-

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

December 19 and 20, 2013

	Board Members	
Thursday, December 19, 2013 8:38 A.M. – 4:51 P.M. Friday, December 20, 2013 8:30 A.M. – 4:10 P.M. Microsoft Innovation and Policy Center 901 K Street, NW, Suite 1100,Washington, DC 20001	Present	Joined via Teleconference
	Matthew Thomlinson (Chair), Microsoft Christopher Boyer, AT&T John Centafont, NSA Greg Garcia, Garcia Cyber Partners Brian Gouker, NSA Toby Levin (Retired) Edward Roback, Department of Treasury Gale Stone, Social Security Administration Peter Weinberger, Google, Inc.	Julie Boughn, DHHS /CMS Kevin Fu, University of Michigan

See Annex A for list of presenters and visitors.

Thursday, December 19, 2013

The ISPAB Chair, Matt Thomlinson, called the meeting to order at 8:38 A.M. and informed the Board and audience that an adjustment had been made to the schedule. Dr. Andy Ozment, Senior Director for Cyber Cybersecurity, the White House, would speak at 8:30 A.M. and Board Chair's opening remarks would be at 9:30 A.M. as Dr, Ozment had to leave for another commitment.

Legislative and Executive Office Update

Andy Ozment, PhD., Senior Director for Cybersecurity, National Security Staff, The White House

Dr. Andy Ozment gave a brief overview of the National Security Office perspective of how the White House National Security Office views Cybersecurity and what the main priorities are:

1. Protect Critical Infrastructure
2. Improve Incident Response
3. Secure the Government
4. Engage Internationally
5. Shape the Future

The thought is to enable critical infrastructure to protect itself by enabling owners and operators rather than have the government protect it. Dr. Ozment referenced the Executive Order 13636[1], *Improving Critical Infrastructure Cybersecurity*, which President Obama spoke about in his State of the Union speech on the same it was signed in February 2013, and provided an update of the progress and what still needs to be done.

Information sharing can be broken down into three categories:

- Issue clearances
- Share more information
- Cybersecurity framework

With respect to clearances, recent accomplishments include identifying owners and operators of currently held clearances that are either inactive or are not held by Department of Homeland of Security (DHS). TSSCI clearances are currently being approved. One of the challenges with clearances is that the clearance process was designed specifically for clearing private sector companies that are offering a service to the government. This results in a contractual relationship with the private sector company so that requirements and expectations can be placed on the leadership of those companies. These assumptions now do not necessarily apply when considering the owners and operators of Critical Infrastructure; however, those assumptions have security purposes.

For example, there is a requirement that the head of each cleared organization have a security clearance. This requirement was created due to a concern that if a lower-level employee has a security clearance and working for a possible untrustworthy head of the company, the lower-level employee could be pressured to divulge secure information. This example demonstrated the necessity for these requirements even though they may not be practical to today's world. Dr. Ozment explained that we are in the process of trying to analyze our current system and determine whether or not it is possible to adjust to meet today's needs.

Is it even possible to construct an entirely different system and achieve the same security safeguards that underlie the motives of the current system? This is a tougher problem than anticipated, but there are a lot of people actively working on it and analyzing whether or not it can be done. There are people currently being vetted through the process, and 90% of the organizations that need to clear an individual were able to receive accurate clearances. DHS is currently working on the remaining 10% of organizations that were not able to get clearances through the system and are currently analyzing whether or not these cases can use the current system at all or whether adjustments need to be made. DHS is not going to offer clearances to everyone in critical infrastructure so we have had to change our culture on sharing information.

In order to change the culture, it is to focus on information that the government has regarding whether a particular company is either being targeted or is the victim of a cybersecurity incident by an intrusion or attack. It is decided to push the broader culture to not necessarily share information with the private sector. While there seems to be success with this private sector culture, it is an antidotal success, which means that if an organization has not been targeted or

[1] http://www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf

classified as a victim, it would not be contacted. However, there are various agencies, such as the FBI, DHS, and sector-specific agencies that are reaching out to the private sector. Feedback from a private sector company described information sharing was so intense at times that the company received multiple inquiries from five different agencies in one day. This maybe great in theory but it needs to be more of a single coordinated inquiry. FBI and DHS are operating in a more coordinated fashion and focused in pulling in data from the other agencies.

A portion of information still needs to remain classified so as to evaluate the value and effectiveness of declassifying and sharing the information. When information was declassified and shared with the private sector so as to provide indicators as alert to various threats, within 3 or 4 days, our adversaries had changed their tactics and altered their activities, and those indicators are no longer applicable.

