INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

MINUTES OF MEETING

March 12, 13 and 14, 2014

Residence Inn Washington, DC/Vermont Avenue, 1199 Vermont Avenue NW, Washington, DC, 20005-3519

	Present	
	Board Members	Non-Board Members
Wednesday, March 12, 2014 9:35 A.M. – 3:57 P.M. Thursday, March 13, 2014 9:04 A.M. – 5:02 P.M. Friday, March 14, 2014 9:03 A.M. – 12:06 P.M.	Matthew Thomlinson (Chair), Microsoft Christopher Boyer, AT&T John Centafont, NSA Kevin Fu, University of Michigan Greg Garcia, Garcia Cyber Partners Toby Levin (Retired) Edward Roback, Department of Treasury Gale Stone, Social Security Administration Peter Weinberger, Google, Inc.	Donna Dodson, NIST Matt Scholl, DFO, NIST Annie Sokol, DFO, NIST Tatiana Laszczak, Exeter Government Services, LLC
	Absent with regrets Julie Boughn, DHHS /CMS	

Wednesday, March 12, 2014

Welcome and Remarks

Matt Thomlinson, Chairman, ISPAB
Vice President, Microsoft Security

The ISPAB Chair, Matt Thomlinson, called the meeting to order at 9:35 A.M. Mr. Thomlinson began by asking Mr. Matt Scholl or Ms. Annie Sokol to explain to the Board regarding the FACA regulations governing this meeting. The Federal Register Notice for this meeting was published/announced short of required 15- day notice, and therefore, the Board was allowed to meet and deliberate, but the Board cannot make any decision, vote or gather consensus at this meeting. Hence, the meeting minutes for the last meeting in December cannot be approved at this meeting. If necessary, the Board may set up a separate teleconference/offline meeting to determine/resolve any urgent issues.

Ms. Dodson, Division Chief of the Computer Security Division at NIST, said she wanted to recognize Ms. Annie Sokol for her outstanding performance in managing and facilitating the ISPAB meetings as the Designated Federal Officer. Mr. Thomlinson also thanked Ms. Sokol. Board members provided updates on their recent activities and what they have been doing since the last meeting. The Chair gave a high-level overview of the meeting agenda.

NIST Updates

Donna Dodson, Division Chief, Computer Security Division, NIST
Matt Scholl, Deputy Division Chief, Computer Security Division, NIST

Ms. Dodson congratulated M/s. Thomlinson and Scholl, on receiving 2014 Federal 100 award. The award was given in support of Mr. Thomlinson's role in supporting the U.S. Government and his work with the ISPAB. Mr. Scholl was recognized for his effort on cybersecurity, and the leadership demonstrated within NIST. Ms. Dodson continued by saying NIST appreciates everything they have done in the community and the contributory support role they have provided to the U.S. Government.

Ms. Dodson also mentioned of another Federal 100 recipient, Mr. Lynn McNulty, who was recognized for his tremendous dedication over time to NIST and his outstanding performance and integrity he displayed in the organization. Mr. McNulty, who had passed away, was a former ISPAB member who previously worked at NIST and US Department of State. Mr. McNulty truly believed in the value of public/private partnerships and he instilled this very important philosophy in the people he encountered throughout his professional career. Lynn McNulty was instrumental in promoting ISPAB's values to NIST. Furthermore, both Lynn McNulty and Dr. Patrick Gallagher, Under Secretary of Commerce for Standards and Technology and NIST Director, received an award at recent RSA conference 2014[1]. Mr. McNulty was the recipient for Lifetime Achievement Award, and Dr. Gallagher was awarded Excellence in the Field of Public Policy Award specific for his involvement in the Public Policy on the Cybersecurity Framework.

Ms. Dodson reported that she heard positive feedback on ISPAB at a recent workshop where Ms. Dodson was speaker. The feedback mentioned Board's impact on across the Federal Government and industry. Ms. Dodson reported that NIST is currently in the process of making some minor tweaks to their Cybersecurity and Leadership Program, for which she will have more information in the following weeks. NIST had a very successful Cybersecurity Innovation forum held in October 2013[2] and January 2014[3]. There is a lot of important work being done in Security Automation and Continuous Monitoring, and there is still a lot to be done.

NIST is getting ready to release a hash standard[4] that will have a fixed-size hash and it will have some options that will provide the sponge function that was discussed during the last ISPAB meeting. NIST has always provided people the key size and the algorithm so one would not have to understand too much on the background of the cryptography at hand. Ms. Dodson explained that when one looks at the expanded use of cryptography, that becomes more of a challenge for NIST in terms of the kinds of standards and guidelines that are released. When discussing Cyber Physical Systems of Internet of Things (IOT), one might think of very small, lightweight devices that have tiny sensors in them which how people might want to use cryptography on those devices and they would not necessarily use on other devices to protect different types of information. The challenge is finding the balance of what NIST's cryptographic guidelines to people and how to apply them. NIST would appreciate any advice on this topic from the Board.

Mr. Matt Scholl followed up with the NIST updates and stated on a more granular level that NIST will be

[1] http://www.rsaconference.com/press/20/rsa-r-conference-2014-announces-recipients-of-17th

[2] http://csrc.nist.gov/nccoe/Events/Events.html

[3] http://www.nist.gov/itl/csd/2014-cybersecurity-innovation-forum.cfm

[4] SHA -3 Standard: Permutation-Based Hash and Extendable-Output Functions http://csrc.nist.gov/publications/drafts/fips-202/fips_202_draft.pdf

releasing a recommendation of a Secure Socket Layer (SSL) Transport Layer Security (TLS)[5] document. This is the first instance of the use of crypto in a specific use case. If SHA 1 was being used with a TLS connection, specifically as a signature hash, that may not be appropriate. The challenge is providing clear guidelines for those circumstances which are not black and white but have particular nuances. NIST is evaluating the correct approach to effectively communicate this clearly; but also in a terminology that can be easily understood by the implementers, industry and validator authorities.

NIST recently released Special Publication 800-157[6], [Draft] Guidelines for Derived Personal Identity Verification (PIV) Credentials. This document was created to alleviate the process of inserting PIV card into mobile device, but instead one can now derive a Public Key Infrastructure (PKI) certificate or Common Access Card (CAC) credential that is chained and rooted in an established identity proofing infrastructure. The comment period for is document is for a period of 45 days, closing on April 21, 2104. The Board commented that the civilian government agencies have been waiting a long time for this technology to come out. Mr. Scholl briefly stated that there were a lot of policies that had to be addressed among competing technologies in order to fully understand this process.

NIST representatives attended the Internet Engineering Task Force (IETF) 89[7], London, England, which discussed security automation from an industry perspective. This was an industry lead gathering that focused on the transition of government to industry solutions.

NIST held the launch of the Cybersecurity Framework[8] at the White house in February 2014, at which time the Framework had been released for about a month's time. Mr. Scholl believed that due to the collaborative nature of the Framework, NIST had a huge jumpstart with the release and attributes its success to the NIST folks and their efforts in connecting with the communities during the development of the Cybersecurity Framework. NIST is currently in its outreach phase of the Framework, which is focused on ensuring that people understand the framework and the implementation. Simultaneously, NIST is gathering data on how organizations are using the framework through tapping on insight from the Department of Homeland Security (DHS) C3 Voluntary Program. The framework is not just receiving attention at national level, but also at international level.

In conjunction with the framework, a Privacy Engineering Workshop[9] will be held in April 9, 2014, at NIST. This workshop will be the first of a series focusing on privacy mechanisms, privacy methodologies and privacy engineering. There are new mechanisms in place for risk management from a cyber-perspective and security engineering and would like to take lessons learned from these areas in order to provide a repeatable process.

There are pieces that NIST will initially explore independently from the framework, such as privacy engineering. One of the items the NIST Cybersecurity Framework team looked at were existing privacy standards, guidelines and best practices that could be used as a reference, but also assist people in their own privacy mechanisms within their organizations. It is intended to address many of those gaps in the framework.

