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

June 11, 12 and 13, 2014
Courtyard Washington, DC/US Capitol, 1325 2nd Street NE, Washington, DC, 20002

	Board Members	
	Present	Non-board Members:
Wednesday, June 11, 2014 8:38 A.M. – 4:49 P.M. Thursday, June 12, 2014 9:04 A.M. – 4:14 P.M. Friday, June 13, 2014 8:59 A.M. – 12:19 P.M.	Matthew Thomlinson (Chair), Microsoft John Centafont, NSA Dr. Kevin Fu, University of Michigan Greg Garcia, Garcia Cyber Partners Toby Levin (Retired) Edward Roback, US Department of Treasury Gale Stone, Social Security Administration Dr. Peter Weinberger, Google, Inc. Absent with regrets: Julie Boughn Christopher Boyer, AT&T	Dr. Willie May, NIST Dr. Charles Romine, NIST Dave Cullinane Matt Scholl, NIST Annie Sokol, DFO, NIST Tatiana Laszczak, Exeter Government Services, LLC See Annex B for list of attendees

Wednesday, June 11, 2014

Welcome and Remarks

Matt Thomlinson, Chair, ISPAB
Vice President, Microsoft Security

The ISPAB Chair, Matt Thomlinson, called the meeting to order at 8:38 A.M. Mr. Thomlinson addressed the Board and mentioned that the Board must approve the meeting minutes for December 2013 and March 2014. Mr. Thomlinson introduced Mr. Dave Cullinane who is currently going through the board member vetting process, and hopefully, he will be approved as an official board member at next meeting in October 2014.

Ms. Sokol informed the Board that Mr. Thomlinson and Ms. Stone had been approved to serve another 4-year term on ISPAB until 2018. In addition, there are a few board members due for renewal for new term in 2015. Ms. Sokol recommended suggested meeting dates for 2015 and confirmed 2015 meeting dates for the NIST Visiting Committee on the Advanced Technology (VCAT) as additional reference. The Chair stated that the board will review the schedule on the last day of the meeting. The Chair followed with a quick overview of meeting agenda[1].

[1] http://csrc.nist.gov/groups/SMA/ispab/documents/agenda/ispab_agenda_june2014_final.pdf

NIST Updates

Matt Scholl, Acting Division Chief, Computer Security Division, NIST

Mr. Scholl began with an update of the NIST Crypto process. NIST has asked the VCAT[2], a Federal Advisory Committee Act (FACA) advisory board tasked with reviewing and making recommendations regarding general policy for NIST to review the procedures and body of work of cryptography and to ensure NIST is continuing to maintain and conduct an open and transparent process[3]. The main focus is on NIST's design and development of cryptography and the associated mechanisms which include operation functions and key management. The VCAT held a series of sub-committee meetings and they asked a Committee of Visitors (COV) which consisted of independent experts in the field of cryptography and standards to review and provide feedback to the VCAT. The VCAT sub-committee met June 10, 2014, and the full VCAT meeting was scheduled June 11, 2014. Mr. Andrew Regenscheid, Computer Scientist, Computer Security Division, NIST, will be updating this Board on Friday, June 13, 2014. Matt Scholl believed that the COV may not have finished their report by today and he is not sure of the status of VCAT deliberations on a recommendation. It is assumed that there will be an interim meeting in July where the VCAT sub-committee will present their report to the VCAT main committee before the VCAT will finalize a recommendation to NIST.

Mr. Scholl reported that NIST Privacy Engineering Workshop held in May 21, 2014[4], which was focused on privacy engineering, specifically related to:

- To address these gaps and challenges, and in support of the activities set forth in section 4.9 of the NIST Roadmap for Improving Critical Infrastructure Cybersecurity (developed pursuant to Executive Order 13636), and

- To focus on the advancement of privacy engineering as a basis for the development of technical standards and best practices for the protection of individuals' privacy or civil liberties

This is the first of a series of workshops. Furthermore, NIST had a state and local[5] government[6] conference on the Cybersecurity Framework - NIST coordinated and presented at the National Governors Association[7] and the National CIO (NASCIO)[8]. NIST focused on the Cybersecurity Framework in relation to other NIST guidance and mechanisms on how the framework was developed. NIST worked with the National Security Council (NSC) and US Department of Homeland Security (DHS) which has a large outreach community to state and local government that helped NIST setup the meeting. Mr. Scholl

[2] http://www.nist.gov/director/vcat/

[3] VCAT report: NIST Cryptographic Standards and Guidelines Development Process was released on July 14, 2014, http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf; http://www.nist.gov/director/vcat/cryptographic-standards-guidelines-process.cfm

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

[5] http://csrc.nist.gov/nccoe/Events/Cyber_Framework_Kickoff_Agenda_20140327.pdf

[6] http://www.nist.gov/itl/upload/Framework_Kickoff_20140327-2.pdf

[7] http://csrc.nist.gov/nccoe/Events/Framework/NGA.pdf

[8] http://www.nascio.org/

reported that it was well received and that NIST planned to have follow-on discussions with the state of Pennsylvania in implementing the Framework and discussions with the NASCIO. The NASCIO would like to coordinate with NIST and put out a data call to include questions on cybersecurity in their next surveys to the state local chamber of commerce and local businesses. Mr. Scholl said that the questions would be simple in nature for the first round such as, "have you heard of the Framework and, if so, where did you hear about it"? The next set of survey questions would be more in depth such as, "what type of cybersecurity measures are you currently using and would you be open to sharing some of your procedures and standards that you are currently using"? NIST will gather that data. Furthermore, NIST received a letter (see Annex A[9]) from the U.S. Chamber of Commerce[10][11] that was very supportive of their current efforts of the Framework.

Mr. Scholl reminded the Board of Dr. Pat Gallagher's last week as the NIST Director and the Under Secretary of Science and Technology. Dr. Willie M. May who is currently the Associate Director will be the Acting NIST Director until a new NIST Director is appointed. Dr. May will briefly visit the ISPAB meeting on Thursday, June 12, 2014 to discuss the transition among other things. There has not been any known discussion of a follow-on Director.

Mr. Scholl provided updates of recent publications such as Draft Supply Chain Risk Management guidelines. The purpose was to try to strike a balance between the scientific, reasonable and actionable approach as well as doing something that is a potentially prohibiting open market pre-trade. This draft SP 800-161 *DRAFT Supply Chain Risk Management Practices for Federal Information Systems and Organizations (Second Draft*)[12] is currently open for comments until July 18, 2014. In addition, this draft is in accordance with legislature on appropriations for agencies to follow this NIST guidance on Supply Chain Management on Supply Chain Management and to have their acquisitions cleared by the FBI for certain agencies. For example, if an agency is going to buy something that is going to be incorporated into a high impact system, the agency must conduct a Supply Chain Risk Management assessment and get approval from FBI, if required. The assessment is related to physical things in software and not cloud related.

NIST CSD also released draft documents - Personal Identity Verification (PIV). FIPS 201-2 *Personal Identity Verification (PIV) of Federal Employees and Contractors* was released in August 2013, and SP 800-73-4 *Draft Interfaces for Personal Identity Verification (3 Parts): Part 1: PIV Card Application Namespace, Data Model & Representation, Part 2: PIV Card Application Card Command Interface, and Part 3: PIV Client Application Programming Interface*. There were some complication with the release of publications between NIST released of these drafts and Office of Management and Budget (OMB). NIST has worked very closely with OMB and OMB has plans to update their memo to allow the use of derived credentials, but NIST had released the drafts ahead of OMB. OMB said that for the device seeking remote authentication the credential must be separate from the device seeking authentication. There has been a lot of discussion around new technologies using the PIV card and the security

[9] https://www.uschamber.com/sites/default/files/documents/files/11June14GroupLetterT-YReplytoDanielCyberBlog_Final_0.pdf

[10] https://www.uschamber.com/press-release/us-chamber-statement-cybersecurity-framework

[11] https://www.uschamber.com/administration-sends-cybersecurity-stakeholders-positive-message-nist-framework-should-be-voluntary

[12] http://csrc.nist.gov/publications/drafts/800-161/sp800_161_2nd_draft.pdf

requirements that should or should not be used with the Near Field Communications (NFC) for PIV. NIST has received a lot of non-concurrence letters regarding this topic and would like to present this more in-depth to the Board so as to invite for feedback and recommendations around security requirements for the PIV card. For example:

- What should or should not be used regarding interoperability, use ability, and user acceptance
- And, where the NFC should be used.