In response to the Board's remark that this will cause the adversaries to work harder, Dr. Ozment explained that the adversaries became aware of the alerts before the information was shared An indicator for a phishing email that highlights the sender or a particular aspect of the header will allow the adversaries to promptly make the change. One of the solutions to this response is Enhanced Cybersecurity Services (ECS)[2]. The layered approach of ECS is a managed security service in which DHS provides classified indicators; it was kept classified but was offered a black box service to private sector customers, and it is now operational for private sector critical infrastructure customers. Previously, the ECS had been offered to Defense Industrial based organizations only but we now have customers that are not limited to defense.

Dr. Ozment proceeded to provide a high-level overview of the Cybersecurity Framework[3]. The preliminary Framework was released in October 2013 with comment period closed on December 13, 2013. NIST is in the process of reviewing comments. The final Framework is on schedule to be released in February 2014. At the same time the Framework is released, DHS will be initiating the Voluntary Program. As part of the Voluntary Program, DHS has been developing incentives to motivate companies to adopt the Cybersecurity Framework.
Dr. Ozment recognized that creating incentives has been difficult as some incentives will need congressional action. The Executive Branch has proposed other incentives. DHS will not have all incentives completed by the launch date, and more incentives will be added over time. These are the biggest efforts under "Protect Critical Infrastructure."

One of the National Security goals is to empower CIOs and CISOs at the department level. The department-level CIO may have 6 or 7 components and within each component there are a CIO and a CISO. IT management has reached an incoherent point at the individual component level and cannot manage the IT requirements at a CIO and CISO department level. The current approach is to use the Cross Agency Priority (CAP) goals[4] across agencies. These consist of the following three goals that started in FY13.

- Trusted Internet Connections (TIC)

[2] http://www.dhs.gov/enhanced-cybersecurity-services
[3] http://www.nist.gov/cyberframework/
[4] http://goals.performance.gov/content/cybersecurity; http://my-goals.performance.gov/sites/default/files/images/Cybersecurity%20CAP%20Goal%20-%20FY2013%20Quarter%201%20Update.pdf

- Continuous monitoring
- Homeland Security Presidential Directive-12 (HSPD-12)

The progress can be found on www.performance.gov. DHS would essentially set targets that would track the progress against those three goals. The performance progress can be viewed every quarter.

Continuous Diagnostic Monitoring (CDM)[5] is a tool that can benefit every level. It allows a department-level perspective of monitoring an agency. For example, a component-level CIO will have more visibility to monitoring the systems, and therefore, it holds the system owners accountable much more effectively. At the White House-level, all the information will roll-up across agencies and will provide a lot more visibility across the agencies and hold department-level CIOs accountable. This is an important tool for monitoring and tracking progress across agencies.

Continuous monitoring is a phased program, and the first phase is setting up capabilities for inventory for hardware and software (What do I have and where is it located), vulnerability management, and configuration management. A broader time scales will be started initially, and narrow down to appropriate risk levels.

Trusted Internet Connections (TIC)[6] initiative is critically important to detection. Finally, HSPD-12 is of the most interest to CIOs, but it is least progressive[7] because there are some challenging areas yet to be resolved such as mobile and hand-held devices. Most importantly, DHS needs to focus on consolidating identity infrastructures, and ultimately, everyone will need to adopt this program.

Measuring performance is a challenge of government-wide management and not just for IT management. This is the motivation to work on empowering CIOs, pushing individual departments and agencies, and crafting to change how department CIOs and component-level CIOs interact. For example, some performance reviews for component-level CIOs should be completed by the department CIO. Also, IT Acquisition should be reviewed by the department-level CIO. These are basic management constructs that do not exist in the agencies at this present time. This explains why department CIOs are both un-empowered and often completely ignorant in terms of IT Acquisition. DHS is focused on providing tools to assist with these management issues.

National Initiative Cybersecurity Education (NICE) is meeting the needs for training and education for CIOs. One of the things NICE has achieved is to create workforce categories, which are being used and implemented in the Human Resources database that is applied across the government agencies. Also, templates are being formulated for agencies' use in this database. Federal agencies are required to re-categorize their IT security workers with security related functions. This will help government agencies to have standard position descriptions to assist in hiring qualified people.

[5] http://www.dhs.gov/cdm
[6] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/2008_TIC_SOC_EvaluationReport.pdf
[7] http://www.whitehouse.gov/omb/e-gov/hspd12_reports

As for FY15 priorities, Dr. Ozment responded that due to the CAP goals for FY13-14, White House Officials were in the process of doing the FY15 budget; however, challenges to the budget hindered a final agreement. They reviewed their CAP goals and work across the classified world with the post-WikiLeaks effort. While the review of FY15 is far from 100% complete, the work to address the priorities of the WikiLeaks is much further along. Concurrently, because of the continuous monitoring effort, DHS has had a joint effort in the classified and unclassified world working on the standards of continuous monitoring which builds upon DHS and NIST work. DHS has been converging towards more similarity between security approaches of classified and unclassified networks.