---

[5] Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

[6] http://csrc.nist.gov/publications/drafts/800-157/sp800_157_draft.pdf

[7] http://www.ietf.org/meeting/89/

[8] http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework

[9] http://www.nist.gov/itl/csd/privacy-engineering-workshop.cfm

National Cyber Security Center of Excellence (NCCoE) is continuing to work closely with federal agencies such as NSA and DHS, as well as industry partners. A month ago, Officials from the State of Maryland and Montgomery County announced they will provide a Phase 2 facility for the NCCoE. Ms. Dodson stated that, along with the National Security Council, NIST is hosting a workshop with state and local government on the Executive Order to begin to think about the framework build outs. The NCCoE has some interesting build outs regarding use cases with medical devices that are building blocks around automation and access controls which would be working to bring in technologies under the National Strategies to Secure Cyberspace (NSSC).

Mr. Scholl informed the Board that Dr. Gallagher will be leaving NIST and Dr. Willy May will be the Associate Director of NIST until a new director can be decided upon. Donna Dodosn has received a well-deserved promotion to the rank of Senior Technical Staff, in recognition of the outstanding impact that she has had on the NIST and ITL missions in cybersecurity for past years. Therefore, Ms. Dodson will be relinquishing her responsibilities as Division Chief of Computer Security Division at NIST. Matt Scholl will assume the position as Acting Division Chief until a new Division Chief is appointed.

NIST and Plans for Internet of Things (IOT)

- and how NIST plans to address some of the upcoming challenges

Daniel Kent, Senior Director and CTO, US Public Sector, Cisco Systems Inc.
Victoria Pillitteri, IT Security Specialist, Computer Security Division, NIST
Matt Scholl, Deputy Division Chief, Computer Security Division, NIST
James St. Pierre, Deputy Director, Information Technology Laboratory (ITL), NIST

Mr. Daniel Kent will be presenting IOT as a future technology space from the perspectives of an industry leader. The other panelists were to offer NIST different perspectives based on Cyber Physical Systems (CPS) standpoint. Mr. James St. Pierre is coordinating the work on CPS with Vicky Pillitteri as one of NIST's leads on application of CPS through SmartGrid.

The Chair asked the panel to address some questions and comments in particular:

- When one wants a device to function properly and just work, how does one achieve that with minimal servicing cycles?
- How do we achieve resilience?
- How do we achieve common design patterns and security principles for these smaller devices?
- Also, it is one thing to have these devices networked in your home and communicate, but another thing to have these devices talking out to each other through one's firewall.
- And lastly, what is NIST's role in addressing these questions?

Mr. Kent provided an overview of the Cisco perspective of IOT, and according to Cisco research, they determine that 50 billion IOTs will be connected to the internet by 2020. Mr. Kent went on to explain, "What are ***things***"? These are machines (like thermostats), living things (such as animals, plants, etc.), vehicles, appliances, household devices, parking spaces, heart monitors, and many more items that will all be connected to the internet for various reasons. Cisco has been working on how to establish some level of taxonomy among these devices. They looked at the components of IOTs as being sensors and devices. Then one would need the network and storage for those devices, because the devices are sending that data to some type of analytical device (that is the brain of the device). Data analytics provide automation to this process and a control system. Mr. Kent explained as Cisco reviewed the IOT, there were two perspectives that one would need to consider: consumer and industrial IOT. The consumer looks at the worth and how much one is willing to spend on the device. Moreover, how much one would be willing to

pay to secure that data and what is the value of the data. All of that plays into how important the data is. We have seen many use cases with the IOT as low-tech as mining and as high-tech as medical devices. Some additional examples of IOT today are public safety and traffic management. Mr. Kent stated that every industry will be affected by the IOT. Cisco's research indicates that there is value on connecting things to systems to make better decisions in employee productivity and supply chain, which expands out to people and the assets that they own as well as customer experience and innovation. Mr. Kent stated that as we connect the IOT to devices that were not previously on the internet, it provides value to consumers and other industries that were not originally connected.

IOT is a not bad thing because of the added value it will give to industry, however, there are security concerns with IOT. Cisco research is more directed on industrial operations versus IT technologies and what the value of the data is. One would have to take the value of the data and the sensor to have some level of visibility and context awareness. Mr. Kent continued by saying that scaling this out is critical. Lastly, he mentioned that Cisco has some recommendations but they are primarily focused on the industrial perspective of IOT, specifically public safety and how IOT will have some larger value.

Cybersecurity Physical System (CPS) can be thought of as an overarching core context when tying in IOT. Mr. St. Pierre continued his presentation that CPS can be thought of integrated hyper networks of cyber and engineered physical elements. Another key aspect is the co-design element. In other words, these devices are not just plugged in together; there are actual tradeoffs of what goes into the cyber and physical part of the system. These elements are adaptive and predictive and ultimately smarter than just being connected. These devices would enhance performance in a wide range of areas, for example, they respond in real-time, they would be agile and flexible, and have security safeguards in place and offer safety, and communicate machine-to-machine from an IOT perspective. Mr. St. Pierre agreed with Mr. Kent's perspective on the need for taxonomy and definition of standards. There are a lot of different domains where CPS applies. What NIST has been hearing from industry is to provide standard platforms. For example, if one makes something for the medical industry, the importance would be to have a core type of device that is a cross-cutting standard across the industry. Mr. St. Pierre stated that NIST is interested in IOT because of the huge potential impact it will have on the economy. Also, NIST sees a role in developing standards; however, NIST needs to do more work and research on the cross-cutting standards for CPS. NIST is concentrating work on domains at this time using SmartGrid which is considered an integral part of CPS.

NIST has several reports[10] [11] available on CPS, Mr. St. Pierre could provide those links. Those are high-level reports that would help frame the needs of CPS. Some of the critical aspects of CPS focus on co-design standards and having secured network systems, tools that bridge those gaps, and capabilities to predict behavior tradeoff as qualities for these complex systems. In addition, there are integrating multi-scale models for the analytics and uncertainty qualities for interpreting risks into reason, as well as the roles played by humans. NIST's strategy for CPS is focused around three areas: Cybersecurity, Advanced Networking and Timing. The goal is to work with the public and private sectors, which will

[10] http://www.nist.gov/el/upload/12-Cyber-Physical-Systems020113_final.pdf

[11] The three reports are:

- *Strategic R&D Opportunities for 21st Century Cyber-Physical Systems*: provides a high-level perspective on key challenges and research opportunities for advancing CPS; intended to inform decisions about the technology R&D that should be pursued. Available at www.nist.gov/el/upload/12-Cyber-Physical-Systems020113_final.pdf.
- *Strategic Vision and Business Drivers for 21st Century Cyber-Physical Systems*: summarizes the ideas generated during an executive roundtable attended by business and technical leaders, representing a spectrum of applications for CPS, from medicine to energy to manufacturing. Available at www.nist.gov/el/upload/Exec-Roundtable-SumReport-Final-1-30-13.pdf.
- *Foundations for Innovation in Cyber-Physical Systems*: summarizes the results of a workshop where scientists and engineers identified and prioritized technical barriers—including measurement science and standards-related needs—that impede progress. Available at www.nist.gov/el/upload/CPS-WorkshopReport-1-30-13-Final.pdf.

help NIST to identify areas of cross-cutting standards for the CPS program.

Mr. St. Pierre affirmed that partnership of public and private will assist in defining the taxonomy and standards of the CPS. This partnership will hold workshops that will have sub-groups addressing use cases, cybersecurity and timing.

The Board inquired whether there are other standard bodies in other agencies that are also working on these topics and whether they communicate with each other. Mr. St. Pierre stated that they are already working with some ISO IC working groups and there are a number of ad hoc meetings that are taking place. NIST plans and hopes to work with industry and academia to help define standards. NIST would like to designate a Chair for industry and academia within the CPS workshops subgroups. Ultimately, NIST would like to take their outputs and develop standard gaps and measurement challenges, work with the community to define architecture taxonomy, analyze use cases to help validation, and develop cybersecurity recommendations so that they understand what the issues are.