Another recent release centers on security engineering (SP 800-160 *Draft Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*[13]). This draft is intended to be the first in a series of the thought processes around the concept of security resiliency with a long term goal as NIST looks towards the Internet of Things (IOT) and getting in front of building security in devices. FIPS-202[14] *Draft SHA 3 Standard: Permutation-Based Has and Extendable-Output Functions* was released in late May with comment period closing on August 26, 2014. NIST will have a follow-on SHA 3 workshop in the fall. There will also be a workshop on Random Number Generation with plans of putting out some guidance on SP 800-90 B[15] *Recommendation for the Entropy Sources Used for Random Bit Generation* which is to focus on the acceptable use of noise. SP 800-90 A[16] (2nd Draft) *DRAFT Recommendation for Random Number Generation Using Deterministic Random Bit Generators* was also released for comments late April this year. NIST has updated some work on Industrial Security Guidelines which is part of a larger look at critical infrastructure and industrial control bar, and is continuing work within security automation with the Internet Engineering Task Force (IETF) continuous monitoring and security working group.

Also, the National Cybersecurity Center of Excellence (NCCoE) is in transition of becoming a Federally Funded Research and Development Centers (FFRDC)[17]. The solicitation period closed on May 22, 2014, and they are currently evaluating submitted proposals.

NIST is looking to do more work in privacy beyond privacy engineering and are trying to establish the right space for NIST that is non-duplicative and that can provide some expertise in. Lastly, NIST is would like to look more closely at cryptography; specifically, related to cryptography when quantum computers arrive, called Post Quantum Computers (PQC).

For example:

- What are the current algorithms
- Key sizes
- Public Key Infrastructure
- And, what needs to happen in this space

[13] http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

[14] http://csrc.nist.gov/publications/drafts/fips-202/fips_202_draft.pdf

[15] http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90b.pdf

[16] http://csrc.nist.gov/publications/drafts/800-90/sp800_90a_r1_draft.pdf

[17] https://www.fbo.gov/index?s=opportunity&mode=form&id=26e935a6df0b24db1f11ce8303d0377d&tab=core&_cview=1

Personal Identity Verification (PIV) Credentials for Mobile Devices

Hildegard Ferraiolo, Computer Scientist, Computer Security Division, NIST [Presentation provided[18]]
(See *Public Comments Received on NIST IR 7977* [19])

Ms. Hildegard Ferraiolo thanked the Board for inviting her to speak on this topic. She began with the scope of the draft document SP 800-157[20] *DRAFT Guidelines for Derived Personal Identity Verification (PIV) Credentials*. The Derived PIV Credential is an additional PIV Credential to satisfy HSPD-12's 'Common Identification mandate. The purpose of this document is to address the gaps, and the goal is to provide alternative approaches to PIV-enabled e-authentication with mobile device - without PIV Card and add-on readers. It was not to advice on any current PIV card functions on how it is to be used today. However, when discussing what a logical work remote authentication is, it was to refer to the multifactor authentication using the PIV cards which is typically considered ones work station (desktop computers) or laptop. Where NIST identified the gap is, using the new mobile device authentication for federal employees and contractors that want to use mobile devices which is hard to do. However in some situations it is impractical to use the PIV card and even cumbersome having to deal with attached readers. The goal is to enable remote access control from your mobile device to your desktop network which also includes signing in on emails and an encryption feature using the PIV card. The Board commented that the gap is not looking at PIV cards as tokens.
PIV card uses phonological/remote access using the desktop and laptop, it is also to leverage PKI credentials. When NIST looked at what security token should be integrated into mobile devices to host the derived credential, it was realized that not all mobile devices were created equal. There were a lot of different capabilities such as different ports and network operators. Due to the many variations of mobile devices we have several approaches or security tokens listed in SP 800-157:

- Define the Derived PIV Credential (a PKI-based credential)
- Both LoA-3 (software) and LoA-4 (hardware) Derived PIV Credential are possible
- Key size and algorithm options are the same as for the PIV Authentication private key
- Defines Derived PIV Credential Lifecycles: Derivation, Issuance, Maintenance (re-key/re-issuance) and Termination

Agencies will have to consider the cost associated with the solution. In addition to where the security key can reside in each token, NIST also defined the life cycle of each solution. The next step is to resolve the public comments and finalizing the SP 800-157 document. Ms. Ferraiolo affirmed to the Board that NCCoE was doing some pilots.

[18] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-06/ispab_jun2014_derived-piv-credentials_ferraiolo.pdf

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

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

The Next Generation (SP 800-73-4) PIV Card and the Purpose of the Pairing Code in the Wireless Environment (Presentation provided[21])

David Cooper, Computer Scientist, Computer Security Division, NIST
(See *the Next Generation (SP 800-73-4) PIV Card and the Purpose of the Pairing Code in the Wireless Environment)*

Mr. Cooper's presentation began with an overview and focusing on current situation with PIV cards, where technology is going with next generation PIV cards and issues with new technologies and capabilities. HSPD-12 was developed 10 years ago which was developed to protect personal privacy, which was first established in FIPS-201 to ensure technologies do not erode privacy protections relating to the use, collection and disclosure of Personal Identifiable Information (PII). The first solution was a contact center face using a card that was reasonably and physically used for logical access. Essentially this solution only allowed to receive from the cardholder was a couple of various number identifiers that agencies used referred to the Universal Unique Identifier (UUID) which is a random number generated for each card. The second yet similar solution was called the Federal Agency Smart Credential Number (FASC-N) which identifies the agency and department one might happen to work in. FASC-N can only search the agency that an individual works for but any other information like name and email are restricted to the contact center. The information is PIN protected for additional privacy protection.

The first generation PIV cards did not have encryption. All the data was transported back and forth over the contact interface and that should protect it from eavesdropping. The first draft of the NIST FIPS 201-2 was released with the idea of a secure channel. Initially, it was developed because NIST wanted to add biometric comparisons using finger print data which would send an encrypted copy of a finger print sample and then receive an authentication confirmation indicating whether the comparison was successful. This would ultimately allow physical access to control systems through a finger print comparison if the system required a higher-level of assurance to establish that the individuals' identity is accurate.

When the first draft was released in 2011, NIST received many comments as to a secure channel is to be established and to enable the full capabilities of the PIV card without restricting to biometric comparison. NIST made some adjustments to FIPS-201-2, and released it for comments in 2012. In the final version, a virtual contact interface (VCI) can be established when a secure channel is established, and this enables the full capabilities offer by PIV card. Minimally, this would allow data over a contact interface when VCI has been established. It will be encrypted which will protect it against passive eavesdropping. With new technologies today, this process does not protect against skimming which is data that can be received by any reader if in close proximity. In terms of skimming information that is available now through the contact interface – one does not have to worry about biometric data due to the PIN protection feature. However when a VCI has been established x.509 certificates on PIV cards can release the cardholders name, email, and country depending on what information an agency requires.

The solution was to revise the SP 800-73-4 document which proposed that the establishment of the VCI require a submission of a pairing code. This would protect the reader to the card against skimming devices. The pairing code is an 8-digit value randomly generated.