The goal to "Shaping the Future" focuses on two areas: Routing Security and National Strategy for Trusted Identity in Cyberspace (NSTIC)[8]. Dr. Ozment suggested that the Board to consider hearing more about NSTIC at next meeting. Passwords are still broken and progress will be slow. NSTIC has a number of identity program pilots that are work in progress.

In conclusion, Dr. Ozment affirmed commitment to cybersecurity and information sharing, DHS has recommended to the White House that there needs to be strong privacy requirements on information sharing.

Welcome and Opening Remarks

The ISPAB Chair, Matt Thomlinson re-addressed the ISPAB members and attendees with opening remarks and followed by a brief updates from Board members. Mr. Thomlinson briefly explained the agenda with focused discussion on EO Cybersecurity Framework and NIST Cryptology and NIST standards and procedures. There will also be some time to discuss Regulatory Updates of Embedded Software Security. Lastly, the Board will have to plan for the next year activities. This meeting was rescheduled from October 2013 due to the government shutdown.

The Chair and Board presented a certificate of appreciation to Mr. Brian Gouker in recognition for his 6-year service on the ISPAB. At the same time, the Board welcomed John Centafont as the new representative from NSA to ISPAB.

Privacy and Civil Liberties Oversight Board (PCLOB)[9]

David Medine, Chair, PCLOB

Mr. David Medine thanked the board for inviting him and called out a personal thank you to Toby Levin (ISPAB member) for their past working relationship at the Federal Trade Commission (FCC). Mr. Medine wanted to start by touching on the Cybersecurity Executive Order (EO). He stated that the Privacy and Civil Liberties Oversight Board (PCLOB) has a small roll under the EO. Agencies are supposed to consult with their agency's Privacy and Civil Liberty Officers to address the privacy concerns that relate to information sharing between the

[8] http://www.nist.gov/nstic/
[9] http://www.pclob.gov/

private sector and the government. Each agency is expected to submit a report by February 22, 2014, and PCLOB has a conciliated role with DHS in reviewing and providing comments on those reports.

PCLOB is the third reincarnation of this board, which started way back to the September 11 events. It is important to have a balance of civil liberties and security; however, if you have lost one, you have lost the other so Congress recommended a creation of a board to help address those issues. Mr. Medine recommended that reading the 9/11 report[10] where it discusses improving information collection and sharing, and particularly towards the end of the report, where there is an emphasis on not to ignore civil liberties for the sake of overly focus on security. Mr. Medine stressed that if we lose our civil liberties, we have lost what makes America a great country.

What Congress did differently is they made PCLOB an independent agency within the Executive Branch. This means that board members are confirmed by Senate. Currently, there are five board members, and PCLOB has staggered 6-year terms so there is always continuity among board members. PCLOB has no more than three board members from any political party. PCLOB is independent which means it does not require clearance from OMB or White House to express their views on legislative recommendations or any other recommendations they might have. One of the challenges of being an independent agency is that there is no help from an administrative perspective; work must been done independently especially since it is a new organization. Currently, PCLOB is working on NSA surveillance report, and it will be published upon approval by PCLOB. The only review it would require is to ensure that there is no classified information in the report.

Mr. Medine described an overview of the PCLOB's main functions. PCLOB has two major functions: 1) an oversight role and 2) an advisory role. The oversight role is to look at existing programs. PCLOB limitations are that the board is only authorized to oversee federal counterterrorism programs, which is not limited to the 16 intelligence agencies but any federal agency that has a counterterrorism program, and as for overall agency authority, PCLOB only provides reports. The PCLOB's mandate is to report to the President and Congress twice a year and optionally, they may provide ad hoc reports. The uniqueness of PCLOB is access to all top SCI clearance level information and is capable of reporting classified information directly to the President, if needed. Presently, PCLOB reports are mainly in public format. Transparency is PCLOB's goal.

The second major function is the advisory role. The PCLOB is charged by Congress to advice on new laws, regulations, and programs. The goal is to work with agencies in development of programs and provide input on civil liberties and privacy during the design phase of a program. This is to assist with any civil liberties and privacy issues that may arise moving forward.

PCLOB has access to government and private sector information for preparation of their reports. From government agencies, PCLOB is permitted by law to request information documents and testimonies from government officials. Essentially if a lower-level government official does not provide the information, the PCLOB is authorized to go to the head of the agency to request the

[10] http://www.9-11commission.gov/report/911Report.pdf

information. With regards to requesting information from private sector, PCLOB has authority to request attorney general to issue subpoena to any private sector organization to release requested information to the PCLOB. To date, the PCLOB has received all requested information from agencies and private sector without the use of a subpoena.

Counterterrorism requires a cooperative effort from the PCLOB and the other agencies' counterterrorism officials. PCLOB does not intend to duplicate the other agencies counterterrorism official's efforts, but to add value to other agencies' processes as well as vice versa. Counterterrorism officials are embedded in their respective agencies so as to monitor daily issues. As an independent agency, PCLOB does not have to report up the chain within the agency in order to obtain clearance. Federal agency counterterrorism officials are responsible to provide 803 quarterly reports. The reports are not useful in their current form because the content is numerical and not descriptive. The PCLOB is working with agencies to make the reports more meaningful and useful.