There is a CPS senior steering group at NIST, of which he is currently a member, for which NIST interrelate IOT to other agencies. The group is a government coordination effort that provides direct contact with the other agencies. NIST evaluates use cases from all agencies, and a lot of these agencies have issues with use cases that NIST collaborates on. It is planned to have draft deliverables by October 1, 2014; however, that is subject to change.

NIST will host a two-day CPS workshop[12] about the cyber security needed for cyber-physical systems (CPSs), with a focus on results of research and real-world deployment experiences, and an official announcement should be released on March 26, 2014. NIST will attend a large CPS workshop in Berlin, Germany in April, and an Institute of Electrical and Electronics Engineers (IEEE) workshop in San Diego, CA the week after.

Ms. Pillitteri reported that there has been collaborative work on cybersecurity and CPS with Committee for Nuclear Regulatory Activities (CNRA) that hosted a workshop in April 2013. The first step should be to develop a solid definition of CPS. NIST has already a working internal definition, but it is necessary to have one common standard that essentially from the output of the workshop. CPS is included in programs such as SmartGrid, but the definition of CPS that is also considered as IOT may or may not be co-designed and co-engineered. NIST will have to find the common drivers amongst a diverse group of agencies. Ms. Pillitteri continued that the intent is for the CPS three sub groups to work in parallel; however, the challenge remains in how NIST would define standards on CPS when nothing is defined at present. Ms. Pillitteri asked the Board's advice on what they think the best approach would be. For example, should NIST focus on defining CPS first or developing the architecture or should the use cases fuel the architecture. Ms. Pillitteri stated that ultimately they would like to make this an efficient process.

The Board noted that some of the discussion today was about protecting the data, which is important, but it is mainly about protecting the consequences of the use of data and the interdependencies of systems of what could happen to it. What is the thinking of how to address this? For example, if one was to pick a system such as transportation and if something goes wrong, the risk is loss of life. Is NIST thinking about the risk management aspect of CPS? The Board remarked that due to the IOT nature, the risk management would be multiplied significantly.

Mr. Scholl replied that it is about protecting the data but also about trusting the analytics, their accuracy, and at the part level how well the sensor is taking measurements. All of these items comprise an active

[12] http://direct-connect.infosecisland.com/documentview/21037-NIST-Workshop-Cybersecurity-for-Cyber-Physical-Systems.html; http://www.nist.gov/el/upload/CPS-WorkshopReport-1-30-13-Final.pdf

internal discussion at NIST. It is also necessary to address concern of the transmission and maintenance of the information. NIST will need to have some use cases to decipher the analytics.

Agencies' Challenges in Implementing NIST Special Publication (SP) 800-53Appendix J

Martha Landesberg, U.S. Department of Homeland Security, Privacy

Ms. Landesberg thanked the Board for inviting her and said that her presentation is based on her experience in DHS and SP 800-53 Appendix J[13] document that was released in April 2013. She stated that the Appendix J document was to assist agencies with a standard privacy plan. The challenges in developing the document were taking privacy controls and embedding them into cyber controls. Upon release of this document and an impactful statement was sent to other agencies emphasizing this as a strong requirement. Some of the initial thoughts on this document were based on two communities: privacy and security within an organization. Ms. Landesberg explained that there were some initial issues with the implementation of this document. For example, stating that the security officials were not familiar with the privacy terms that were referenced in Appendix J and that the privacy officials in the agencies were not aware of the security controls provided in SP 800-53. DHS became aware of this issue during the implementation stage of Appendix J and one of the challenges was to get the two communities to communicate with each other. Ms. Landesberg emphasized that this is a new way of thinking for some agencies. In the privacy portion of the document, each agency is required to have a privacy plan and do the necessary training. A new process in this requirement is to have a Chief Privacy Officer at each agency oversee and approve the access controls in Appendix J.

DHS is working to embed the privacy controls in SP 800-53 Appendix J into DHS's internal guidance manual. This will be a heavy socialization process, but this will be a marginal effort for DHS due to the deeply embedded privacy network throughout DHS. When DHS worked to build the framework as to how to implement SP 800-53 Appendix J, they realized that it was important to find a common language that the privacy personnel could understand.

The timing to implement is based on the Office of Management and Budget (OMB) requirement that legacy programs have a year to implement all the new controls and new non-pre-existing programs have to implement from the anniversary date by April 4, 2014. These are some of the challenges that DHS is seeing specifically related to SP 800-53 Appendix J.

Since SP 800-53 Appendix J is a new process, training needs to be organized for all agencies. There are some interagency training initiatives that were developed in the Best Practices sub-committee of the CIO Privacy Council; however, the Education sub-committee will be taking over the training initiatives from this point on. Also, the International Association of Privacy Professionals (IAPP) organizes a Federal Privacy Series annually, at which Ms. Landesberg presented last December. There were a lot of questions regarding these new requirements and a lot of questions remain today. The CIO Council[14] for Privacy sub-committee for Best Practices developed several PowerPoint modules to help train the trainer for agencies. The training was based on a federal survey on what types of training are needed. The DHS Education sub-committee will be putting together an Appendix J workshop that will assist with the training effort, and the PPT modules developed are awaiting approval from the CIO Privacy Council. Also, the DHS Best Practices Privacy Sub-committee was tasked to work with Federal Risk and Authorization Management Program (FedRAMP) at GSA to develop an approval process in regards to SP 800-53 Appendix J for cloud service providers.

[13] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[14] https://cio.gov/about/groups/; https://cio.gov/about/groups/privacy-cop/

The Board would like to know who is responsible for the process for including continuous monitoring and incident response in the context of SP 800-53 Appendix J. Martha Landesberg responded that it is responsibilities of every agency's Privacy Officer to report incidents. While she is able to described DHS's incident response process, the process for incident response varies from agency to agency. DHS's incident response educates all employees to report an incident also to the agency's Privacy Officer. DHS has a mature process in place and an incident response Privacy Officer is in charge of monitoring the databases. When an incident occurs, it is reported to U.S. CERT within one hour. There is an incident process in SP 800-53 Appendix J.

In response to the Board's question on whether an individual is contacted directly when a privacy breach occurs, Ms. Landesberg stated that it depends on nature of the breach and the type of data compromised. For example, if a social security number was compromised, then the individual would be contacted. In the event that an email was accidently sent out within the agency or department with sensitive information, it would be considered an internal privacy incident and it would be addressed in a different way. The incident response data is captured and the Chief Information Security Officers (CISO) reviews the statistics and provides quarterly internal reports. DHS also annually provide incident data to congress. DHS currently has a working group working on updating SP 800-53A Rev.1[15], *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, which covers metrics in regards to the requirements of SP 800-53 Appendix J. DHS will collaborate with NIST as this project progresses.

As to whether there are any real impactful changes or it is simply just a formal documentation of changes from SP 800-53 Appendix J, Ms. Landesberg believes the metrics developed proved to be valuable since implementing the requirements from SP 800-53 Appendix J. For those agencies with small privacy offices or few privacy officials, it will require more work for them. When developing drafts for SP 800-53 Appendix J, DHS organized four workshops and three public comment sessions with NIST help. Many agencies asked why it is necessary to add Appendix J. It is necessary to incorporate privacy controls in implementing security controls especially there were not a lot of controls set in place that communicated between privacy and security.

The Board asked if controls in Appendix J are focused on agencies that do not have a mature process in place as DHS, and whether the roadmap for SP 800-53 Appendix J is intended to provide a privacy plan for other agencies. Ms. Landesberg affirmed that SP 800-53 Appendix J is fully functional standard and there is no intention to raise the bar on privacy. SP 800-53 Appendix J recognizes certain privacy act requirements that many privacy staff may not consider as important as others. DHS had a head start as the first federal agency to have a mature privacy plan.

[15] http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

Transportation Sector and Vehicle-to-Vehicle

Suzanne Lightman, Computer Security Division, NIST

Ms. Lightman introduced the vision that is driving the vehicle-to-vehicle communication called Smart Transportation[16]. This concept is for all vehicles and transportation infrastructures to communicate with one another seamlessly and autonomously. This concept also allows communication with roads, tunnels, and manufacturers. Ms. Lightman explained that there are a lot of reasons for this concept and the enormous push for this is safety. The World Health Organization reported 1.24 million accidents that ended in death were reported in 2012, which is believed to be under reported. The government safety organizations around the world see Smart Transportation as a way to reduce that estimate by 75% – 99%. In addition, Ms. Lightman said from a government perspective is to focus on efficiency.