[21] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-06/ispab_jun2014_pairing-code_cooper.pdf

Big Data and Privacy (Presentation provided[22])

Marjory S. Blumenthal, Executive Director, President's Council of Advisors on Science and Technology, Office of Science and Technology Policy

Ms. Marjory Blumenthal explained to the Board that the President's Council of Advisors on Science and Technology (PCAST)[23] were charged with two projects:

1) Scoping Study
2) PCAST report to inform and accompany the White House report[24]

The PCAST was charged with this task last January 2013 and had 90 days to complete the analysis. One report was to focus on policy and the second was to address technical issues, and both reports were done in simultaneously. The PCAST usually consults with subject matter experts and sometimes will have a dedicated working group. However, due to the projects timeframe the PCAST did not have the time to select a working group. The PCAST as a whole approves the reports. In this case the PCAST had half the council works on these projects. The PCAST focused on basic concerns regarding what is technologically feasible and what is privacy. There were three workshops hosted at different universities. As the PCAST at some new technologies within the context and management perspective, they found there are also side effects that can compromise privacy. There is a lot of variety in the data and metadata. The PCAST found that privacy has focused more on small data conventional statistics in the past and the problem is that people emit data continuously in many different ways. The PCAST defined the data collected in two ways:

1) Born Digital – Generated by computers (examples, clicks, tapes, GPS, cookies)
2) Born Analog – By product of the physical world (examples, sensors collect)

Due to these concepts, the world that we live in today has a big data over-collection issue. With the big data collected, there are new ways for analytics to create new information (see PPT slides). In terms of the different kinds of infrastructure, the Cloud perspective continues to be the dominant infrastructure. The Cloud infrastructure can handle big data which has the potential to offer consistency and elevate a level of security. Ms. Blumenthal explained that some of the biggest players are called producer users such as Google, Amazon and Facebook. This was technology developed for the producers own use and ended up offering it to the public.

Cybersecurity enforces policy for computer use and communication, but poor cybersecurity is a threat to privacy. The conclusions of the reports ended in five recommendations (see slides for additional information):

1) Recommendation 1: Policy attention should focus more on the actual uses of big data and less on its collection and analysis
2) Recommendation 2: Policies and regulation should not embed particular technological solutions, but rather should be stated in terms of intended outcomes

[22] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-06/ispab_jun2014_big-data-privacy_blumenthal.pdf

[23] http://www.whitehouse.gov/administration/eop/ostp/pcast

[24] http://www.whitehouse.gov/administration/eop/ostp/pcast/docsreports

3) Recommendation 3: With support from OSTP, the NITRD agencies should strengthen U.S. research in privacy-related technologies and in the relevant areas of social science that inform the successful application of those technologies
4) Recommendation 4: OSTP, together with the appropriate educational institutions and professional societies, should encourage increased education and training opportunities concerning privacy protection
5) Recommendation 5: The United States should adopt policies that stimulate the use of practical privacy-protecting technologies that exist today. It can exhibit global leadership both by its convening power and also by its own procurement practices

Privacy & Civil Liberties Oversight Board (PCLOB) Updates

Assessment of DHS cybersecurity privacy report[25]
Sharon Bradford Franklin, Executive Director, Privacy & Civil Liberties Oversight Board

The Chair introduced Ms. Sharon Bradford Franklin and added that the Board had written a letter of recommendation in support of the PCLOB's mission.

Ms. Franklin began by confirming the Board's interest in PCLOB's report on the NSA's bulk telephony metadata collection program under Section 215[26] and the DHS review process of the Cybersecurity Executive Order (EO). Cyber Intelligence Sharing and Protection Act **(**CISPA) had a role for the board would be in coordination with DHS. There may also be a role in the Senate Intelligence Committee which would consist of assessing the sufficiency of procedures on the privacy protections on civil liberties within information sharing. The PCLOB would like to focus on PCLOB and informant sharing between the government and private sector and vice versa. The PCLOB would like to discuss in more details what information can be shared between government and the private sector.

Under the Executive Order, the PCLOB's role is to consult with DHS to develop the §215 report. When DHS provided the draft report, it was basically a preliminary as not much had been implemented. As a process point the PCLOB would like to be part of the process much earlier but understands that DHS had new leads. As the PCLOB reviewed the report, it was discovered that the agencies involved had not come up with one cohesive report. The information was compiled but not in a cohesive manner as agencies used different formats and factors. The PCLOB highlighted some areas that could use improvement: when information is shared unrelated to cyber incidents, there was inconsistent recognition of the fact that the person not be the perpetrator but could be the innocent victim of the attack. There was also inconsistent thinking on what standards should be in relation to PII. The Board inquired if a large amount of PII is stolen, and does the FBI see that information and what FIPS apply too. Ms. Franklin explained that is specifically related to law enforcement question may be what is the trigger that response. She also explained that she does not think there is a uniform answer.

[25] http://www.dhs.gov/sites/default/files/publications/2014-privacy-and-civil-liberties-assessment-report.pdf

[26] http://justsecurity.org/6142/pclob-releases-report/

FISMA FY13 Report (Presentation provided)[27] [28] [29]
Trevor H. Rudolph, Office of E-Government & IT, OMB, Executive Office of the President

Mr. Rudolph introduced his presentation by saying that the FY13 Federal Information Security Management Act (FISMA) Report was an interagency effort and DHS contributed the majority of the work. Mr. Rudolph's role was in organizing and assembling the data. He stated that the three main focuses of the report are as follows:

1) Section II: Key Ongoing Information Security Initiatives
2) Section III: Key Security Metrics
3) Section IV: Security Incidents and Response in the Federal Government

The FY12-14 Cross-Agency Priority (CAP) goals are continues monitoring, strong authentication, Trusted Internet Connections (TIC) consolidation, TIC[30] capabilities and Cyber CAP progress. OMB is in the process of establishing 15-17 metrics. In response to the Board's question of whether the agencies reporting metrics are self-reported, Mr. Rudolph said that there is some self-reported data that include asset management, configuration management and continuous monitoring. Although this information is self-reported by the agencies to DHS, there are some automated reports and DHS is doing a good job of standardizing the process. He continued by saying that DHS and OMB would like to receive more automated reports from the agencies. This is a challenge because the data self-reported and automated reports are a skew to the numbers reported. OMB/DHS is pushing to move forward to have more machine generated reports and less self-reported information. The DHS Certified Volunteer Program (CVM) will be a tremendous help in improving the automation challenge.

The trends for the CAP goals for FY12-13 focus on continuous monitoring, strong authentication leveraging HSPD-12 and TIC. There have been fluctuations within this report. As agencies develop better report processes and automated reports, the agencies may find additional systems that they were not originally aware of. Usually, when OMB notices a fluctuation of data reported, they will contact the agency directly and work with the agency in determining the issue(s). Most of the incidents reported were non-cyber incidents and more serious incidents were less than <2% (from CFO agencies) and <1% (from non-CFO agencies).

The Board asked for comparison of these metrics with private sector, and Mr. Rudolph stated that while they are interested in how the government compares with the private industry, they generally review inter-agency data. In response to the Board of whether any agencies are not on the list, Trevor Rudolph confirmed of some agencies mainly CFOs. In conclusion, Mr. Rudolph informed the Board that they are currently working on the FY15 – FY17 CAP goals. OMB is evaluating where the focus areas moving forward.

[27] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-06/ispab_jun2014_fisma_rudolph.pdf

[28] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf

[29] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy_2013_fisma_report_05.01.2014.pdf

[30] ISPAB last discussion on TIC was in June 2013 meeting.

US CERT (Presentation provided)[31]

Matt Scholl, (Moderator), Acting Division Chief, Computer Security Division, NIST
Ann Barron-DiCamillo, Director, United States Computer Emergency Readiness Team (US-CERT), Assistant Deputy Director, National Cybersecurity and Communications Integration Center (NCCIC), Department of Homeland Security

Mr. Scholl introduced Ms. Ann Barron-DiCamillo from US-CERT. Ms. Barron-DiCamillo began by providing some background information about the US-CERT guidelines. US-CERT guidelines were provided in FISMA 12 years ago which consisted of a 6-category system for cyber-security incident reporting. However, that system was geared towards where *we were* twelve years ago in reference to collecting data. For example the process was reviewing phishing and access controls in the process of incident response - US-CERT has noted that through the years it is the sub-categories that get to the impact of an incident and these sub-categories were so broad that they did not always capture the true impact of the incident. US-CERT is trying to update and get to the impact of an incident /data loss as well as get there quicker. The process has evolved to the current approach and that US-CERT will have a continuous evolution of a cyber-incident data that is dynamic within the cyber environment.

