encourage growth. It also discussed areas of engagement on infrastructure availability and access, crafting policy, protecting standards in technology advancement, and encouraging the internet of things market.

There have been two requests for comments. The second had four areas centered on approach, possible gaps, and possible activities for the future. We received approximately 50 responses. A number of responses focused on cybersecurity vulnerability. The NTIA has been thinking about processes to handle vulnerabilities. A multi-stakeholder process focused on the internet of things has started following its announcement last summer. There was a virtual meeting in January, and a second meeting in the works to evaluate working group progress. There are four active working groups. The next meeting will be in April, followed by additional meetings over the summer. It has been challenging to determine technical specifications, and understand what the potential barriers are in the market. Learning how to make things patchable is critical. Responsibilities for all players need to be defined.

Communication is important for everyone, not just consumers. It is not always clear among venders, retailers, service providers and others where responsibilities lie. Arriving at understanding of what the types of patch-ability are, will help with creating transparency for everyone. Developing a common terminology is important to keeping a stable environment for all involved.

The first meeting was held in partnership with the Consumer Technology Association (CTA). There is interest in these areas from small manufacturers. They have recognized issues exist, but are not part of the process. It's not easy for smaller entities because of resource constraints. CTA recently published guidelines on installation of devices for home users.

L-U-N-C-H

NIST/ITL Update

Chuck Romine; Donna Dodson; Kevin Stine; Matthew Scholl, NIST

The Chair welcomed Chuck Romine, Donna Dodson, Kevin Stine, and Matthew Scholl of NIST to the meeting to discuss NIST ITL updates. Ms. Dodson noted the passing of Howard Schmidt, formerly of NIST and friend of the community. It was felt a letter of appreciation to his widow from the Board should be drafted.

Quantum Computing

NIST published and submitted calls for building quantum-resistant cryptographic algorithms. The work is officially under way. It's open until November 30, 2017 for submissions. A few submissions have been received to date. The PQC team actually got back from Japan last week, where they were in the Asia-Pacific Post-Quantum Cryptography Conference. Japan and Korea are going to work with NIST on this, as well as others from the EuroCrypt sessions last year. Germany and the E.U. were also working with us.

They've done a great job at both putting together international collaborators, and then having the call along with the specifications on what we're looking for out in the public. In preparing, we had to determine how to handle the bit strength expression in cryptography, that is the 2^{128} key strength. Key strengths are not necessarily binary in a quantum environment.

We received a lot of feedback on evaluating and assessing cryptographic strength in a quantum world, using binary technology. While still using a 2^{n} construct, they were able to evaluate cryptographic strength from multiple perspectives on quantum circuit sizes, runtimes, and circuit-adapted quantum environments and arrive at a composite look at security in a quantum world. The call for participation was developed based on these results. Over the next four years these items will be standardized, and the process of creating commercial products will begin.

A document on light weight encryption will be coming out later this month. Lightweight encryption would only be used in specifically defined situations. There is concern it will be applied where it should not be. Work is ongoing to determine where it is best used.

Researchers at Google were able to demonstrate a Secure Hash Algorithm-1 (SHA-1) attack. SHA-1 has gone from being theoretical to being real, demonstrating a collision with a hash. NIST advocated against building SHA-1 any more in 2011. It was reiterated in 2013, and four years later it was broken. They used expanded cloud environments and virtualizations to extend processing capacity. It amounted to a brute force attacking cryptography. We're continuing to examine current inventory to be sure it's still fine, but beginning to think about progressions out as quantum resistance comes in.

We had a blockchain workshop with HHS, where they brought blockchain use cases in health care environments. Cryptographic techniques and technological implementations of blockchains were examined. Some fundamental blockchain documents will be published this year.

Currently, we are investigating security properties of tools and how they work together. If we improve the tool sets we use, we may prevent attacks later. We are looking at ways people can protect themselves from destructive malware attacks. A document will be published soon with techniques and ways for people to protect themselves. The work includes multiple agencies such as NSA and DoD, and industry as well.

Work is going on with next generation access control with identity mechanism systems. They are looking at additional mechanisms besides the current PIV card for identity, such as continuous identity association. It's in research today.