The big problem that the government has is that the roads are insufficient, overcrowded and new infrastructure is expensive. However, automated vehicles would provide a solution to these issues. For example, instead of building a new beltway, the government could use automated cars to put more vehicles on the existing beltway which would be overall less expensive. The theory behind this concept is called the "grains of rice scenario," i.e., when grains of rice are poured quickly through a funnel, a bottleneck happens quickly. However, the rice flows through easily and quickly when the grains are poured through slowly. This scenario is commonly used when describing the theory behind automated cars. The real issue is how to implement automated cars from today and that lifespans of non-automated cars are long.

Today, there are cars that have significant capabilities of automation and cars on the road that do not have any automation. Many in the auto industry are actively interested but they do not have the cutting edge of innovation. There are several reasons for this scenario. For example, there are concerns for accepting significant fault as and when something goes wrong with the innovation. Car manufacturers cannot afford to take on any possible expense setback because these are expensive purchases that people do not regularly invest in. They also are innately conservative about advertising the concept of automated car. Besides safety regulations, other issues have a bearing on cybersecurity concerns revolving around vehicle-to-vehicle communication. For example, there are concerns of what needs to be done when control is transferred or hijacked.

There are other issues relating to cybersecurity such as a central control for automated vehicles. There were incidents where hobbyists altered the setting of vehicles so as to get more engine power which resulted to damage to the vehicles. The hobbyists simply reconfigured back to the factory setting before returning the car to the dealer for repair. Car companies are in a constant battle in developing new security features as criminal adversaries are able to quickly counter with new reverse-engineer solutions. Ms. Lightman offered a list of critical cybersecurity issues and concerns with particular focus on vehicle communication:

- Communication within the vehicle itself
- Different systems communicate within each other and run through a single bus
- Vehicle-to-Vehicle communication
- Grid-to-Vehicle communication (roads talk to vehicles)
- Car Company Communication to the Vehicle
- Confidentiality
- Integrity
- Availability
- Bandwidth

[16] http://www.ssti.us/; http://www.smartgrowthamerica.org/documents/the-innovative-dot-second-edition.pdf

The other concerns center on interface with the actual functions about the criminal element to the car companies such as the complication to interfere with the system while the car is in motion and efficiency of the safety locks system. This is the concern with latency, e.g. the car on the road must be able to react to real-time events without delay. Some additional emerging issues are monitoring and privacy. It is a huge issue for vehicle that has an identifier (tags) and from a black box car insurance perspective, to track the vehicle via black box and impact on insurance rates.

In order to deal with issue of data ownership and control of who owns one's data, the Society of Automotive Engineers (SAE), which is an organization known for providing the auto industry standards that are generally accepted automotive principles, has created a committee called the Electrical System Security Committee with three sub-committees: Supply Chain, Auto Cybersecurity, and a Research Focus. These sub-committees are comprised of major manufactures, supply chain members, and various governments. The Department of Transportation (DOT) NHTSA that is actively involved in this area and has its own cybersecurity division. The division is concentrating on vehicle-to-vehicle communication and internal infotainment systems. At this point, NHTSA does not have any standard and there is no emerging factor for the manufacturers to progress in this area.

Car manufacturers resist any attempt to be interoperable or integrated. Car manufacturers will not share any information on security vulnerabilities among them unless in most extreme necessities. They have many de facto standards and not many formal standards in place. There are safety regulations through U.S. National Highway Traffic Safety Administration (NHTSA), but those standards differ from the European Union (EU) and Asia Pacific countries. Car manufacturers desire to have formal standards applicable for all countries.

Although this concept has its benefits and issues, it is about finding the proper approach of how to move forward, addressing cybersecurity issues, and considering the wide spectrum of the automotive vehicles. The complication is that car manufacturers do not want to cooperate with each other. From business perspective, the car manufacturers are highly competitive but are operating on margins. The car manufacturers are competing and have no agreement on margins. They each want to be able to provide competitive features that are not offered by the others.

NHTSA would like to work with car manufacturers to develop guidelines that can be implemented by car manufacturers. A potential output of this collaboration would be input and involvement to the establishment of Smart Car regulation within the car industry. NHTSA's security division has been in the process of restructuring. They have engaged NIST but from a minor perspective. They have not progressed far to start any type of collaboration with NIST. NHTSA will initiate a dialog with nist as soon as restructuring is settled.

U.S. Department of Homeland Security (DHS) C3Voluntary Program – Critical Infrastructure Cybersecurity[17]

Thad Odderstol, U.S. Department of Homeland Security
Kevin Dillon, U.S. Department of Homeland Security

Mr. Dillon is from the Cybersecurity Communication, Stakeholder Engagement Division at DHS, and he explained his branch's main focus is to adopt the *Framework for Improving Critical Infrastructure Cybersecurity*[18]. DHS is to focus on industry engagement of the Framework management, with respect to

[17] http://www.dhs.gov/blog/2014/02/12/dhs-launches-c%C2%B3-voluntary-program

[18] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

the public partner relationship.

Mr. Odderstol is from the Chief Stakeholder Risk Assessment and Mitigation branch of DHS, and he provided a brief overview of DHS's main focus of adopting the Framework. The major efforts are focused on encouraging adoption of the Framework. The approach taken to support adoption efforts has been to create the C3 Voluntary Program to advance the department's mission for critical infrastructure resilience while also addressing the Framework and engaging the cybersecurity community. Thad Odderstol stated that in support of the their coordination efforts, they tried to take a step forward in coordinating across the departments and sectors, including Federal, state and local government, and private sector partners to support on a national level. This effort not only supports the Framework adoption, but also focuses on the enhancement of their partnership efforts.

The C3 Voluntary Program has three major goals:

1. Support Cybersecurity Infrastructure
2. Increase awareness of the NIST Framework
3. Support efforts by sectors and organizations to address cyber as an all-hazards approach to enterprise risk management

The three primary activities in supporting these goals are:

1. Converging critical infrastructure community resources to be able to support cybersecurity risk management resilience
2. Connecting critical infrastructure stakeholders to the national resilience efforts
3. Coordinating critical infrastructure call centers to be able to maximize the national effort

Mr. Odderstol provided a brief explanation for each primary activity, beginning with their convergence efforts. In order to assist in this effort, they consolidated all of the department resources that support cyber for the national critical infrastructure on the U.S. CERT.gov website. They created a new portion on the website which aligns those resources with the NIST core functions of the Framework and partitioned it by stakeholders (Federal, state and local government, and the private sector). The alignment represents what the C3 Program can offer to reinforce risk management and resilience, while also reinforcing the principles of the Framework. The vision of this program as it evolves across the public and private sectors is to increase the amount of resources that are available on the website. Currently, it is only the department resources that are available but the C3 program would like to add cross-sector efforts. The idea is to promote sectors that have their own approach to adopting the Framework and critical infrastructure.

To support this collaboration effort, C3 is engaging partners directly from Federal, state and local government and private sector communities. The program is focused on engaging key stakeholders in the business communities that can support business-to-business drivers for industry to pursue adoption of the Framework. The program is assisting with awareness efforts and mentoring opportunities to engage small and medium size businesses. Efforts continue working sector-to-sector to develop strategies. This was a defined requirement from the Executive Order (EO) to work with each sector in order to develop implementation guidance. The approach focuses on questions such as:

- *How can C3 focus efforts to build and increase awareness of cybersecurity risks?*
- *How can the organization understand where the sector wants to focus its engagement in order to adopt the Framework?*

Lastly, Mr. Odderstol explained their support of coordinating efforts. He mentioned that the program is continuing to support outreach with each sector and their partners within the business communities as well as the cross-sector communities. Some of the assistance that has been provided by the department to support the Framework adoption is the development of awareness campaigns. These campaigns consist of webinars with industry associations, state and local government, and sector partners. The program is also providing outreach collateral self-service options on the U.S. CERT C3 Program portion of the website. The tools provided are messaging kits, FAQs, sample blogs and social media content, and leadership content. The goal is to provide as much information as possible to help promote awareness and participation.