Adjustments that have been to the US-CERT reporting efforts: (see PPT slides):

- Replaced Categories with Threat Vectors
- Introduced Impact Classifications
- Moved root cause analysis to “closing” phase of the incident response process
- Eliminated “non-cyber” incidents from notification requirement
- Separate mandatory from voluntary notification
- Introduced a 1-hour notification timeframe for mandatory incidents
- Greater focus on coordination and bi-directional information sharing
- Changed paradigm from “reporting” to “notification”

US-CERT will continue to improve with response time, and US-CERT is focused on better coordination with bi-directional information sharing and actionable information. Most important of the lessons learned gathered from the FISMA guidelines were that some incidents were not actionable and difficult to coordinate and report because there was not any bi-directional information sharing. As a result, US-CERT has tried to apply the understandng to the new federal notification system. This new focus is on notification. US-CERT realizes that with early awareness with impacts and treats they can be more responsive in their overall response to the victim or entity as well as leveraging the information to see if there are any trend activities associated with that incident. US-CERT also sees a responsibility for non-cyber incident reports as a requirement for one’s privacy office within agencies. They want to eliminate some times duel and even triple reporting of PII. The goal is for US-CERT to gather better actionable data for operational use regarding cyber operational data. The Board would like to know if this change is coming from OMB, and Ms. Barron-DiCamillo stated that US-CERT has been working with OMB as well as Federal departments and agencies to update the notification guidelines. This is not just coming from US-CERT, but it is a collaboration and coordination effort with other agencies. For example, there are some incidents that have PII that do have cyber relevancy. Reporting PII is important and needs to be collected but not by cyber operational components - US-CERT is trying to focus their resources on this so one would report a majority of the PII incidents to the agencies privacy office and not US-CERT.

[31] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-06/ispab_jun2014_us-cert-incident-reporting-guidelines_dicamillo.pdf

With regards to an example of PII, what would US-CERT consider the loss of a laptop? Ms. Barron-DiCamillo explained that the loss of a laptop has data on it which is more than PII and that would be a determination of the agencies Security Operations Center (SOC). If a PII report was delivered from privacy office, the privacy office would decide there is a cyber-relevant data and require coordination with US-CERT. Ms. Barron-DiCamillo mentioned that there are multiple documents being released to inform agencies of the changes and explain how these updates are to be communicated to agencies.

Thursday, June 12, 2014

International discussions and meetings- Norms, governance issues

Ari Schwartz, Senior Director for Cybersecurity on the United States National Security Council Staff, The White House

The Chair welcomed Mr. Schwartz's return to the ISPAB as Mr. Schwartz served as a member of this Board for some years. The Board asked Mr. Schwartz about the blog news article discussing how the government deals with vulnerabilities related to discovery and exposure. Also, the Board would like to know if there is a way to coordinate across the government and agencies as generally everyone has different views of vulnerability detection.

Mr. Schwartz affirmed that about two years ago the government did get together to discuss a focus on how different agencies report and communicate vulnerabilities. The government's focus is to have and ensure a concrete process to have a pre-disposition to disclose information and vulnerabilities. It is important to understand the purpose is not to discuss thousands of vulnerabilities but some key areas. In addition, a vast majority of the vulnerabilities are disclosed but there are a lot of questions that have to be defined. For example, some questions are:

- How much harm does this vulnerability cause?
- How likely would "we" the government know if someone was exploiting it?
- How likely would someone discover the vulnerability on their own?
- Can the vulnerability be patched or mitigated?

The President's review group following the NSA disclosures led us to re-work the vulnerability process. The thought process of the questions developed is geared towards all agencies. He also explained that the larger the entity the more difficult it can be to discuss because more people are involved in the decision making process. There is also an issue of being too transparent in getting the information and releasing it. If they are overly transparent they could put people in harm's way. This is a classified process but they have been moving in the direction to disclose more information.

Board Discussion

The Board reviewed the Meeting Minutes for December 2013 and March 2014. Toby Levin motioned to approve and Kevin Fu second the motion; the meeting minutes were approved by unanimous consent. The next meeting will be held on October 22, 23 and 24, 2014, at the US Access Board, 1331 F Street NW, Washington, DC. The Board noted that VCAT meeting is scheduled for October 7-8, 2014. The Board reviewed and approved the following dates for 2015 meeting as proposed by Annie Sokol, DFO, ISPAB:

ISPAB 2015 Meeting Schedule:
February 11, 12, and 13, 2015
June 10, 11, and 12, 2015
October 21, 22, and 23, 2015

NIST Updates from ITL Director

Dr. Charles Romine, Director, Information Technology Laboratory

The ISPAB took advantage of unscheduled presence of Dr. Charles Romine, ITL Director, and invited him to share a few thoughts with the Board. Dr. Romine began with recognition of resignation and imminent departure of Dr. Pat Gallagher who has led NIST for the past six years. He further iterated that Dr. Gallagher leads NIST in a way that has provided NIST as a whole with an extraordinary visibility and leadership role within the Federal government innovation and initiatives space. The Secretary of Commerce and the President have emphasized the importance of innovation as a driver for information technology (IT) in the economy. Dr. Romine acknowledged Dr. Gallagher for his efforts in positioning NIST with a strong influence within IT.

Quantum information science has been a dominating force at NIST for over the past ten years. There have been a lot of discussions about quantum science in regard to the possibility if quantum computer is developed the entire infrastructure that we have today will collapse overnight. Over a year ago, NIST was tasked by the President to come up with an industry standard for cyber security. Because NIST has established such a good position on cyber security, NIST was in position to be assigned the task. NIST takes pride in maintaining a neutral stance while preserving a good relationship with the private industry. The Cybersecurity Framework[32] was developed through an overall transparent process, and Dr. Romine commended the NIST team for their outstanding efforts and commitment to the task – stating that he could not be prouder of them. In addition, NIST strengthened its relationship with industry.

Dr. Romine mentioned that currently solicitation responses on NCCoE's FFRDC are being reviewed. He believes that NIST has offered a good balance between long term and short term research, and it is especially important in attracting talent if an organization does not have long term goals and focuses more on the short term. However, NIST cannot solely focus on research because it is difficult to compete with the academia community. The Board asked Dr. Romine to explain a balance can be defined between the long term and short term challenges of attracting the right people and the retention rate. With regards to retention in general, Dr. Romine reminded the Board of NIST's a compelling mission. NIST employees can share this passion in the kind work they do and they will find it meaningful to know that it has a serious impact with the government and private sector. Also, NIST leadership is conscientious and particularly conscious if great people start to leave. NIST has quality people that are passionate about their work. Although NIST is not completely immune to the fact that the government from an administrative stand point does not support an innovative environment. Dr. Romine also mentioned that salary may be an issue because NIST cannot offer competitive pay as industry. But NIST does have incentives and partners with other experts, academia and research laboratories.

Dr. Romine laid out a few critical areas:

1) NIST's current focus is privacy which is a gap in the EO Cybersecurity guidelines. This is partly because of the industry needs to have the right tools collectively to accompany privacy guidelines. NIST is excited to work with industry and the ISPAB on this issue.
2) The Secretary of Commerce has requested strategic planning effort from NIST.
3) The Department of Commerce (DoC) has vast data but it is not available to the public. NIST would like to use that information and make it available to the public, but there are privacy concerns when accessing and allowing availabilities to the data for innovation.