Mr. Medine listed other areas of interest as follows:

- Foreign Intelligence Surveillance Activities
- Information Sharing Environment
- Fusion Counterterrorism Center (NCC) – Reviewing updated guidelines
- FBI and Homeland Security – Intelligence related activities related to counterterrorism
- Cybersecurity
- Working with Privacy and Civil Liberty agency officials

In differentiating terrorism and criminals, PCLOB has not yet addressed how we will determine our jurisdiction between terrorism and criminals because there will be gray areas that may involve foreign intelligence, law enforcement, and surveillance, that may or may not have a counterterrorism component.

The PCLOB has a statutory limitation to only counterterrorism. With regard to our current effort (post Snowden) after the WikiLeaks, 13 Senators asked PCLOB to take on a public study of the two surveillance programs:

- Section 215[11] Access to Business Records under FISA
- Section 702[12] of FISA (known as PRISM)

Both programs address the surveillance of phone metadata specific to persons not in the U.S. The PCLOB is evaluating the legal component to these programs, looking at statutory authority for these programs and whether the programs are operating consistent with that authority. The PCLOB is also looking at the constitutional issues. For example, issues were raised with the 1st and the 4th amendments that these programs violated the Constitution. The PCLOB will also be reviewing the civil liberties, privacy as well as national security, and to determine the right balance. This Section 215 report will be completed end January, and the report on Section 702 will be completed sometime in spring 2014.

[11] http://apps.americanbar.org/natsecurity/patriotdebates/sections-214-and-215
[12] http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa

Enhance Shared Situational Awareness (ESSA): Information Sharing Architecture (ISA) - Framework & Requirements Brief - Information Security [Presentation provided][13]

Greg Garcia, (Moderator), Principal, Garcia Cyber Partners
Antonio "T" Scurlock, Enhance Shared Situational Awareness (ESSA) Portfolio Management Team (PMT), DHS Co-Lead
William "Bill' Jones, Enhance Shared Situational Awareness (ESSA) Portfolio Management Team (PMT), FBI Co-Lead

Greg Garcia, Board member, provided an overview of Enhance Shared Situational Awareness (ESSA), and that ESSA originally initiated as Comprehensive National Cybersecurity Initiative 5 (CNCI5) in 2008. CNCI 5 was in reference to the idea of connecting the centers through an understanding among the major operational centers. There were five major operational centers at that time, and currently, there are six operational centers: US CERT, Intelligence Communities, Incident Response Centers, Defense Cyber Investigation under the Justice department and NSA, and the National Threat Operation Center. It was recognized that these centers were not communicating with each other and needed to have a better capability of connecting the dots across the Government Cyber Infrastructure. DHS has added the Cybercom Center to the six operational centers.

Mr. Scurlock thanked the board for inviting DHS and the FBI to present on this subject. ESSA is a triad initiative effort between DHS, FBI, and NSA. It was only recently referred CNCI 5 with the goal to connect the operational centers to improve ESSA. Mr. Scurlock provided an overview of the topics which included:

- Problem space and what we propose as a solution to that problem space
- The solutions set and then discuss challenges and an initiative moving forward

The problem space in cybersecurity is a team sport and the collective efforts being performed independently are not enough. Essentially ESSA needs to increase security resilience and have a better understanding of situational awareness that is not just our own infrastructures and architectures but our partners' as well. ESSA would also like to study our adversarial infrastructure and architectures. When it was discovered that government agencies do not communicate with each other using the same terminology, it was determined to change the way agencies report incidents. The issue is that each agency has formulated its own terminology. The resolution is to adjust the intercommunication between organizations. If agencies focused on functional tasks of their missions, then agencies would find that their functions were similar to one another. The Information Sharing Architecture (ISA)[14] that was created defined a set of cybersecurity functions that were designed to accommodate the full range of cybersecurity

[13] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-12/essa_isa_intro_requirements_overview.pdf
[14] https://www.dhs.gov/topic/information-sharing

activities that may or may not be performed by a particular organization. The seven functions are (see ISA handout):

- Network Operations Functions (NOF)
- Computer Network Defense Function (CNDF)
- Domain/Sector Awareness Function (D/SAF)
- Threat Assessment Function (TAF)
- Threat Operations Function (TOF)
- IOA Planning Function (IOAPF)
- IOA Coordination Function (IDACF)

One of the benefits of removing that inter-organization language piece was that agencies were capable of faster communication of reportable incidents. Another component to the seven operational functions was the Enduring Functional Exchange (EFEs) of the seven categories of information. The thought process behind this was that you can only investigate and troubleshoot in so many ways. This standard communication assisted with 90% of the information communicated by using these functions, and includes the development plan, creating a course of action, mitigating the incident and articulating the threat and/or adversary.