Mr. Odderstol explained that they have done assessments on sectors but ultimately it is up to the individual sector to build out the strategy of implementation with their organization. The C3 Voluntary program is available in a support capacity to these different sectors.

The Board commented that given the fact that this is a voluntary implementation, how does one assess compliance and evaluate whether or not the Framework is in fact being successfully used within a sector. Mr. Odderstol explained that they are not assessing compliance issues on how the Framework is being used because they have no authority given that it is a voluntary program. He stated that the program is trying to drive participation and engagement and reinforce the use of the Framework.

The Board clarified by stating that there is not a conformance assessment but more of a drive to build out a sector specific implementation strategy. Then each sector would have to do their own assessment and evaluation on how well it's being used within their organization. Mr. Odderstol agreed with the Board and reiterated that they are in a supporting role, but if there is interest, they can combine some of the work they are doing now with some past programs to assist sectors better. He also mentioned that they can help recommend or point out types of vulnerabilities for sectors but the idea is not to duplicate their efforts. The goal is to work with sectors in any capacity possible in order to support the Framework and critical infrastructure. To date, the C3 Program has organized fifteen webinars to support the Framework adoption and is averaging 1 to 2 webinars a day.

The initial focus within the first year of the program is to build momentum with each one of their stakeholder's communities and increase awareness. Mr. Odderstol stated that they target every sector in their awareness activities. Most of the feedback they received is geared towards the programs and the services they offer, and they forward any feedback about the Framework to NIST.

Mr. Dillon began by stating that they have had the Cybersecurity Resilience Review (CRR) methodology since 2009. The CRR to date has done 300 onsite reviews including state and local government and private sector risk management reviews. The Executive Order 13636[19] created an additional purpose to develop a self-service tool and forced an acceleration of the capability to conduct CRR. The CRR has aligned with the Framework in collaboration with NIST, and a user guide to resilience management model is created to assist with having an operational repeatable process. Some of the key principles to this process include Asset Management, Configuration Management, Change Management, Controls Management, external Entities Management, Incident Management, Risk Management, and Training Awareness. The CRR program is adjusted according on the audience but it enforces these repeatable process areas as well as the Framework. DHS perform this review at no cost to the entity. The goal is not to use it as an audit; but to be able to eliminate barriers by using self-service tools, full question guidance, and a self-assessment package. The Board would be interested in the data of comparison of entities and possible further discussion at another meeting.

[19] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Updates on NIST Cryptographic Process
Donna Dodson, Division Chief, Computer Security Division, NIST
Andrew Regenscheid, Computer Scientist, Computer Security Division, NIST

Ms. Dodson began by thanking the Board members for attending the NIST's primary advisory committee, Visiting Committee on Advanced Technology (VCAT)[20] meeting in February 2014[21] (see Annex B for agenda and attendees), which was discussed in the ISPAB December 2013 meeting. The outcome from VCAT February meeting required current sets of mandates and directions that requires responses and be able to look long range at NIST's research programs. The VCAT charged Dr. Gallagher with the task to setup a Committee of Visitors (COV) to help NIST examine of their cryptography work. Ms. Dodson would like to present a brief overview and then take a few questions from the Board. Mr. Regenscheid mentioned that the goal of this session was to gather input for a report back to the VCAT for the next meeting in June 2014. The VCAT will be inviting external experts on to the COV to help NIST develop recommendations. There are two major areas that the VCAT is interested in receiving feedback on:

1) Reviewing NIST's processes that they use to develop their standards
2) Reviewing NIST's existing set of publications and ensuring that those publications were developed in accordance with NIST's principles and that they meet the level of technical excellence that community has come to expect from NIST.

The purpose of this document was to help the community understand how NIST has developing their crypto publications and would like to open a dialog with the community to receive feedback. Furthermore, VCAT is requesting feedback with respect to NIST principles for developing NIST crypto publications and does NIST have effective mechanisms in place for communicating to the community. Mr. Regenscheid is looking to gather inputs how to best use the COV's from this session and everyone else's time through June. Since the last meeting, a short document[22], Draft NIST Interagency Report 7977[23], *NIST Cryptographic Standards and Guidelines Development Process*, about our process regarding publications was shared. NIST released that document mid-February for public comment (allowing a 60-day comment period) based on the Board's feedback from the last meeting.

The Board inquired whether NIST decided to explore discussion on Random Bit Generator Number during this public comment period. Matt Scholl, Deputy Division Chief, Computer Security Division, NIST, confirmed that it was decided not to pursue this discussion so as not to divert from the main focus to this particular issue.

Ms. Dodson believed that the people no longer have the level of comfort in this process. NIST IR 7977 asked specific questions and also explained how NIST intend to handle the feedback. There were few comments received as of this point, but most comments[24] are usually submitted closer to the close of the comment period.

Mr. Regenscheid reported that the COV will be conducting a review of NIST's existing body of

[20] http://www.nist.gov/director/vcat/vcat-051414.cfm

[21] Meeting minutes http://www.nist.gov/director/vcat/upload/Final-Feb-2014-Minutes.pdf

[22] http://csrc.nist.gov/groups/ST/crypto-review/

[23] http://csrc.nist.gov/publications/drafts/nistir-7977/nistir_7977_draft.pdf

[24] http://csrc.nist.gov/groups/ST/crypto-review/public-comments-nistir7977.pdf

cryptography publications (30 in scope documents) and he asked specifically as to how NIST should structure this review to ultimately produce information that fits COV's need to conduct the review. NIST is turning to COV to pick the publications that they would like to focus on. Andy Regenscheid reported that they have time to provide some information to the COV depending on the question of appropriate information.

The Board noted that the feedback consists of two things: the posts with the specific content of the questions that were asked in the public comment document and how to have a process that is to protect NIST against assertion of bad faith. The Board considered that it would be useful to publish NIST's decision process of the crypto algorithm associated with the random bit number generator, and this would protect NIST for future concerns. Ms. Dodson stated that reports were posted on the selection process on the NIST website. She also suggested the cryptography algorithms and SHA 1 would be good publications for COV review. It might be more of a sampling than the 30 publications. The Board recommended starting the review with the focus on content of the publications and then process before searching for unpublished public deliberations.

Thursday, March 13, 2014

National Security Staff (NSS) Update

J. Michael Daniel, National Security Staff, The White House

Mr. Daniel thanked the Board for inviting him to the Board. He began by providing an overview of the NSS cybersecurity directorates for FY 14. NSS has five broad areas of focus:

1) Protection of U.S. Critical Infrastructure and what the NSS is doing to improve it. This area has had some positive visibility due to the release of the Cybersecurity Framework. The first NSS effort is on improving information sharing between the private sector and the government.
2) Focus on security of the Federal governments' networks – whether classified or unclassified.
3) Improving the ability for incident response and mitigation including law enforcement capabilities, including the management of federal government responses when incidents do occur. This includes responding appropriately, quickly and effectively to address the problem so that a recovery can occur quickly.
4) Focus on international governance of cyberspace in which there are several different efforts going on in this specific area. The key focus is internet governance and the technical management of the internet. Some foreign governments want to control it.
5) Lastly, NSS is focused on the future, specifically hardware, software and business practices of cybersecurity and make them inherently more secure. This is directed at economics and human factors behind the malware market and the impact on economies.

Cross Agency Priorities for FY15-17

John Banghart, Director for Federal Agency Cybersecurity, National Security Staff, The White House
Trevor H. Rudolph, Office of E-Government & IT, OMB, Executive Office of the President

Mr. Banghart began by providing an overview of cross agency initiatives and goals. He provided a brief history of the CAP goals[25] as a refresher. The CAP goals were initially setup in 2010 when the legislation was passed and the first CAP goal went into effect in 2012. The CAP goals concept was to survey the entire Federal government and identify the areas that the White House would want to have some particular focus, not just limited to cybersecurity.