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

4) Dr. Romine mentioned that Dr. Willie May is the Associate Director and will soon be the Acting Director. Donna Dodson has been promoted as the Senior Technical Advisor which is equivalent to a position of Associate Director. NIST in searching for a new Director to replace Dr. Gallagher. NIST would prefer to promote from within NIST but due to the position description NIST will be searching on a national level to fill the position. He has been working on the position description that should be accurate and clearly represents what NIST is looking in the position. It is necessary that this Director position to remain in an acting role for extensive period.
5) Lastly, Dr. Romine would appreciate the Board's contribution on the following topics: privacy engineering, and big data analytics and enhancing approaches in relation to improving cyber security.

Controlled Unclassified Information (CUI)[33] Program and NIST Standards (Presentation provided)[34]

John Fitzpatrick, Director, Information Security Oversight Office, National Archives and Records Administration (NARA)
Patrick Viscuso, PhD., Associate Director, Controlled Unclassified Information, Information Security Oversight Office, NARA
Dr. Ron Ross, NIST Fellow, Project Leader, FISMA Implementation Project, Joint Task Force Transformation Initiative

Mr. John Fitzpatrick started the discussion with an overview of the Controlled Unclassified Information (CUI) Program, CUI objectives and CUI implementation. The CUI program is to provide some order to a chaotic information environment that has a long history of the government placing procedural controls on information types. These information types have existed for a long time and are labeled in many different ways. There are also many types of instructions on how to protect this information and whether they should be protected and when to allow public release across the government. The CUI program objective is to place a regulatory umbrella approach process on how to identify the unclassified information that merits protection. Information is imperfectly shared, and procedures and instructions for protecting that information can be confusing and inconsistent. For those reasons, the process of information sharing needs to be improved with better consistency and understanding of the reasoning of why the government should place controls on information.

Mr. Fitzpatrick emphasized that the CUI program is very open and transparent, and proceeded to explain the policy and reasoning behind establishing this program. The CUI Program is not for classified information. The CUI approach is described (see slide 6) as "An open and uniform program to manage all unclassified information within the executive branch that requires safeguarding and dissemination controls as required by law, regulation, and Government-wide policy".

The roots of this initiative stemmed from the Bush administration. At the time, the focus was on a narrower space than it is now which was specifically related to counter-terrorism and Homeland Security. The Bush administration raised the issue within the President's memorandum on *how do we place controls on these sets of information* within Homeland Security and counter-terrorism. The Obama administration approach to the issue is much broader government-wide approach which is outlined in EO 13556[35] issued in November 2010. This EO took a lot of lessons learned from the Bush's memorandum and from the Department of Justice (DOJ), the Secretary of Homeland Security and attorney general

[33] http://www.archives.gov/cui/

[34] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-06/ispab_jun2014_cui_nara_nist.pdf

[35] http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf

which made a number of recommendations which provided interest in this in creating a structure around identifying information that should be protected. This created the need for the EO.

The EO states that some controls should be removed and reduced in number regarding what is considered unclassified information because they do not meet the threshold for unclassified information that requires controls. In order to establish what meets the threshold, the CUI Program representatives met with interagency representatives to review the threshold and required controls. The feedback received included 2200 descriptions from agencies that described the information and included comments/reasons of why the information meets the EO threshold for unclassified information. Many agencies submitted similar information, and there were common types and some specifics. Provided on the NARA website CUI registry[36], there are 22 broad categories, 85 sub-categories, and 314 unique level-down categories that map back to the EO which meets the threshold requirements.

Lastly, Mr. Fitzpatrick discussed implementation and how that will affect government agencies. There will be phases for implementation, and the CUI program will work with OMB and the Executive agents to determine the dates. The current efforts for the CUI revolve around maintaining the registry, finalize the CUI policy and focus on the National Implementation Plan (NIP). Also, the CUI and sub-categories will be incorporated in as information types into the next revision of the NIST SP 800-60 Rev.1 [37]– where the work of the CUI EA will be integrated.

NIST Leadership Transition

Dr. Willie May, NIST Associate Director, Acting Director

Mr. Thomlinson introduced Dr. Willie May to the Board. Dr. May wanted to briefly address the ISPAB due to the transition of Dr. Pat Gallagher's resignation and Dr. May standing in as the Acting Director until the role can be filled. Dr. May recognized and commended Dr. Gallagher's work at NIST and in the cybersecurity space. He also thanked the ISPAB members for their exceptional service in addressing areas of focus within IT security and privacy. Dr. May emphasized that cybersecurity is very important to NIST moving forward and asked for the Board's continued advice and recommendations on *areas that NIST should focus on and continue to do in IT security and privacy.*

Emerging Guidance and Standards affecting Medical Device Security

Dr. Kevin Fu, (Moderator), Associate Professor, The University of Michigan
Ken Hoyme, Distinguished Scientist, Adventium Labs (presentation provided)[38]
Dale Nordenberg, M.D., Co-Founder, Executive Director, Medical Device Innovation, Safety & Security
Bakul Patel, Policy Advisor, Office of Center Director, Center for Devices and Radiological Health, FDA

Dr. Kevin Fu introduced the panel. Mr. Ken Hoyme has been developing the software and hardware in medical devices, implants and even airplanes. He also is a member of Advancing Safety in Medical Devices (AAMI) that works with emerging standards and guidelines related to medical device security.

[36] http://www.archives.gov/cui/registry/category-list.html

[37] http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf; http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf

[38] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-06/ispab_jun2014_medical-devices_hoyme.pdf

Mr. Bakul Patel is the Policy Advisor from FDA / CDRH within the Office of Center of Directors. Dr. Dale Nordenburg is a Physician, and is the Co-founder of Medical Device Safety Innovation Security Forum for providers and manufactures. Dr. Fu highlighted Mr. Hoyme's affiliation with Advancing Safety in Medical Technology (AAMI) working group that have put out a number of medical standards and guidance behind the medical device. Mr. Hoyme kicked off the discussion and explained that the focus of medical device community on hospitals and device manufactures is on saving lives and faith based risk management. Within the industry there is a tension that also trains our skill sets. For examples, companies will have trained personnel in embedded technology and implanted in medical devices with a real-time safety skill sets. The safety culture tends to be a collaborating field driven by data (numeric driven) from physics and measurements of things directed on predicting on how someone in the future might use a medical device in an adversary way. And, at the same time, there are real-time systems on the IT side of these devices. There is a need to bring the medical and security communities together for greater understanding and collaboration on these issues.

The overriding safety risk management standard in medical devices is one that Association for the Advancement of Medical Instrumentation (AAMI)[39] helped to establish as well as ISO 14971which require risk ranking such as (refer to presentation slides):

- Between Risks
- Individual Acceptability
- Overall residual Risk

These ranking mechanisms help to establish what is acceptable and unacceptable – both require mitigation. In the medical world, there is a certain amount of acceptable risks associated with them given that these devices provide a medical benefit shown through clinical studies.

The current focus of AAMI is on FDA areas. As background information, he mentioned that FDA issued some guidance a year ago that addresses market solutions. For example, what devices are intended to do in design processes and what really defines a risk management process. AAMI developed a working group that Dr. Fu and Mr. Hoyme assisted in driving the working group to define and communicate the safety issues in the medical devices. The AAMI Risk Management process is similar to the NIST SP 800-30 Rev 1, Guide for Conducting Risk Assessment[40], and ANSI/AAMI/IEC 80001-1:2010[41] Managing Medical IT Networks which addresses the disclosure of security device characteristics.

There needs to be standards for enabling integration of hospital devices. Currently, AAMI and UL (Underwriters Laboratories) are jointly developing a suite of standards on medical device interoperability - the AAMI/UL 2800 family of standards to address safe medical device interoperability.

Mr. Patel stated that within FDA the emphasis is to ensure product safety and usability. For example, one would not want a 15 digit past code in order to turn on any medical equipment. FDA is very cautious and does recognize many standards such as ANSI/AAMI/IEC 80001-1:2010. Within a pre-market review one should consider what is a good practice to promote and maintain safety. FDA can assist in regulating and providing standards to the medical device manufactures but has not enforced end user accountability.