We continue to update and make changes to our crypto test and validation program. The team is working to push the testing requirements as close to the vendor as possible, still keeping the value that an independent laboratory gives for a second level of assurance. They can then validate algorithms provide the correct answers. The National Vulnerability Database (NVD) has been growing rapidly. It used to be just software, but now includes hardware. Medical device communities are now asking to join NVD. NVD is one of NIST's top four websites. The NVD team publishes a vulnerability standardized ontology on how vulnerabilities are expressed, scored and rated. This is the Common Vulnerability Enumerator (CVE). It is a unique identifier with an associated Common Vulnerability Score (CVSS). The goal is to start to open it up to everyone to be able to check against each other. It creates confidence things are being scored correctly.

STIX is able to use CVEs to identify a unique vulnerability. The CVE is part of a STIX data feed. It should become tool based so that it can continue to be expanded.

The Commission on Enhancing National Cybersecurity

The Commission's final report was delivered to the President on December 1, 2016. Since December, people have had an opportunity to digest the report. There have been a number of different cybersecurity announcements and activities at the end of the previous administration, and the beginning of the new one. Some of the themes tie back to some of the commission recommendations and proposed actions.

Internet of things and other activities

NIST has been in IoT for some time. There is now a cybersecurity for IoT program at NIST. The current focus has been getting a better sense of the work to be done both within NIST's portfolio but also across government and industry. RSA provided an opportunity to have in-depth discussions on what's happening currently.

Small business cybersecurity continues to be an area of focus. NIST is examining how it can be most effective in light of the current environment. Active engagement and more interagency involvement are being considered as ways to improve interactions with small businesses in this area. NIST is looking at available resources to assist in this effort.

Rodney Petersen of NICE spoke at the previous ISPAB meeting. There has been a lot of interest in ongoing activities related to the National Initiative on Cybersecurity Education (NICE). SP 800-181, the National Cybersecurity Workforce Framework is approaching the end of its final draft stage. We anticipate publication in May, 2017.

National Cybersecurity Center of Excellence (NCCoE)

The Center has hit its stride with three new long term partners: Amazon, ForeScout Technologies, and IBM. We've been in conversations with partners and collaborators, and communities of interest in our work. A lot of good things are coming from it, particularly practice guides. A guide on situational awareness for electric utilities is out for comment currently. The guides try to speak from a business perspective, then follow with risk assessment, security architecture, and security controls. They are mapped to the framework and identify the SP 853 controls. The final section demonstrates what the final result looks like in terms of products and services used to create the final result.

The Center is also involved in multi factor authentication work with the retail community. It will also host a workshop on DDOS. Many good things are going on. The Center is always willing to host new events.

B-R-E-A-K

Public Comments

Mr. Mike Nelson, Public Policy for Cloudflare

The Chair welcomed Mr. Mike Nelson, Public Policy for Cloudflare to the meeting to provide comments as a member of the public.

Cloudflare is one of the biggest players in protecting against Distributed Denial of Service Attacks. It protects about 6 million different websites and web properties by filtering traffic through 53 different countries where it has 103 different data centers. It is one of the largest internet connective networks working with hundreds of different ISPs to create this giant filter that's blocking the traffic from the botnets. Once we built that infrastructure, we've also been able to do a lot of other things including accelerating the delivery of the bits coming from these 6 million websites. We've also rolled out new leading edge cyber security technologies making it much easier for people to adopt HTTPS, for instance.

A little less than two years ago, we rolled out universal SSL and in three weeks, we doubled the number of websites that use HTTPS. We've also been pushing DNS stack, TLS 1.3, which is a much more efficient form of encryption. We're trying to push the internet in a good direction. Most of our customers don't pay us anything; they just use our free basic service which blocks DDoS attacks. I've been at Cloudflare for just over two years, but I've been working on internet policy for almost 30.

Mr. Nelson shared a couple of observations from the last two days. I was delighted that you covered a lot of the obvious things that needed to be covered. The Board did very well talking about the White House report, IOT Security Framework 1.1., and a very, very good presentation on the DDOS threat. I didn't hear a lot there that I didn't agree with, but I do think it's useful to focus on what I didn't hear the Board talk about.