EO Cybersecurity Framework [Presentation provided]

Donna Dodson, Chief, Computer Security Division, NIST
Matt Scholl, Deputy Chief, Computer Security Division, NIST
Adam Sedgewick, Senior Information Technology Policy Advisor, NIST
Jon Boyens, IT Specialist, Computer Security Division, NIST
Naomi Lefkovitz, Senior Privacy Policy Advisor, NIST
Victoria Pillitteri, IT Security Specialist, Computer Security Division, NIST
Kevin Stine, Group Manager for Security Outreach and Integration Group, Computer Security Division, NIST

Mr. Scholl thanked the board for inviting NIST back to provide a follow-up status of the EO Cybersecurity Framework. He continued by saying this is a significant event for the NIST Computer Security Division, one they have been working on this past year.

Mr. Sedgewick mentioned that the staff on the panel today contributed to some piece of the Executive Order. He provided a brief overview of the main focuses that will be briefed during this meeting; mentioning the progress of the Cybersecurity Framework[15] (*what is accomplished and what is planned next*), information sharing, and comments that NIST received on the privacy section of the framework. Mr. Sedgewick mentioned that he would like to seek the Board's advice from this discussion.

The presentation of the Cybersecurity Framework overview includes a timeline of the Framework schedule and its progress (slide #4). Previously in February 2013, NIST released the Cybersecurity Framework RFI[16]. NIST received 245 responses from individual organizations to large associations. NIST posted the comments publically and began the analysis. NIST

[15] http://www.nist.gov/cyberframework/
[16] http://www.nist.gov/cyberframework/cybersecurity-framework-rfi.cfm

validated the resolution at the 2nd workshop held at Carnegie Mellon University, in Pittsburgh, PA, May 2013. NIST's priority during this workshop was to determine whether or not the right questions were asked. An average of 4-500 people attended each workshop, which included general sessions and individual working groups. The working groups were led by strong facilitators that assisted with extracting information from the group. Then, NIST regrouped and evaluated the information discussed during the individual work groups. Mr. Sedgewick explained that once NIST had the information from the workshops, they outlined it based on what they thought the Framework should be. At NIST's 3rd Workshop the outlined approach of the Framework was validated. As a result NIST collected eight different sets of data and regrouped in order to evaluate the data captured and to make the data cohesive. The data collected from the 3rd workshop was reviewed in the 4th Workshop in Dallas, TX.

The requirement under the Executive Order is to provide the preliminary Cybersecurity Framework within 240 days and then the final within a year. NIST missed the preliminary deadline due to the October 2013 furlough. However, NIST did post a preliminary draft[17] end October 2013 for a 45-day comment period, which ended on December 13, 2013. NIST received 210 comments and a few comments are still forthcoming. NIST have reviewed all comments to determine whether any comments were in or out of scope. The Framework will be released on February 13, 2014.

Mr. Sedgewick explained that now he has discussed the Framework process, he can discuss the actual Framework in more detail.

The Framework itself consists of key components that identify existing standards, best practices which are reliant on international standards best practices that elevate the use of those that will be affected. It has to be meaningful to business owners and the people that are implementing the framework. The Framework consists of three components (see slide #5 of the presentation): 1) Framework Core, 2) Framework Profile, and 3) Framework Implementation Tiers. Mr. Scholl emphasized that they changed Implementation Levels to Tiers due to the Industry CMMI standard levels.

The Framework Core functions consist of the following: (as shown on slide #6 of the presentation): Identify, Protect, Detect, Respond, and Recover.

The Framework Categories are the subdivisions of a function into groups of cybersecurity activities and sub-categories such as informative references. The intent was to keep description levels based on outcomes, based upon the goal one is intending to achieve. When developing subcategories and informative references, Mr. Sedgewick explained that NIST focused on areas that are cross sector standards like ISA-99, ISO-27001, 800-53, and critical control documents. NIST is not recommending organizations to necessarily use these standards but to consider these unique requirements. The board suggested that since these documents are recognized as standards, it is essential to ensure they are mapped correctly within the Framework. Mr. Scholl replied we have been sensitive to the potential misuse of the Framework requirements and incorporating these forms. There are people on the other end of the spectrum that do not currently have a standard within their organization and this Framework will provide a basis to set

[17] http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf

up a cybersecurity standard. The next steps are to find areas of improvement (see NIST Update PPT slides). However, essentially this Framework is what we think the stakeholders want.

In some areas where standards may be lacking and in other areas there may be an overabundance, it is necessary to have a technical and standardization component in areas of improvement. It was noted of the debate on whether "areas of improvement" represent appropriate interpretation. While that was worded in the Executive Order, but the interpretation is for future collaboration and evolution. In addition, the "Areas of Improvement" list was compiled through Request For Information (RFI) comments and workshops. Mr. Stine explained the Framework profile, current issues, and achievement goals in one's organization are based upon the specific needs. This is all based on an organization's assessment of risks using informative references to develop the target Framework and have an understanding of where an organization stands today and where it needs to be. Once a target is identified, that then becomes the current standard.