[40] http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

[41] http://www.aami.org/publications/standards/80001.html

Dr. Nordenberg began his presentation by recalling the presentation he gave to the Board three years ago on the public health perspective regarding medical devices, and he followed up with the following areas to his question – "What should the medical community ask about the medical devices available today?":

- How preventable is the outcome?
- How many times do medical devices encounter a patient?
- What happens if the device does not function properly?

The entire healthcare system uses medical devices and the system would come to a complete standstill if the medical devices stop working. The landscape in the medical arena is changing rapidly, and there are many different classes of devices that compound the issue of security for medical devices. Furthermore, many medical devices are not regulated. Manufactures are very concerned in secure safety measures but they are seeking clear direction.

The challenge for quality assurance is a conflict of cyber device management and the motivation for patching devices. For example, what is the protocol if there is an old device that needs an update? In the medical device standards community the emphasis is on agile perspective.

NCCoE (National Cybersecurity Center of Excellence) Updates

Matt Scholl, Acting Division Chief, Computer Security Division, NIST

Mr. Scholl began his updates with an overview of NCCoE. NIST was asked to establish a center as a partnership operation with the State of Maryland and Montgomery County Maryland government, and an official memorandum of agreement was finalized by Dr. Pat Gallagher, NIST, and Governor O'Malley, State of Maryland, to collaborate in the operation of this center. The center's mission is to look at applied engineering mission space so the overall mission itself is to jumpstart or accelerate the use and adoption of existing cybersecurity technologies. This is structured by adopting specific constructions of use cases. The methodology behind is to reach out to a community; for example, healthcare and to find out what are the challenges in cybersecurity through implementation, understanding return on investment, and addressing threats. NCCoE will initiate collaboration with the community to create use case(s) that is/are specific example of their challenges. The use case would be published via federal register notice or Request for Information (RFI) and be available for public comments. It is an open request to industry to collaborate with NCCoE to build a prototype that would closely demonstrate the identified challenges. This would provide that community in this case, healthcare with a concrete understanding of the issues and architectures which will help them deploy a system. This process is intended to be modular so that if an organization presents one technology in the build process, another organization with another technology can also participate to help build a system.

The center is currently working on five use cases which have been published for public comments. There are two for healthcare, two for financial services and one for electric power. Three of the use cases are approaching the build phases for implementation. For the Energy Sector Identity Access Management use case, four companies have started building use cases at NCCoE. In response to the Board's query on companies that have collaborating with NCCoE, Matt Scholl listed those technology vendors as: CISCO, HP, ITRUST, ID Data Web, Red Hat and Microsoft. NCCoE plans to work on building blocks that are universal to different use cases and are important across multiple communities; for example, trusted geo-locations, cloud, derived credentials, and trustworthy email. Vendors will be invited to visit NCCoE for demonstration of their technologies.

NCCoE has been in operation for past two years and at the location nearby NIST's campus in Gaithersburg, Maryland. Mr. Scholl would like to invite the Board to hold a meeting at NCCoE. The center is hosting a quarterly open house scheduled for June 19, 2014 to update the public and various communities on the status of the centers activities. NIST identified that the federally funded research and development centers (FFRDCs) would be the best mechanism to support the mission of the center. This will be the first FFRDC for the Secretary of Commerce. The proposals for the FFRDC were received on May 29, 2014 and the intent of award is to be awarded this fiscal year.

Board Discussion on Heartbleed

The Chair led the discussion on the recent Heartbleed security bug found in the Open SSL cryptography library which was released to the public on April 7, 2014. Mr. Thomlinson believed this topic is a useful discussion and he asked the Board if it is necessary to have a follow-up discussion at future meeting. He asked the Board to think about this incident in terms of the response, the source and/or testing involved. Mr. Scholl mentioned that NIST has been reviewing the vulnerability threat, and it seems none of NIST testing systems would have detected this vulnerability.

Dr. Fu queried the Board as to the true causes for the public opinion is to blame faulty implementation. Dr. Weinberger mentioned that if one imagines doing a formal verification of the open SSL, one may probably find that the protocol is underspecified by the number in which it is supposed to be returned or, if that is not the case, then it was missed during implementation. He added that if one finds the bug using a formal implementation method that is a pretty fine level of detail to ensure one has modeled after. When this open SSL, which was established as a standard source, became widely used, the question of verifying the implementation process should have been raised. With the Heartbleed bug found, it raises the question from a security perspective of other sources that the general public relies on. We realized that there were many things we did not understand at the time when it was developed. There have been other bugs found related to this openSSL but were not as damaging. In this case the vulnerability can be patched but some vendors have not done so.

The Board discussed the issue of notification of such occurrence – who and how, and in this particular case, the people/organization (Google) that discovered it. Google had to consider a complex number of questions to respond such as who and how should be informed they told so as not to leak the information prematurely and caused more damage. At some point it was a difficult transition to release the information publicly. There are three questions to categorize such bugs:

1) How does one prevent this type of flaw
2) How does one detect it (example static analytics, fuzzing etc.)
3) How does one respond within the open source community

The board discussed that Open SSL – has had a long series of problems – some of them have had no problem with the implementation process but at the source bugs were found. If you look at open source, there are no federal dollars going into it. The good news in this incident is it was found before it could be exploited. Additional questions and comments to think about are:

- Will this bad library come back to us?
- There is an incentive not re-write the code – libraries, bad or otherwise, are being used over and over again which are also old codes.
- How much of this is a single point of failure?

The Board would like to know the effects and impact of this openSSL incident has on the government, and would like to invite DHS representative to discuss the government response and perspective for such special incidents. For example, whether there are procedures in place to handle these incidents and when it was last implemented. The Board would like to know of the foundational risks for government based on this incident (Heartbleed).

Friday, June 13, 2014

Mr. Thomlinson called the meeting to order at 8:59 A.M. and introduced the presenters for the following discussion.

Federal Cloud Credential Exchange (FCCX) and the NSTIC

Douglas Glair, Manager, Digital Identity Services, USPS (presentation provided)[42]
Naomi Lefkovitz, Senior Privacy Policy Advisor, NIST

Ms. Lefkovitz began with an overview of Federal Cloud Credential Exchange (FCCX) and how it relates to National Strategy for Trusted Identities in Cyberspace **(**NSTIC**)** and Federal Identity, Credential, and Access Management **(**FICAM**)**. On average, users have 6.5 web passwords, 25 accounts requiring passwords, and enter approximately 8 passwords per day. It is necessary to bring convenience, security and privacy to on-line interactions for users. NSTIC has a specific goal in mind that focuses on individuals and organizations to utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. It is more than a goal to have the Federal government as an early adopter of multi-factor credentials. The NSTIC program has developed a process known as FICAM which consists of trusted framework solutions of identity solutions using 4 levels of security requirements. These levels do not certify the identity provider but approve the provider's solution as a trusted source. These levels are identified from level of assurance (LOA) 1 as the lowest level which is of little to no confidence of identity required to LOA 4 the highest level which is of very high confidence of asserted identity {see presentation slide #5}. The FCCX accelerates NSTIC and FICAM by allowing agencies to securely interact with a single "broker" to authenticate consumers. She explained that this process would alleviate a government employee from getting their credentials approved five times when accessing five different agencies. The way it is intended to work is for an individual to login to a FCCX exchange and have their credentials authenticated only once for multiple agencies. This would assist federal employees and contractors particularly those who are required to verify their identity for multiple levels of security.

As to the determination of appropriate LOA, Ms. Lefkovitz stated that the agency is responsible for setting the LOA based on their risk assessment for each agency. It is an agency to choose the acceptable level and indicate on the application for FCCX. She continued by saying that they have about ten agencies that are onboard and additional five currently undergoing the implementation phase of FCCX. The idea is to have a broker in the middle with one protocol for the agency. The benefits of this process are:

- Centralized interface between agencies and credential providers – reduces costs and complexity, speeds up integration timeline for new IDPs
- Enhanced consumer privacy and experience; user does not have to get a new credential for each agency application
- Decreased Federal government authentication costs

Mr. Glair said that they are also focusing on the user experience and enhancements of what they will work towards in the future. The FCCX process is when the user accesses an online application page and the technology will offer the user two options: embedded selection on agency page or standalone page as described in the presentation. The NSTIC program is encouraging the user to select the embedded

[42] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-06/ispab_jun2014_fccx-briefing_glair.pdf

selection which will allow multiple access to various agencies whereas the standalone option will only offer login to one agency.