The first, and most obvious topic, is what happened in Congress on Tuesday. The resolution to repeal the Federal Communications rules on the privacy of data that internet service providers collect. Part of the open internet order of internet neutrality included provisions that put the SEC in charge of protecting the privacy of ISP data. Those rules were repealed by Congress. And as a result, there are really no rules. It will be a while before that is sorted out. The Chair noted the rules that were repealed were the privacy rules, which are different from the internet rules, and that the protections that exist today. Just to be clear.

Because the open internet order has now been repealed, consumers are no longer under the FTC, we are now in limbo. The other point there is not that we should be talking about what the lawyers did, the point is that there's a huge amount of interest now among internet users for virtual private networks, and how can they leave fewer digital breadcrumbs in cyberspace.

The other thing that the Board has talked about a lot in the past, but didn't spend a lot of time on, is back door encryption. NIST is part of those discussions, but this is an issue that's getting hotter and hotter; clearly, we have to somehow communicate to people who assume there's a magic technology that can somehow allow back doors that only the good guys can use to look at the bad guys. NIST has all this credibility and it needs to do a better job of explaining to policy makers around the world that if this was possible, it would already have happened.

The third issue, there was not a lot of discussion about, is the vulnerability equities process. There is legislation being proposed to formalize the vulnerabilities equity process. Senator Schatz, Congressman Lieu, and the exposure of the CIAs hacking tools through WikiLeaks have certainly highlighted the importance of understanding what vulnerabilities the government has and how they'll be used. For us, a company that has most of its business overseas, it's very worrisome that the federal government is not helping companies. Not all parts of the federal government are helping US companies fix and deal with vulnerabilities.

The most important thing that there could have been more about, was software defined networks. We heard a lot of discussion about internet of things security. But there was not enough discussion of how cloud based security services can help us solve the internet of things security issues that are popping up everywhere. The "internet of things" is a very unfortunate term because it focuses the regulators on the things. The big thing it does is when a regulator, or a policy maker hears about the internet of things, they turn to their telecom regulator.

The solution to most of our problems with the internet of things, and certainly most of the privacy concerns, is in the cloud. It's where the data that comes from the internet of things goes. We're not thinking about the whole picture. Mr. Nelson's preferred term is the cloud of things (COT). Or even better, the cloud of all things (COAT). If we get this right, that's what we'll have. People get very comfortable putting things on the internet and connecting it to the cloud. And we'll be able to use the power of the cloud to solve a lot of the security problems that we're facing. What worries me, is that I keep hearing on The Hill, in Brussels, and in other countries, is that the answer is regulating all the things. We had a bit of a discussion about that today. That's just not going to be practical. We're not going to have global government; so we're not going to get a global answer.

We're going to need to focus a lot more on how we can build the cloud so that the data coming off of those things can be dealt with properly, so we can lock devices that are emitting bot traffic. There's a lot of things that can be done without having to fix the thing. If we insist that every little thing be regulated a certain way, we're going to miss out on a lot of the most exciting opportunities that involve five cent and ten cent things. Because we're not going to be able to accommodate all the regulations coming from three or four different governments as necessary. That's a longer speech. I really hope we can get to the cloud of all things by taking advantage of all these cloud based security services that can help us solve some of the problems that we discussed today.

Two other real quick things. There could be more discussion of formal methods, and ways we can develop the tools to check software. We have a lot of these great tools and we haven't made them easy to use. Ease of use is the last thing on that list of things that I hope that the Board spends more time on. Our whole company is based on that. One of our three co-founders has the title, head of ease of use. It's that important. That's what we've tried to do with all these new technologies.

There is some work going on in security and usability. It's been said, security should be, easy to do the right thing, harder to do the wrong thing, and easier to back up and undo the wrong thing. That's a pretty tall order in this space today. It's one of the things the cloud could provide. That's what we were able to do with our universal SSL. People could go online and push a button, and five minutes later their website was running HTTPS. That's what we need to do.

The other two things, just to add in, on my wish list, I really hope that NIST will be able to do more of the international agreement. Given the politics of the bill and the budgets, it's difficult, but never has there been more need for your expertise in the discussions happening overseas. Particularly in the area of encryption back doors. The French, the UK, the Germans, they're all talking about the magic technology that's going to somehow alleviate the problem that law enforcement has in strong tech encryption.