Mr. Banghart explained the way the CAP goals are structured and developed is that they form a committee and develop an interagency process that includes three to five areas across the Federal government. In this committee they ask questions such as "Where are our weaknesses and where do we need to drive more consistency between agencies?" Also, CAP is generally focused on classified and non-national security systems. Identified areas within the cybersecurity focus include:

- Trusted Internet Connection (TIC) – Trying to drive down the number of access points that the Federal government agencies have to the internet
- HSPD-12 (which is the PIV card adoption)
- Continuous Monitoring (in a general sense)

Every quarter, CAP goals data is collected over a set of metrics that's developed for each one of the identified priorities, and the information is available publically on www.performance.gov (CAP Quarterly

[25] http://goals.performance.gov

Reports). These quarterly reports provide a clear idea of agencies performance. The charts breakdown by agency and provide metrics on whether any agency met their target metrics. These reports provide extremely useful information with a cross section view of unclassified networks by agencies and their success rates. There is a follow-on process in the White House called a CyberStat which a meeting set-up with a particular agency, the National Security Council from OMB, CAP Goal Members, and leadership from the specific agency so as to discuss how best to achieve their goals. These reports are being used by the White House and agency leadership to make changes.

The subsequent set of goals was developed in November 2013 for CAP goals FY15. NSS set-up working groups called JFY15 for CAP goals. U.S. CERT and the National Security agency present a briefing on what they thought were currently most significant threats, and how to share services while being cost effective. These are the three goals: Continuous diagnostic and mitigation (ICM, CVM programs etc.), changing the focus to Identifiable Credentials Access Management (ICAM) instead of the PIV cards, and anti-phishing which a significant issue particularly on the civilian side. There are many inconsistencies across the agencies and the question moving forward is how to manage this from a budget perspective and from an overall perspective.

FISMA and Continuous Monitoring – OMB memo update

Trevor H. Rudolph, Office of E-Government & IT, OMB, Executive Office of the President

Mr. Rudolph presented an overview of OMB's top priorities and goals. The initial effort to move away from static reauthorization process was to create a policy framework for enabling agencies to monitor their own systems in an ongoing basis. To meet this goal, OMB found that they needed to create the technological infrastructure within agencies. Ultimately, the infrastructure is going to be in the form of local or agency level dashboards and that every agency will report up to the continuing monitoring metrics as well as continuous diagnostic mitigation. He mentioned that they are hopeful for real-time awareness from cybersecurity threats and vulnerabilities across the Federal space.

For technological infrastructure, they realized there were some gaps in agencies regarding policy for cybersecurity defenses. This was addressed among OMB, the National Security Council and the GSA working together to create a government wide blanket purchase agreement (BPA). This BPA can be used by Federal, State, Local, and Tribal governments. The purpose of the BPA is to establish a basic set of continuous monitoring tools at their respective agencies. For example, if an agency lacked the tool for that specific infrastructure, they could use the BPA to fill that gap and the Continuous Diagnostic and Mitigation (CDM) program through DHS will pay for it. To date, the first Task Order on the BPA was awarded in January 2014 and the total value was $41M. DHS did a comparison of the BPA to the IT GSA-70 schedule and estimates that the agencies cut their costs by 30% using the BPA.

Federal Communications Commission Works in Cybersecurity

Clete D. Johnson, Chief Counsel for Cybersecurity, Public Safety and Homeland Security Bureau, Federal Communications Commission

Mr. Johnson began by providing a brief overview of FCC's role in the cybersecurity initiative. He stated that the FCC is mostly focused on security resilience of networks, public safety and national safety. Currently, communications including crucial public services like "911" emergency learning systems, rely heavily upon IP based networks. A question that the FCC has been asking is how to help build those responsibilities for the public to ensure security and resilience. The FCC has a lot of network expertise within the government – for example – communication networks operate, where they are vulnerable and be resilient.

Mr. Johnson emphasized that the Chairman of the department has been clear in the vision for the agency and he would like the FCC to play the role that it needs to play not what the FCC wants to play in relation to interagency collaboration. The FCC sees a role in bringing coherence to the initiatives processes that tailor to the Cybersecurity Framework including the DHS C3 Voluntary Program. The FCC believes that the availability of voluntary programs is the best way to approach the adoption efforts of the Framework.

The FCC has a separate entity of this work called the Communication Security Reliability Interoperability Council[26] (CSRIC). FCC works with industry and agencies to build best practices and processes using the NIST Cybersecurity Framework. FCC is expecting the 4th session of CSRIC to encourage implementation to cybersecurity. The 4th session speaks to implementation to the Cybersecurity Framework. CSRIC provides recommendations to FCC and helps FCC with guiding the Framework. For the first time, there is a public and private guide to managing corporate risk and if you include cyber vulnerability. With regards to documentation of the FCC process, all activities will be transparent and available to the public and all discussions are open to public participation. The FCC works closely with NIST and DHS, and engages public private sector stakeholders.

GAO Report of GAO-14-34,[27] *Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*

Greg Wilshusen, Director, Information Security Issues, Government Accountability Office (GAO)

The main focus was to provide the Board with a review of the GAO-14-34 report, which is to capture agency responses to data breaches of Personally Identifiable Information (PII). Mr. Wilshusen briefly reported that the work on Smart Card update is still ongoing and currently in the audit phase. It is worthwhile for the Board to follow up in the future.

Some background information on the GAO-14-34 report: it was requested by U.S. Senators: Parker, Colbert, and Collins as members of the Homeland Security Government Affairs Committee. The scope of this report consisted of eight agencies: Centers for Medicare and Medicaid (CMS), Department of the Army, Veterans Affairs (VA), Federal Deposit Insurance Corporation (FDIC), Federal Reserve Bank (FRB), Foreign Investment Review Board (FIRB), Internal Revenue Service (IRS), and the Security & Exchange Commission (SEC). The GAO reviewed three large institutions and three independent agencies that had a large number of systems that contained PII information. GAO specifically selected the VA and the Federal Advisory Board based on their data breaches.

There were two objectives in evaluating these agencies. The first objective was to assess the extent to which agencies had developed and documented their policies and procedures for responding to the data breaches. This includes determining how well agencies have implemented those policies and procedures. The second objective was in regard to the role of DHS and U.S. CERT and the services they provide to agencies in response to these types of data breaches. Mr. Wilshusen explained that they used FISMA criteria which require agencies to develop policies and procedures for detecting and responding to breaches of systems. The other reference used was OMB memo M-07-16[28], *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, which details reporting of PII incidents to U.S. CERT.

[26] http://transition.fcc.gov/pshs/advisory/csric/

[27] http://www.gao.gov/products/GAO-14-34

[28] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

Mr. Wilshusen explained that GAO drilled down and evaluated two key management practices and four operational practices. For example, the key management practices established a data breach response team instead of waiting for an incident to occur – *decide who is going to do what and when* – and that the response team consists of senior officials that can make decisions and move resources if necessary. Secondly, response awareness is to train employees on the roles and responsibilities in responding to the data breach. The four operational areas consisted of preparing reports, suspected data breaches and submitting to the U.S. CERT and also internally in the organization. Thirdly, assessing the level of impact within the agency and offering assistance, and, finally, analyzing the breach response and lessons learned.

The report findings were that generally agencies had the policies and procedures in place to support these practice areas regarding data breaches but their implementation was inconsistent. Agencies, for example, have mentioned that reporting an incident within one hour is difficult. Many times the data they get within one hour is not valuable. As a result of the findings, GAO made twenty-two recommendations. The Board would like to explore if those two ongoing efforts that identify cyber and non-cyber incidents were reported to U.S. CERT and the number of PII incidents are non-cyber security incidents. For example, if 400 incidents are reported to the U.S. CERT, that number is misleading if cyber and non-cyber incidents are not distinguished.

Updates on FedRAMP

Sabari Gupta, President and CEO, Electrosoft (Presentation[29] provided)

Mr. Thomlinson introduced the speaker Ms. Sabari Gupta and stated that she is going to provide a company perspective of the FEDRAMP and the implementation process. Mr. Scholl added that Dr. Sabari Gupta is going to discuss the certification process of GSA through the Joint Authorization Board (JAB) to be a certified 3PAO assessor and then certifying the CLOUD providers through FedRAMP.