Ms. Lefkovitz provided an overview on the Framework Appendix A, which is to protect privacy and civil liberties. Ms. Lefkovitz stated NIST wants something that is tangible and that can provide guidance. The thought was to be complementary to the Framework Core. The Board commented that privacy is a consideration and there was the thought that this can be worked into the methodology. Specifically it was posited that privacy and civil liberties are not separate but actually worked into the Framework. The tiers are not considered a race to the top; they are based on an organizations' own personal organizations risk management.

NIST is specifically channeling the framework to include a methodology as a starting point. NIST will consider pros and cons including privacy when resolving comments. At present, it would be confusing to include in the Framework. One key question about privacy was whether or not it should be a separate appendix B or incorporated into the Framework core.

In summary, there have been no surprises from submitted comments. The comments requested for clarification on: privacy, defining tiers and how they relate to the CORE, scope, key words, and value of the implementation guide. NIST is still reviewing comments, but are asking what it means to ***adopt*** the Framework? The Framework is essentially proposed to be used to establish a cybersecurity program. The Board commented that the Framework may not contain enough description. Mr. Scholl requested the Board, upon the release of the Framework in February 2014, to review and provide feedback.

NIST Update

Donna Dodson, Chief, Computer Security Division, NIST

Ms. Dodson provided a brief overview of NIST cryptology, its current activities, and the importance of discussion to be held on December 20th. NIST requests the Board to provide some assistance in two areas that will be exhibited at the industry day at the National Cybersecurity Center of Excellence (NCCoE)[18]. The focuses of NIST NCCoE/FFRDC Industry Day[19] were

[18] http://csrc.nist.gov/nccoe/
[19] http://www.nist.gov/itl/ffrdc-industry-day.cfm

cybersecurity, healthcare, and use cases that seeking feedback. Some of those focuses are meant as follow on work to the EO Cybersecurity Framework.
Federal Information Process Standard (FIPS) 201-2[20] Personal Identity Verification of Federal Employees and Contractors was finally approved and published in September 2013. The publication guidelines on how to use the PIV card and the infrastructure for the PIV card were updated. This publication also expanded to strengthen authentication to mobile devices[21] for Federal ID credential security standard. This is a challenging area because NIST can see the capabilities this technology can provide over time in particularly that agencies are clearing a way to take advantage of mobile devices, e.g. identifying a proofing process. The question being considered is, *how do we maximize that security but still have flexibility with hand-held devices?* NIST is continuing to build on identity management in the crypto space as well as looking at additional challenges, capabilities and format preserving cryptology in an unencumbered, which is proving to be more challenging than originally expected.

NIST is working together with the Joint Quantum Institute (JQI) and University of Maryland working together on a quantum resistance program. NIST has completed draft documents while still researching on how to make an assessment appropriately in a short time frame. It is necessary to be an industry led approach. NIST is still working on plan and strategies for emerging program, and simultaneously, researching on a number of activities in the cybersecurity space.

The Visiting Committee on Advanced Technology (VCAT) is meeting on February 5-6, 2014, at NIST. During the meeting, the sub-committee for cybersecurity will be meeting and include a discussion on NIST cryptography activities. Mr. Scholl would like to encourage ISPAB members to participate in the discussion between 2:00 – 5:00 P.M.

The meeting recessed at 4:51 P.M., on Thursday, December 19, 2013.

[20] http://www.nist.gov/manuscript-publication-search.cfm?pub_id=914530
[21] http://www.nist.gov/itl/csd/piv-090513.cfm

Friday, December 20, 2013

The Chair reconvened the meeting at 8:30 A.M.

The Chair informed the members and audience that Board Discussion which was originally scheduled at 8:00 A.M. had been moved to the last session at 3:45 P.M. The Board will focus on NIST cryptography in the morning, and a break for public participation will be recognized if there was any request submitted from members of the public.

NIST and Cryptography [Presentation provided]

Donna Dodson, Chief, Computer Security Division, NIST
Lily Chen, Group Manager, Computer Security Division, NIST
John Kelsey, Computer Scientist, Computer Security Division, NIST [Presentation provided]
Dustin Moody, Computer Scientist, Computer Security Division, NIST – [Presentation provided]
Andrew Regenscheid, Computer Scientist, Computer Security Division, NIST [Presentation provided]

Ms. Dodson began the discussion by providing a high-level historical background of the NIST Cryptography program. The work began in the 1970s with the development of the Data Encryption Standard. At that time, there were only military grade and proprietary algorithms, but there were not any cryptographic algorithms that had been generally studied and available to the public. The financial services sector was the main driver for development. In the 1980-90s, the American Bankers Association went through the standards of the credited American National Standards Institute X9 (ANSI-X9). NIST has worked actively with ANSI-X9 for decades in development of cryptography and related cryptographic standards. Over the years, cryptography was considered a controlled standard. NIST had two cryptographers and both of them had careers that started at NSA. NIST's group has grown and now NIST has ten people who are experts in the development of cryptographic algorithms. Through the years, NIST recognizes the critical need for more cryptographers. NIST is very proud of the team and is the largest it has ever been.