They're also dealing with the vulnerabilities programs, the Board could help there. The only place that needs help more than the foreign governments is probably the state governments. It's a little cheaper to get to the state capitals. This week, the district attorney from San Bernardino, the head of the national district attorneys association, is in town talking about magic technologies with back doors on encryption. I know there is limited bandwidth, but if there's any way to help people understand cyber security technology better, that would be incredibly useful.

Mr Nelson is on Twitter, @mikenelson, or mnelson@cloudflare.com. He has business cards those who may be interested. He thanked the Board for its time.

Board Review and Discussion

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

The Board discussed the following items from the first two days of the meeting.

1. Future meeting date - June: 28-30 2017. Mr. Scholl will check with the Access Board today.
2. Consistent theme on vulnerabilities to Federal systems. What should the Board consider and weigh in on? Election system, DDOS, federal websites. These things together can give advice from the board. Consider government wide strategy for bounty programs; voting – suggest a study into what's required to modernize and ensure voting infrastructure is prepared. Mr. Scholl will research existing materials. State cybersecurity grants possible way to modernize. Federal website modernization.
3. DDOS preparedness for agencies. The Board has considered all these topics, not proposing solutions.
4. Executive Order –The Board can write letter on important parts of risk assessment that need to be included.
5. Automated Indicator Sharing – converting threat indicators into remediation.
6. Implement CSF as foundation and funds to make it all happen. Agencies don't have budget for modernization. Follow-on to December 2016 letter. Separate modernization from line item budgets. Privacy office and technology office should be included in modernization effort.
7. Privacy and Civil Liberties Oversight Board (PCLO). Not all positions on the board are filled. Discuss more Friday.

Meeting Recessed

The meeting recessed at 2:55 p.m., Eastern Time.

Friday, March 31, 2017

The meeting opened at 9:03, Eastern Time.

Legislative Assistant, Office of Congressman Jim Langevin

Nicholas Leiserson

The Chair welcomed Nicolas Leiserson, Legislative Assistant, Office of Congressman Jim Langevin to the meeting to speak on the current legislative landscape in the House of Representatives. Congressman Langevin is the current co-chair of the House Cybersecurity Caucus.

On the legislative front, the number one item has been the Congressional budget. The Congressman's staff is still trying to determine how cybersecurity fits into the picture. There is still confusion about provisions. There has been a slow ramp up on some DHS initiatives previously authorized under the Cyber Security Act such as automated indicator sharing. There seems to have been a slow uptake thus far. There has been a great deal of oversight on the Cybersecurity Act by Congress. Presidential Policy Directive 41 (PPD-41) has also received attention.

Data breach notification is likely to be the next piece of major legislation. Interestingly, New Mexico recently became the 48th state to enact its own breach notification law. There are at least four bills on the House side from the last Congress, and possibly five or six on the Senate side. There is ongoing debate about how to weigh the various components. It has moved in the process, but still requires conflicts between the various proposals.

During the 115th Congress, there will be focus on workforce development. We will be examining how to harmonize the different workforce incentives that came into different departments and agencies from various bills. They will also be concerned with workforce retention. Some cyber mission personnel at US Cyber Command are coming to the end of their four year terms. It should be in the government's interest to retain them as opposed to training new people.

The government may be missing opportunities by having more rigid career paths that don't allow people to move around between being a civil servant and working on the agency side, or allow them to stay for only a few years. It seems evident that we can't just depend on colleges and universities because there is a new generation of people out there that are working on those types of things. There seems to be a bottleneck in getting people into the jobs. They will be examining how to remove that bottleneck. Congress is also interested in measuring whether its policies have a positive impact.

Gathering data for metrics to determine performance has been challenging. Insurance companies are trying to collect data to support what controls affect premiums. Data breach insurance companies tend to be more interested in looking at outcomes and how attackers got in. One of the larger problems is that insurance data is not public. Details of how attacks occur are never shared. Causes of plane crashes eventually become public, and there are lessons learned from it. There is no national database for cyber events as there is for automobile insurance. There is no way to uniformly describe cyber incidents. There are voluntary programs to report incidents, but the problem becomes how to incentivize people to actually report. One way is the DHS VCCI program. Information provided is not subject to exposure rules. It is exempt from FOIA. People who share are still conservative about what they share. There is a lot of complexity in the issue.