Ms. Gupta gave an overview of her company (ElectroSoft, see PPT slides). She said that her company is a management and technology services company with a focus on identity management and cybersecurity. In discussing FedRAMP and FISMA, Electrosoft has been doing FISMA work since 2006 and FedRAMP work since 2012. ElectroSoft has worked on FedRAMP and FISMA such as gap analysis, mentor organizations, policy and procedure development for government customers and a private industry, assisted government customers with developing SSPs required by FISMA, third-party independent assessments as the assessor, and continuous monitoring.

Electrosoft has been a collaborator and supporter of NIST since 2001. Dr. Gupta will be providing her company's perspective on the FedRAMP assessments as a 3PAO certification assessor. ElectroSoft has also done other assessments and audits such as PKI and HSPD-12, but would like to focus on the 3PAO certification process and provide the Board some insight in reference to the 3PAO Accreditation process, market demand. An overview of the 3PAO process was presented and included details on Electrosoft's 3PAO accreditation in January 2012, which was also beginning of FedRAMP's JAB accreditation process. She mentioned that the process was not too difficult based on the company's expertise. There were no site visits but a lot of documentation submitted including responding to two round of JAB feedback, and phone interviews with the JAB. The tests were conducted on submitted artifacts. For example, she stated that the submissions were related to the ISO 17020 standard and the documents submitted were geared toward providing a mock assessment in terms of the System Security Plans (SSPs). The SSP had to have certain weaknesses and a security assessment report spreadsheet was

[29] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-03/fedramp_ispab_march_2014.pdf

submitted. The JAB wanted to ensure that they understood the process based on the documents submitted. They received their accreditation in August 2012.

Ms. Gupta stated that there is no requirement to have FISMA completed prior to accreditation because it was not initiated. Re-accreditation is required to be completed annually. The process changed from being a JAB lead government process to now being run by a third-party accreditation party. Initially, there were no fees or costs associated with this accreditation process, and applicants will be doing all the work. The hardest part was documenting the process.

Electrosoft is due for re-accreditation this year. The third-party organization that is providing the accreditation certifications is called the American Association for Laboratory Accreditation[30] (A2LA). The A2LA started in November 2013 and recently began accepting 3PAO applications. A2LA established a calendar for existing 3PAO's to go through the accreditation process. Ms. Gupta stated that based on their start date A2LA gave them a target date of July 2014. ElectroSoft has started the process but it is not to submit early. Although she cannot comment on the entire process because she has not gone through it yet, she does have some concerns based on the website statement of requiring submitting four recent 2PAOs. Ms. Gupta noted that there has not been many 3PAO's that have supported the entire FedRAMP process so four entries is a relatively large number. The cycle will be a yearly cycle and cost as much as $10,000 or more to do the re-accreditation. This high cost may prompt many companies to evaluate the justification for acquiring the accreditation. Furthermore, there is a new requirement for an on-site inspection.

On gauging market reaction to the process and cost of accreditation, Ms. Gupta responded that ElectroSoft receives on average 2 to 4 inquiries a month (see PPT slide 7). The inquiries from Cloud Service Providers (CSPs) who are interested in getting FedRAMP, are generally of a consulting nature and the organizations are not ready for auditing services. Government customers are frequently unwilling to cover for high FedRAMP costs ($200k to $5M, see PPT slide 9). In addition, CSPs are overwhelmed by all the controls that the FedRAMP process requires. According to the information on FedRAMP website[31], there are twelve CSPs with JAB authorization, four CSPs with agency FedRAMP authorization, and three CSPs in the testing phase.

In closing, Dr. Gupta provided some potential concerns and issues moving forward:

- Extreme rigor and cost of FedRAMP JAB Authorization may slow cloud adoption by agencies
- FedRAMP Agency Authorization may represent more cost-effective approach in the near-term
- Many CSPs waiting for dust to settle before embarking on grueling path to FedRAMP

[30] https://www.a2la.org/

[31] http://cloud.cio.gov/fedramp/cloud-systems

Friday, March 14, 2014

Mr. Thomlinson called the meeting to order and introduced the first presenters this morning. He explained they will be discussing the idea of quantum computers. He offered a question regarding how one might prepare for the possibility of quantum computers.

Quantum World and How NIST is Preparing for Future Crypto

Dustin Moody, Computer Scientist, Computer Security Division, NIST (Presentation[32] provided)
Andrew Regenscheid, Computer Scientist, Computer Security Division, NIST

Dr. Moody began with an overview of the NIST Quantum Cryptography project and an overview of why quantum computers are necessary (See PPT slides). NIST currently does not have quantum computing but would like to discuss the thoughts if NIST did have one. Today, NIST has crypto-applications such as encryption, signatures, and key-establishment. NIST standardized those various crypto systems and algorithms. The cryptosystems fall into two different categories: Public Key, and Symmetric.

A Symmetric Cryptosystem is described as setup of a shared key with another secure party. A Public Cryptosystem is described as a key that is not already planned out ahead of time and needs to be created in order to use cryptography. With public key systems there are many different varieties such as RSA and Elliptical Curves which are in use today such as cryptosystem is used for items purchased online. These have been standardized and NIST has a good understanding. For Symmetric systems, AES is usually used. Hash functions can be used as a tool for both types of cryptosystems.

In approaching the discussion on how crypto systems would change in a quantum computing world, Dr. Moody described two algorithms that were discovered in the 80s where a quantum computer was built so that these algorithms could be used. The two algorithms are:

- Shor's Algorithm
- Grover's Algorithm

Shor's algorithm is able to factor in large numbers in polynomial time. RSA for example was safe because it takes too long to factor large integers. With a quantum computer, Shor's algorithm could factor large integers easily, and also, it could modify to solve the discrete log problem in polynomial time.

The Board asked why there is a distinction between polynomial and expediential time significant in the world of practical cryptography as opposed to Quantum computers.

The impact that these algorithms would have on the world today would be that all cryptography systems that we currently know and understand well, would be obsolete. The distinction between polynomial and expediential time is significant in the world of practical cryptography as opposed to quantum computer for Shor's algorithm would be fast enough to break any feasible level of security for RSA and discrete law. In addition, Grover's algorithm plays a role for quantum computers as well by allowing search on a database at quadratic speed.

The Board commented that NIST suggested that the Federal government require people to increase their RSA key length to 2000 bits with good predictive powers. Essentially, the impact of quantum computers is speculation and if and when will this concept be at the forefront. Mr. Scholl, Deputy Chief, Computer Security Division, NIST, and also Designated Federal Officer, ISPAB, responded that NIST is not yet

[32] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-03/a_quantum_world_v1_ispab_march_2014.pdf

ready to make any recommendations on quantum computing because research is still on-going. The purpose for this research is to build on our lessons learned in timing and transitions (referencing DES) and it will take some time extracting information out of infrastructures.

In today's world Public Key Cryptography is receiving the most attention which brings up a new field known as Post-Quantum Cryptography. This field focuses on trying to find cryptosystems that would be resistant to quantum attacks but that would still run on classical computers. This new field would need to be studied extensively as well as quantum computers bearing in mind the following:

- A lot of these proposed systems have not had the research and time required to understand whether they would be efficient,
- How to implement these systems on hardware and software,
- Study security issues behind the systems,
- Perform crypto analysis on them, and
- Study overall deployment

For these reasons, there will need to be a lot of time and research going into this effort. Dr. Moody posted the question as to whether we have enough time to perform the required research before a quantum computer is developed. There are a few quantum computers that can factor 20 or 21 numbers, but that capability is not enough for anything impactful. Currently, no one has a large enough quantum computer to break anything substantial. Optimistic estimates are between 5 to 10 years that quantum computers would be available but no one knows for sure. With the uncertainty of when this will occur, it is a perfect time to start research. NIST has started a Quantum computer program consisting of a Cryptography Technology group with five members, and a Quantum group with two members. The main objective is to examine those cryptosystems that are believed to be quantum resistant by studying their properties and determining whether they are suitable for quantum cryptography as well as monitoring the progress on the computers. Some of the cryptosystems that NIST Quantum Program will be reviewing include: Lattice based, Code based, and Multivariate based cryptography.