The concept is once the process of FCCX is initiated, the request goes to the agency and to the service provider page on the Federal CLOUD network. The third party "broker"will not recognize the specific agency and will strip out the URL. Secure key was selected as the broker in FCCX and they are currently going through the FEDRAMP certification process. A key component of FCCX from a privacy perspective is that the broker does not retain or store any PII information and only the user's unique character string numbers ensuring privacy by design is submitted every time a user is authenticated. Although using Secure Key as the broker for the FCCX exchange, multiple credential providers may also be used. There will be a fee to agencies for this service but it will save more money for them and there is no cost for the user. The cost for service providers and broker are being finalized. The NSTIC program is paying for unlimited authentication across agencies.

No Public Participation was requested.

NIST Updates on Cryptography Process

Andrew Regenscheid, Computer Scientist, Computer Security Division, NIST

Mr. Regenscheid iterated NIST's focus is to restore public confidence. This has been a challenging time and thanked to the ISPAB's support and a lot of support in general.

Since the last ISPAB meeting, NIST has put out a number of publications including FIPS 202 SHA 3[43] (Draft), key management[44] update, and the PIV[45] [46] document updates. NIST has also updated SP 800-90A[47] (2ND Draft) which was the Deterministic Random Bit Generators (DRBG) issue. NIST has removed those guidelines.

The VCAT review of NIST's cryptography program and processes are underway. The VCAT invited a Committee of Visitors (COV) to assist NIST in this review. The COV sub-committee will conclude its review and present the report in July to the VCAT. NIST will release the report and recommendations at that time and before the next ISPAB meeting scheduled for October, the VCAT will make a

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

[44] SP 800-57 Part 3-Rev.1 DRAFT Recommendation for Key Management: Part 3 - Application-Specific Key Management Guidance http://csrc.nist.gov/publications/drafts/800-57pt3_r1/sp800_57_pt3_r1_draft.pdf

[45] SP 800-78-4 DRAFT Cryptographic Algorithms and Key Sizes for Personal Identity Verification
http://csrc.nist.gov/publications/drafts/800-78-4/sp800_78-4_revised_draft.pdf

[46] SP 800-73-4 DRAFT Interfaces for Personal Identity Verification (3 Parts)
Part 1- PIV Card Application Namespace, Data Model and Representation
Part 2- PIV Card Application Card Command Interface
Part 3- PIV Client Application Programming Interface

[47] http://csrc.nist.gov/publications/drafts/800-90/sp800_90a_r1_draft.pdf

recommendation to Dr. Willie May, Associate Director for Laboratory Programs, NIST. NIST needs to thoroughly document the on-going processes.

Board's Review and Wrap-up

Annie Sokol, DFO, reported that the Board's Membership requirements/openings as follows:

Requirements as stipulated in the Charter:

1) Four members representing Federal Government with at least one of whom shall be from the National Security Agency;
2) Four members from outside the Federal Government who are eminent in the information technology industry, at least one of whom is representative of small or medium sized companies in such industries;
3) Four members from outside the Federal Government who are eminent in the fields of information technology, or related disciplines, but who are not employed by or representative of a producer of information technology.

Openings – Currently, the Board needs to fill one position in both category 2 and 1 as Julie Boughn is no longer a federal employee. NIST is finalizing the lengthy process to appoint Dave Cullinane as a member which will be the 4th member for category 3.

Possible nominees for consideration:

- Danny Toller, DHS – NIST will look into having him to attend the meeting in October. (Cat 1)
- Chuck Brook (Liaison from DHS) (Cat 1)
- Earl Crane (Cat 2)
- Lynn Goldstein (Cat 2)

The Board suggested looking for nominees who are from authentication service, Security or CISSO type (federal government position) or Kaiser Permanente POC. NIST does have a list of applicants to join ISPAB. The board noted that the NIST Director will have to approve new board members.

Review agenda discussion topics, action items and future topics.

NIST updates

- No Actions.
- To plan on hosting a future ISPAB meeting either at NCCoE or NIST

PIV Credentials for Mobile devices and Wireless environment

- Should the pairing code be a requirement for agencies and how important is the general principle

Big Data & Privacy

- Report has short comings, the Board recommends to follow up on this topic specifically of technology not analytics
- The issue is how does one ensure that the privacy information is being built into big data?
- Discuss cloud computing and geolocations as a technology development (example, building technical integration for a policy)

- Health IT (next phase) Meaningful Use Program – the Board would like to have a presenter come and discuss certifiers or standards from a big data and privacy perspective and also a presenter on HHS, e.g. Tamie Roberts, NIST.

PCLOB Updates

- Section 215 Report did not have a lot of meaningful information due to time constraints;
- Section 702 Report projected to be completed by October 2014 which will be in time for the next ISPAB meeting. The Board would be interested in inviting David Medine to give an update.

FISMA FY13 Report

- CAP Goals – It does not deliver the needed help or benefits
- Request for a presentation/discussion from DHS on Continuous Monitoring Program and/or Continuous Diagnostics and Mitigation (CDM)

US CERT

- Risk /action based presentation – great presentation and updates
- Report on trends – US CERT was built on baselines for FY2015
- Lower level use of NSTICS – Information exchange topic follow-up for future meetings

International discussions/Norms – White House Update

- The Board agreed that it is always good to have an update from representative from the White House
- Status on MLAT (Mutual Legal Assistance Treaty)[48] (suggested to invite either Nathaniel Gleicher or Ari Schwartz)

Feedback from Charles Romine and recommended topics for future discussion

- Privacy Engineering
- Data Analytics – Charles Romine
- Can we provide engineering systems that address privacy?
- Naomi Lefkovitz, NIST, to update on Privacy Engineering workshop in October

CUI and NIST Standards

- It was agreed to be vigilant on this topic and specifically look at resource impact
- It will be CUI/ sub-categories on the applicability to agencies and how many sub-categories will be used
- Private sector and information sharing regarding CUI and the resulting effect.

Medical Device Security

- The Board found the discussion and issues presented very interesting
- FDA does have authority over manufacturers but no users
- Meaningful Use Program – Get a speaker for a future ISPAB meeting
- Board needs to determine whether to reaffirm the NIST / FDA guidance and action to be taken such as submitting a recommendation letter. No action was agreed to be taken by the Board
- Review safety issues concerning this topic
- Discussed if there are any legal or criminal issues considered as reckless endangerment cases

[48] http://www.whitehouse.gov/the-press-office/2014/01/17/fact-sheet-review-us-signals-intelligence

- Manufactures responsibility is to demonstrate safety. The question remains whether FDA has the authority to withdraw a product if manufacturers fail to take action on known risks. There was only one known instance that occurred in 1976
- Medical Device Security Board thoughts:
    - There will be a lot of un-anticipated issues with medical devices
    - Does the current model need to be changed
    - Require a certain process that organizations should follow
    - Consideration for Device manufactures to have clinical trials

NCCoE Update

- Use case report would be of interest to the board. This was discussed for a 2015 ISPAB Meeting follow-up discussion

HeartBleed Discussion

- CDM, configuration management when there is an incident
- Predict common dependencies across government agency foundations and whether the government is exposed to openSSL bugs
- The Board would like to have an update from DHS to discuss on lessons learned in scenarios like Heartbleed
- National Security Staff update to discuss how they handle such occurrences
- Review government response with incidents

Fed CLOUD - FCCX

- The Board had the following questions but agreed that no further follow up is necessary:
    - What is the issue and public perception of the issue?
    - How does USPS explains privacy to the consumer as it is not easily distinguished to users?
    - Does the CLOUD exchange increase or decrease phishing emails?
    - What are the risks?