House Science Committee Staff

Rajesh Bharwani, House Science Committee

Cliff Shannon, House Science Committee

The Chair welcomed Rajesh Bharwani and Cliff Shannon of the House Science Committee to update the meeting on House cybersecurity activities relating to the NIST Framework and across agencies in the government.

Mr. Bharwani discussed the recent NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017 (HR-1224) that relates to assessing and unifying compliance to the NIST Cybersecurity Framework across government agencies. Congress has placed a great deal of focus on cybersecurity during the last Congress and the current one. He cited two reports as being particularly influential for HR-1224: the *Report on Securing and Growing the Digital Economy* published by the Commission on Enhancing National Cybersecurity, and the CSIS Report *From Awareness to Action: A Cybersecurity Agenda for the 45th President.*

A witness to the GAO hearing on its findings on federal agency cybersecurity noted that it consistently identified shortcomings in the governments approach to ensuring security of federal information systems and cyber-critical infrastructure. NIST is to provide guidance to OMB and other agencies on how to best use the framework in increasing their security and information management efforts. A working group is being set up to define metrics for agencies to increase analysis capabilities and assess effectiveness of the plan.

NIST is directed to conduct a government-wide assessment of the state of federal cybersecurity, followed by individual agency assessments to check compliance with NIST standards and guidelines. Reporting requirements will be established to assess overall progress. In two months, an interagency report with FISMA and NIST cybersecurity teams to give Federal agencies a comprehensive guide to understanding cybersecurity risks. The NIST Framework will be mapped to FISMA requirements. The Committee is resolved to assist agencies in overcoming the federal government's cybersecurity shortcomings.

There is no consistency across the government on how standards are implemented. Credible audits are needed now. NIST may be best for that capability, as it has a strong background, and there is confidence NIST will get the job done. If credible audits were going on elsewhere in the government, the proposed audits would not be needed. The sense of urgency on this issue has been lacking in the past. The situation the federal government finds itself in right now is such that steps must be taken to start curing vulnerabilities immediately.

The Science Committee is working with its counterparts in the House and Senate to attempt to tweak the bill to meet outstanding concerns. Events cannot continue on the current course. The threat is multiplying, and to do nothing is irresponsible. They are waiting to see the final content of the executive order that will come from the White House.

Science Technology Engineering and Math (STEM) education is important and will be looked at. It is in an early stage. The Science Committee was tasked with starting conversations last year. Work will be continuing on that basis.

Professional Staff Member and Investigator, Chairman John Thune, Senate Commerce Committee Staff

Cherilyn Pascoe, Professional Staff Member and Investigator, U.S. Senate Committee on Commerce, Science and Transportation

The Chair welcomed Cherilyn Pasco, Professional Staff Member and Investigator, U.S. Senate Committee on Commerce, Science and Transportation to the meeting to give an overview of legislative priorities. The board members introduced themselves to the speakers.

The Commerce Committee has worked very closely with NIST and other agencies in its jurisdiction for many years. We will provide an overview of some of the priorities that have developed in the last few years. Their work in cybersecurity started with the Cybersecurity Enhancement Act of 2014. This law authorized development of the NIST Framework in coordination with industry, as well as research and development priorities and workforce development. We recently incorporated cyber security into the Federal Aviation Administration (FAA) extension to address cybersecurity concerns with aircraft.

NIST, with DHS, was instructed to raise awareness of the Framework across agencies. The NSF was also instructed to include cybersecurity related research topics when considering grant awards. NIST was also authorized to research computer and network security. Small business cybersecurity guidance has been a priority. NIST will provide prioritization on tips and recommendations, and possibly do videos that will assist small businesses with understanding the framework. Going forward, agencies will post resources for small business on their websites.

The Departments of Transportation and Commerce have new Secretaries. Letters have been sent to them requesting they prioritize cybersecurity within their agencies. They have agreed to keep us informed as they work through creating the right level of cybersecurity in their agencies.