NIST developed the data encryption standard using DES and ANSI-X9 (in the1980s). The U.S. government had a policy description to give the access under court management. NIST published Encryption 185 standard (classified) in addition to a lot of work done on how cryptographic keys were placed in the encryption standard. NIST developed keys that were split essentially into two sets. One set was provided to a NIST Escrow Agents[22] and the other to a member from US Department of Treasury. When both keys came together, encrypted data was able to be accessed.

The NIST encryption standard was not well received in the industry. DES was coming to the end of its life and the question was, *where are we going*? NIST decided to have a world-wide competition. NIST had a couple of workshops where organizations were able to submit algorithms. There were sixteen responses that came in from around the world, which NIST selected five submissions. During the selection process, NIST asked the community for cryptanalysis detailed solutions. NIST also created a website called the crypto lounge forum to

[22] http://www.itl.nist.gov/fipspubs/fip185.htm

cater for experts around the world specifically for this effort. NIST then published how the process for selecting those five submissions. The evaluation specifically focused on performance and security for the advanced encryption standard. All data used by the NIST staff was published in the NIST Journal of Research during each round of analysis. The process was open to the public and online. Throughout the process, NIST worked closely with NSA. NSA was aware that NIST shared the cryptographic solutions with the public.

NIST selected an encryption standard that is being used worldwide. In addition, NIST developed a few other algorithms around the same time of the encryption standard. For example, the DSA algorithm is used but not as frequently as some other ones used today. Furthermore, SHA-1 cryptography was run, the public asked NIST to have another competition but NIST wanted to wait a year so as to take time organizing such a competition. Subsequent published papers lost confidence in SHA-1.

FED-STD-1027, Federal Standard: Telecommunications: General Security Requirements for Equipment Using the Data Encryption Standard issued 14 April 1982 provides the basis for FIPS 140, A Framework for Cryptographic Standards. It used to take 32 days to validate a smart card's cryptography algorithm; however, the time it use to take to validate the process has lessened significantly due to the use of non-national security that has been validated through the FIPS 140 standard. Agencies currently rely on this as standard. NIST has a full cryptography toolkit that provides a standard for cryptography which is a broad set of knowledge. There are only few organizations that have developed cryptography solutions, such as IEEE/ANSI-X9, that are still being used today.

A recent press article questioned one of the developments of NIST's guidelines in cryptography. The press report pointed back to information released by Mr. Snowden[23]. The query related to functions described in NIST's special publications that did not offer the security that it claimed to have and whether the compromise was done intentionally by the National Security Agency. Ms. Dodson emphasized the importance that people trust NIST processes and standards, and in what NIST is doing today. Therefore, NIST decided to open up its public comment process and invite the community for feedback on the functions of the special publication, and specifically pointed to the function in question. In the meantime, NIST recommended public[24] not to use the function in question until the issue has been resolved. Ms. Dodson would like to seek the advice and guidance of the board as they move forward. Ms. Dodson would like to thank Ed Roback, Board member, for his support, input and providing historical background.

Mr. Roback added that there was a technical working group between NSA and NIST for creation of FISMA of 2002. It was required by law to maintain communication with NSA and having an NSA member on the ISPAB. As NIST developed standards and guidelines, NIST coordinated work being performed with US Department of Defense and Intelligence communities. The

[23] http://www.fiercegovernmentit.com/story/nsa-inserted-backdoor-nist-random-number-generator-method/2013-09-09
[24] http://www.fiercegovernmentit.com/story/nist-advises-against-use-random-bit-generator-algorithm-apparently-backdoor/2013-09-11

premise is to use NIST work as a baseline. NSA has a series of algorithms that were extracted from NIST toolkit which is the reason to reopen discussion of SP 800-90A[25] .

NIST has maintained open and transparent to public for its work and activities, such as cryptography and Cybersecurity Framework process. NIST works with standard development organizations and industry, and when NIST publishes papers/standards such as on FISMA or access controls which received thousands of comments. NIST has actively solicited people in the community and organizations and sought out experts either to gain their feedback or to recruit them.