NIST Cryptographic process

- The Board would like to have an update specifically after release of VCAT Recommendations

New Topics for consideration

- Follow up on supply chain risk[49]
- Continual authorization issue
- CAP Goals – how do they apply to CLOUD (like TIC or a user perspective/VPN)?

The meeting adjourned at 12:06 P.M., Friday, June 13, 2014.

[49] DFARS Case 2012-D050

Annex A

June 11, 2014

Michael Daniel
Special Assistant to the President and Cybersecurity Coordinator
The White House
Washington, DC 20500

Dear Mr. Daniel:

Our associations, which represent nearly every sector of the American economy, applaud you and the administration for supporting a dynamic and flexible approach to addressing cybersecurity risk. Your May 22 blog, *Assessing Cybersecurity Regulations*, sends businesses and other stakeholders an important message that the *Framework for Improving Critical Infrastructure Cybersecurity* (the framework) should remain collaborative, voluntary, and innovative over the long term.

Like you, we have invested considerable time and energy toward developing the framework. The National Institute of Standards and Technology (NIST) handled a challenging assignment in ways that ought to serve as a model for other agencies and departments.

We agree with your assessment in the blog that business and government “must build equally agile and responsive capabilities not bound by outdated and inflexible rules and procedures.” Our organizations particularly urge independent agencies and Congress to adhere to the dynamic approach advocated by the administration and that is embodied in the nonregulatory, public-private framework.

In addition, industry has demonstrated its commitment to using the framework. Many associations are creating resources for their members and holding events across the country and taking other initiatives to promote cybersecurity education and awareness of the framework. Some examples are listed here. Associations are planning and exploring additional activities as well.

- The American Gas Association (AGA) has hosted a series of webinars on control system cybersecurity and is working with small utilities to develop robust cybersecurity programs. Among other activities, AGA is standing up the Downstream Natural Gas Information and Analysis Center (DNG–ISAC), an ISAC designed to help support the information-sharing interests of downstream natural gas utilities.

- The American Hotel & Lodging Association (AH&LA) has conducted a series of widely attended cyber and data security webinars to assist small, medium, and large hotel and lodging businesses with implementing key information security measures and risk assessments.

- The American Water Works Association (AWWA) has created cybersecurity guidance and a use-case tool to aid water and wastewater utilities’ implementation of the framework. The guidance is cross-referenced to the framework.

- Members of the Communications Sector Coordinating Council (CSCC)—made up of broadcasting, cable, wireline, wireless, and satellite segments—have participated in multiple NIST, Department of Homeland Security (DHS), and industry association-sponsored programs, webinars, and panels with future events being planned.

In addition, the communications sector has roughly 100 cybersecurity experts engaged in the Federal Communication Commission's (FCC's) voluntary Communications Security Reliability and Interoperability Council (CSRIC) to adapt the framework for the segments, focusing on an understanding of shared responsibilities across the ecosystem, the impact on small and medium enterprises, evolving threats, and barriers to implementing specific risk-management capabilities.

- The Electricity Subsector Coordinating Council is working with the Department of Energy (DOE) to develop sector-specific guidance for using the framework. The guidance leverages existing approaches to cybersecurity, including DOE's *Electricity Subsector Cybersecurity Risk Management Process Guideline*, the *Electricity Subsector Cybersecurity Capability Maturity Model*, NIST's *Guidelines for Smart Grid Cyber Security*, and the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection Cybersecurity Standards.

- The mutual fund industry, represented by the Investment Company Institute (ICI), has recently added to its committee roster a Chief Information Security Officer Advisory Committee. The committee's mission is to collaborate on cybersecurity issues and information sharing in the financial services industry and provide a cyber-threat protection resource for ICI members.

- The Information Technology Industry Council (ITI) recently visited Korea and Japan and shared with these countries' governments and business leaders the benefits of a public-private partnership-based approach to developing globally workable cybersecurity policies. ITI highlighted the framework as an example of an effective policy developed in this manner, reflecting global standards and industry-driven practices.

- The National Association of Manufacturers (NAM) has spearheaded the D.A.T.A. (Driving the Agenda for Technology Advancement) Policy Center, providing manufacturers with a forum to understand the latest cybersecurity policy trends, threats, and best practices. The D.A.T.A. Center focuses on working with small and medium-size manufacturers to help them secure their assets.

- The oil and natural gas sector has established a new Oil and Natural Gas Information Sharing and Analysis Center (ONG–ISAC) to provide shared intelligence on cyber incidents, threats, vulnerabilities, and responses throughout the industry.

- The Retail Industry Leaders Association (RILA) has created the Retail Cyber Intelligence Sharing Center (R–CISC), featuring information sharing, research, and education and training. This ISAC enables retailers to share threat data among themselves and receive threat information from government and law enforcement partners.

- The U.S. Chamber of Commerce has launched its national roundtable series, *Improving Today. Protecting Tomorrow*™, recommending that businesses of all sizes and sectors adopt fundamental Internet security practices.

As you note in your blog, NIST and multiple stakeholders produced a smart framework that stakeholders are proud of. But more work lies ahead. We look forward to working with policymakers to ensure that preexisting regulations are harmonized with the collaborative and voluntary nature of the framework. Businesses also seek the enactment of information-sharing legislation to achieve timely and actionable situational awareness to improve our detection, mitigation, and response capabilities.

We share your commitment to protecting America's business community and enhancing the nation's resilience against an array of physical and online threats. Government and business entities need to leverage the framework to strengthen collective resilience and security and make ongoing improvements.

Our organizations look forward to working with you and your colleagues to build on the progress that we—industry and government—have made together.

Sincerely,
Airlines for America
American Chemistry Council
American Fuel & Petrochemical Manufacturers
American Gas Association
American Hotel & Lodging Association
American Petroleum Institute
American Water Works Association
ASIS International
BSA | The Software Alliance
CTIA–The Wireless Association
Edison Electric Institute
The Illinois Chamber of Commerce
Information Technology Industry Council
National Association of Manufacturers
National Business Coalition on E-Commerce & Privacy
National Cable & Telecommunications Association
NTCA–The Rural Broadband Association
Retail Industry Leaders Association
Security Industry Association
Software & Information Industry Association
Telecommunications Industry Association
United States Telecom Association
U.S. Chamber of Commerce

Annex B

LAST	FIRST	AFFILIATION	ROLE
Curran	John	Telecom Reports	Media
Mazmanian	Adam	1105 Media	Media
Perera	David	Politico	Media
Thomas	Carlos A	ECI	Media
Barron-DiCamillo	Ann	DHS	Presenter
Blumenthal	Marjory S.	OSTP	Presenter
Bradford Franklin	Sharon	PCLOB	Presenter
Cooper	David	NIST	Presenter
Ferriaolo	Hildegard	NIST	Presenter
Fitzpartick	John	NARA	Presenter
Glair	Douglas	USPS	Presenter
Hoyme	Ken	Adventum Labs	Presenter
Lefkovitz	Naomi	NIST	Presenter
Nordenberg	Dale	Medical Device Innovation	Presenter
Patel	Bakul	FDA	Presenter
Regenscheid	Andrew	NIST	Presenter
Ross	Ron	NIST	Presenter
Rudolph	Trevor H.	The White House	Presenter
Schwartz	Ari	The White House	Presenter
Viscuso	Patrick	NARA	Presenter
Ahu	Jay	MDISS	Visitor
Brown	Evelyn	NIST	Visitor
Fernando	Himali	VA	Visitor
Grassi		NIST	Visitor
Hale	Lawrence	GSA	Visitor
Herman	Carol	AAMI	Visitor
Lewis	Samantha	US Dept of Treasury	Visitor
Newton	Elaine	NIST	Visitor
Romine	Charles	NIST	Visitor
Scherger	Tucker	VHA	Visitor
Smith	Matthew	GZM Inc.	Visitor
Suh	Paul	DHS	Visitor
Taylor Moore	Debbie	Cyber Zephyr	Visitor
Van Dervort	Emma	ISOO	Visitor