There have been discussions on commerce and using a different angle with creating an environment where sharing threats is possible with the Russians. Work is going on with potential legislation for testing and deployment of self-driving vehicles. Security concerns for self-driving vehicles play into the current auto safety security challenges. The auto industry and the Department of Transportation are taking steps to continue the work in this area. The committee's jurisdiction is very broad. It includes NIST and R&D in the workforce, also aviation, autos, transportation, and communication and Verisign security.

House Energy and Commerce Professional Staff Member

Jessica Wilkerson

The Chair welcomed Jessica Wilkerson, House Energy and Commerce Professional Staff Member, to the meeting to provide updates on cybersecurity in the committee. The Board members introduced themselves to the speaker.

Ms. Wilkerson handles cybersecurity issues that fall within the jurisdiction of the Committee, and will be providing updates only on the issues she deals with. There have been two coordinated exposure act drills, one in February and one back in November. These drills entail bringing vulnerabilities to light, stating how they are exploited, and providing time for companies to fix those vulnerabilities. This is an important part of improving cybersecurity as companies will not be able to find all their vulnerabilities on their own. It takes being able to accept outside help and additional researchers to find solutions. It is a two-sided problem.

The subcommittee has been working with industry, particularly the automobile and medical device industries to institute a safety recall on cyber control systems those are connected to. We have been working with NTIA and expect to continue to work with them in the future. Companies may not understand they are not required to pay for experts to come and search for vulnerabilities. There was previous discussion in the board meeting regarding bug bounties and how and whether people should be paid for discovering vulnerabilities. Some people make money discovering vulnerabilities, and expect to be paid; there are others who do it out of a desire to help. Ms. Wilkerson's committee is examining the situation.

The Joint Encryption Working group filed its end of year report in December. It is available on the committee website. The group is currently in discussion on next steps. They have done two big pushes on automobile cybersecurity. There is a great concern on On-board Diagnostic (OBD) 2 vulnerabilities. There have been good conversations between the industry and other government entities, and work continues. They are looking for an industry process to work with all concerned parties to arrive at a solution that works for all involved.

In healthcare cybersecurity, there is a hearing on Tuesday to talk about preparing cybersecurity for work in public and private health relationships. We are looking at things like the National Health Information Sharing and Analysis Center, their working council, and the Department of Health and Human Services as specific agencies and this ecosystem, this model, of health partnerships that's grown up over the last two decades. We are trying to figure out how we can better strengthen and support them.

The committee has also examined industry information security where it was found that operations and security tend to be at odds with each other. Typically, operations wins, leading to cybersecurity problems within the agency. There is a full report, also on our website, with recommendations to elevate Health and Human Services (HHS) systems to the authority of the CIO. The hope is to balance needs across the agency. A bill to this effect was introduced in the last Congress, but won't be re-introduced this Congress. They are talking to the bill's sponsors to see if there is still interest in looking at the bill. They worked very closely with FDA last year to mitigate serious vulnerabilities that had been exposed. The Mirai hearing last October discussed what could be done about security of devices and how to prevent attacks in the future.

AIP/ASA/AAAS Congressional Fellow, Office of Rep Derek Kilmer

Rebecca Reesman

The Chair welcomed Ms. Rebecca Reesman, AIP/ASA/AAAS Congressional Fellow, Office of Representative Derek Kilmer, to the meeting to update the Board on cybersecurity activities in Representative Kilmer's office. The Board members introduced themselves to the speaker. Ms. Reesman handles cybersecurity and space issues for the congressman. They introduced the State Cyber Resiliency Act to fund FEMA-administered grants for cybersecurity planning and implementations. States may have stated needs for cybersecurity, but when funds are allotted they never see any money. Software cybersecurity tends to take away money from physical security. A report published last year the National Association of CIOs noted that most state cybersecurity budgets didn't spend more than two percent of the allotted amount. It points to a big need.

The goal of the bill is to create a new grant program at DHS specifically for states to use the money for cybersecurity. It's meant be a full lifecycle approach to cybersecurity, in terms of what the money is available for, and it includes efforts to assist with developing the cybersecurity workforce, which is a struggle for the government.