Public participation – there is no request received for public participation at this meeting**.**

Legislation Update

Nick Rossi, Minority Deputy Staff Director for the U.S. Senate Committee on Commerce, Science, and Transportation (Committee's Ranking Member, Senator John Thune of South Dakota)
John Williams, U.S. Senate Committee on Commerce, Science, and Transportation

Mr. Williams began the legislation update by referencing that the last congress the House and the Senate were very active in various pieces of cybersecurity. The House passed an Intelligence Committee piece on Information Sharing and the Science Committee also reported out legislation to fund research to organize a cyber-research plan to encourage education and training. Originally the Senate wanted to pass a comprehensive package to capture all of these areas such as information sharing, FISMA reform, standards and standards settings piece. However, the overall legislative decision was for all the committees to regroup and come up with their various pieces. The Congress Committee created a bill of standards that would be a building block to the NIST Cybersecurity Framework Version 1.0. Also, DHS wants to pass an Information Sharing bill but they are still working on it. Another legislation issue is the data breach incidents (example Target breach). There are ongoing efforts and work on data breaches from a cybersecurity perspective; however, most common data breaches are from entities holding a lot of personal information. Data breaches unrelated to cybersecurity are considered separate types of data breaches. The broad issue is that the retailer side of industry has a disproportionate business focus. The recent breach at Target is a good example of retailers focusing on a larger marketing department and

consumer analysis data. But the question remains as to how they are securing that information. For long term perspective, there needs to be an effort to secure data across industry and agencies.

Mr. Rossi began by stating that the House feels as though they have already addressed the major focuses related to cybersecurity. Last April, they passed the Information Sharing Bill, FISMA Reform, and the research and development Bill. The missing piece is setting standards which is somewhat addressed in the Homeland Security Bill which has yet to pass. Mr. Rossi explained that the Information Sharing Bill probably would not pass with the same amount of numbers as last time. In the Senate, there is a bill for support through NIST and to continue an ongoing basis to develop the standards and best practices and to address the research and development. The other areas in this bill relating to information sharing are going to be stalled because the House considers they were already addressed.

Board Discussion

Mr. Thomlinson led the Board's evaluation of each meeting session as follows:

NIST Update
- Follow-up on the Derived Credentials from PIV document that is currently out for draft.
- Invite DoD, CAC, PMI for a follow-up discussion
- Discuss issues raised in OMB memo M-06-16[33] in reference to Derived Credentials

IOT and CPS
- Follow-up on the FCC Technical Advisory Committee
- Follow- up on June workshops regarding CPS
- Re-address NIST's role for Taxonomy and the need to have security engineering upfront

NIST SP 800-53 Appendix J
- Review ongoing metrics
- IG perspective on privacy controls

Vehicle to Vehicle Communication
- Invite a representative from DOT to speak about this concept

DHS C3 Voluntary Program
- Review CDM Program
- Invite Phyllis Schneck to provide an overview of DHS's cybersecurity work plan

NIST Cryptography
- Provide an update on the VCAT at the next Board meeting
    - COV feedback
    - Deliverable feedback

NSS Update
- Invite Michael Daniel back as a follow-up

CAP Priorities for FY15-17
- The Board is interested in reviewing CAP metrics

[33] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf

FCC Cybersecurity

- CSRIC 4 update regarding the Framework and Implementation

GAO-14-34

- Review Smartcard and CMS Report
- Review cyber vs. non-cyber incident response and have a follow- up discussion about reporting the two

FedRAMP

- Invite a representative that is a SaaS Provider

Quantum Follow-up

- Propose holding a day at NIST for a Quantum Session Review in the fall.
- Invite NIST new Director to visit ISPAB or invite Dr. Willy May

Legislative Update

- Interested in having them back in future meetings.

The meeting adjourned at 12:06 P.M., Friday, March 14, 2014

Annex A

LAST	FIRST	AFFILIATION	
Banghart	John	NSS, the White House	Presenter
Castelli	Chris	InsideCybersecurity	Visitor/Media
Curran	John	Telecom Reports	Visitor/Media
Daniel	J. Michael	NSS, the White House	Presenter
Davis	John C.	Teknoworks, Inc.	Visitor
Dillon	Kevin	DHS	Presenter
Gupta	Sarbari	Electrosoft	Presenter
Johnson	Clete D.	FCC	Presenter
Kent	Daniel	Cisco Systems Inc.	Presenter
Landesberg	Martha	Privacy Office, DHS	Presenter
Lightman	Suzanne	NIST	Presenter
Moody	Dustin	NIST	Presenter
Newton	Elaine	NIST	Visitor
Odderstol	Thad	DHS	Presenter
Pillitteri	Victoria	NIST	Presenter
Regenscheid	Andrew	NIST	Presenter
Rogers	Susan	Cyberwise Contingency Planning, Yale University	Visitor
Rossi	Nick	US Senate Committee on Commerce, Science & Transportation	Presenter
Rudolph	Trevor H	OMB	Presenter
Scoville	Douglas	Treasury Department	Visitor
Sedgewick	Adam	NIST	Visitor
Smith	Michael C.	Vision 2020 Consulting	Visitor
St. Pierre	James	NIST	Presenter
Suh	Paul	DHS USCIS	Visitor
Thomas	Carlos A.	ECI	Visitor
Williams	John	DHS USCIS	Presenter
Wilshusen	Greg	GAO	Presenter

Annex B

AGENDA
VCAT Subcommittee on Cybersecurity
February 5, 2014
Executive Conference Room

Subcommittee Members: Roberto Padovani (chair), Rita Colwell, Tony Haymet, Bill Holt, Pradeep Khosla

2:30 pm – 2:35 pm	**Call Subcommittee to Order** Roberto Padovani, Chair
2:35 pm – 2:55 pm	**Addressing Cybersecurity Risk, a focus of the Cybersecurity Framework for Critical Infrastructure** NIST Cybersecurity Leadership • Donna Dodson, Chief Computer Security Division (CSD), Acting Executive Director of the National Cybersecurity Center of Excellence (NCCoE), ITL, NIST • Adam Sedgewick, Senior Information Technology Policy Advisor, NIST • Matt Scholl, Deputy Chief of CSD, ITL NIST • Kevin Stine, Manager Security Outreach and Integration Group, CSD, ITL, NIST
2:55 pm – 3:25 pm	**Optimum Balance – Cultivating Long Term Expertise to Support Short-Term Priorities** NIST Subject Matter Experts • Doug Montgomery, Manager, Internet & Scalable Systems Research, Advanced Technologies and Networking Division, ITL • Lee Badger, Manager Security Components and Mechanisms Group, CSD, ITL • Nate Lesser, Deputy Director NCCoE, ITL • Lily Chen, Acting Chief Cryptographic Technology Group, CSD, ITL • Dustin Moody, Cryptographer, Cryptographic Technology Group, CSD, ITL
3:25 pm – 3:55 pm	**NIST Response to the Nation's Cybersecurity Needs** Information Security and Privacy Advisory Board (ISPAB) Members: • Matt Thomlinson, Vice President, Microsoft Security, Microsoft and ISPAB Chair (remote) • Chris Boyer, Assistant Vice President – Public Policy, AT&T Services • John R. Centafont, National Security Agency (remote) • Kevin Fu, Associate Professor, Department of Electrical Engineering and Computer Science, University of Michigan (remote) • Greg Garcia, Founder and Principal, Garcia Cyber Partners • Ed Roback, Chief Information Security Officer and Associate Chief Information Officer for Cyber Security, Department of Treasury
3:55 pm – 4:30 pm	**Review of Cryptography Standards Development Processes** Patrick Gallagher, Under Secretary for Standards and Technology and NIST Director
4:30 pm – 5:30 pm	**Formulation of Recommendations** VCAT Subcommittee on Cybersecurity

(absent), Al Romig (Absent)
External Expert: Frank Quick, Senior Vice President, Engineering, Qualcomm Research