The grant program works in two pieces. The first year, the states get a claiming grant, which allows them to evaluate their needs, and create a cyber plan outlining the vulnerabilities and areas they need to work on, following that the states will receive implementation grants. The program is authorized for five years. It is set up so that state and local CIOs, emergency management officials, and EMT officials are specifically included in the process in order to be sure the operational side is included in the process. The goal is to reach the smaller localities and make sure they get the resources they need.

We worked on this in coordination with the support for this idea from a number of places, associations, including the National Government Association, National Association of State CIOs, National League of Cities, National Association of Counties, and others. The bill is in two committees at least on the House side. It should get bi-partisan support. Administratively, DHS and FEMA will oversee the program. The bill has been submitted without a dollar amount for now. It is difficult to assess how much states will need. The goal moving forward to receive some amount of money for the program, even in a pilot configuration. There is a possibility it could be tied to the infrastructure package talked about by the current administration. There is interest from states in the program and potentially receiving funds.

Final Discussions

Board items –

1. Yesterday letter on voting system modernization. Designation of voting systems as critical infrastructure. Important to look at timely issues.
2. Letters to OMB, DHS. Thoughts on current facts and issues that form common themes.
3. Keep checking on ransomware activity as topic for the future.
4. Topics for meetings: ransomware, Network evolution in the federal government, Next generation identity management, Baldridge update, and visit to NCCoE.
5. Future topic: Blockchain discussion.
6. Revisit the briefings that did not happen this time.
7. Future topic: Bug bounty programs.
8. Future topic: International norms.
9. Future topic Discussion on deterrence.
10. Invite the White House for updates at a future time.
11. Letter: Mr. Boyer will draft the previously discussed letter. Ms. Levin motioned the letter be drawn up, seconded by Mr. Garcia. The letter was approved.
12. The Board can consider privacy related topics for future discussions.
13. Greg will draft letter of appreciation to Mrs. Schmidt in honor of her late husband.

Meeting Adjourned

The meeting adjourned at 11:49 a.m., Eastern Time.

ANNEX A

List of Participants

Last Name	First Name	Affiliation	Role
Scholl	Matt	NIST	DFO / Presenter
Barrett	Matt	NIST	Presenter
Bharwani	Rajesh	House Science Committee	Presenter
Castro	Daniel	Information Technology & Innovation Foundation (remote)	Presenter
Dempsey	Kelley	NIST	Presenter
Dodson	Donna	NIST	Presenter
Hall	Travis	NTIA	Presenter
Hallawell	Arabella	Arbor Networks	Presenter
Jenkins	Neil	DHS	Presenter
Leiserson	Nicholas	Office of Congressman Jim Langevin	Presenter
McQuinn	Alan	Information Technology & Innovation Foundation	Presenter
Mill	Eric	GSA	Presenter
Pascoe	Cherilyn	Senate Commerce Committee	Presenter
Price	Hunter	Department of Defense	Presenter
Reesman	Rebecca	Office of Rep. Derek Kilmer	Presenter
Romine	Chuck	NIST	Presenter
Ross	Ron	NIST	Presenter
Schwartz	Ari	Venable LLC	Presenter
Shannon	Cliff	House Science Committee	Presenter
Stine	Kevin	NIST	Presenter
Wenger	Eric	Cisco	Presenter
Werntz	W. Preston	DHS	Presenter
Wilkerson	Jessica	House Energy and Commerce	Presenter
Drake	Robin	Exetergov	Staff
Salisbury	Warren	Exetergov	Staff
Donelan	Sean	Qmulos LLC	Visitor
Grant	Jeremy	The Chertoff Group	Visitor
Lipner	Steve	SAFECode	Visitor
Mill	Eric	GSA, Tech Transformation Service	Visitor
Nelson	Michael	Cloudflare	Visitor
O'Connell	Veronica	TwinLogic Strategies	Visitor
Geller	Eric	Politico	Visitor/Media
Higgins	Josh	Inside Cybersecurity	Visitor/Media
Mader	Jason	Federal News Radio	Visitor/Media
Marks	Joseph	Nextgov	Visitor/Media
Rockwell	Mark	Federal Computer Week	Visitor/Media
Somers	Meredith	Federal News Radio	Visitor/Media
Weber	Rick	Inside Cybersecurity	Visitor/Media