Mr. Regenscheid led the discussion with focus on SP 800-90 Deterministic Random Bit Generators (DRBGs) and SP 800-90A Dual Elliptic Curve Deterministic Random Bit Generator (Dual EC DRBG). Mr. Kelsey, NIST cryptographer, provided a brief description of how cryptology works. He stated that in order to do cryptology, you must have Random Number Standards (RNS) and this is often something that people were getting wrong ten years ago and are still getting wrong now. The American Banking Group (ANSI-X9) tasked themselves to come up with standards for random number generation that roughly began in 1998. Mr. Kelsey stated that when he came on board at NIST in 2003, not a lot of progress had been made. There were ideas from documents like X9-17 and DSA, but no unified progress. This eventually became a U.S. Government effort and led to the creation of the X9 document that was published in four parts (one of the documents is still under administrative efforts with X9). When X9 is close to being finished, it is intended to publish these documents as NIST's Special Publications. This is because X9 documents are difficult to access it is not free, and in addition, these documents receive limited review. NIST decided to put together three documents (SP 800-90A, SP 800-90B, and SP 800-90C) that incorporated the X9 documents. The first publication is SP 800-90A: Deterministic Random Bit Generators. The idea behind DRBG is going to break down cryptography into two parts:

1. Unpredictable process – Achieved by configuring your electronics in an unpredictable way or interrupting your time, etc.
2. Then, feed it to the DRGB (the seed) which no attacker can guess. The DRGB takes this algorithm and turns it into a stream of bits that look random. You cannot tell this is actually not random without breaking some cryptographic code.

These are four algorithms in SP 800-90A:

- CTR-DRBG = block cipher based
- HMAC-DRBG = HMAC (hash function) based
- Hash-DRGB = hash function based
- Dual-EC-DRBG = elliptic curve based

Mr. Kelsey provided an extensive presentation on the process and working of Dual-EC-DRBG, there is an internal state to generate an output and, once generated, one would have to update the state after every state output. If you did not update the state after generation, one would always

[25] http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf

generate the same output. The security behind this operation is that the Elliptical Curve (EC) randomizes the data and does not allow one to go backwards in this process unless they solved the mathematical code that is encrypted in this process, which is really hard to do. We basically want to run this algorithm on a computer, but we want it to look like there is someone flipping a fair coin repeatedly and writing those numbers down (1s and 0s, see slide 6 in PPT). If the attacker can tell the difference between the two, then we lose. In addition, if the attacker can predict our outputs, then they can control our keys, which is extremely bad.

DRBG has two system parameters: P and Q. Ps and Qs are points on a curve. Mr. Kelsey explained the information is included in SP 800-90 and available to public. These standard parameters ultimately came from the designers of DRBG at NSA. An interesting question is *what if you don't trust the people that created Ps and Qs*. The thought is if the P and Q are randomly generated, they are Dual-EC-DRBG secure. If Ps and Qs are not randomly generated, it can create a trapdoor which means someone knows what the output of the algorithm seed is.

This was discussed in an X9 meeting and didn't seem to be a real threat at the time. In retrospect, a hash function should have generated and pulled so that there would be no way to use a trapdoor. If anyone is concerned with generated Ps and Qs parameters, there is a mechanism to create your own.

The news stories suggested that NIST intentionally allowed trapdoor to weaken the standard. NIST looked at these stories very seriously. NIST was aware of the trapdoor in the X9 documents, and that DRBG has constants; the security of the relationship is the math problem between the Ps and Qs. NIST does not know if NSA did anything with generating these algorithms. NIST is concerned with reassuring public so NIST eliminate the Dual EC DRBG from SP 800-90A. NIST have not received many comments/feedback from the community regarding this. Lessons learned include developing standards in an adversarial world as well as the concern that transitive trust is a big problem in the computer.

Mr. Regenscheid provided an overview of NIST Cryptographic program and standards development processes. It is important to NIST to have the community's trust and confident in NIST process. The first step is for the public to have a common understanding of how NIST develops its processes. NIST has three general processes for 1) develop processes through international competitions, 2) adoption of existing standards, and 3) development of the new standards.

Mr. Regenscheid asked the Board for feedback and recommendation on improvement of the process. The Board commended NIST for the process they currently use and they do not envision another process as open and conducive to the public, and most important, the current process seems to work. The trust issue that we see with the DRBG issue, curve, and SHA3 is that it is not about the normal process. There is an adversarial influence and there is only a small community that can address these adversarial issues, not the standards itself. Mr. Kelsey stated that the DRBG went through the ISO and X9 processes, and it would be interesting to understand what need to change. The Board commented that part of the process is relying on a large part of the community and perhaps there might be a way to provide video demonstrations that NIST can host to get the public thinking about the issues and the future. This would help educate the public.

Ms. Dodson said NIST has searched for ways and tools to educate people and to bridge the gap between technologists and the public. The educational videos do not have to be entirely about cryptography. NIST do plan to webcast workshops as they work under budget constraint; however, the past webcasts had very few attendees.

Mr. Kelsey gave a presentation on SHA3, describing a hash function. The standard size of collision resistance is 256-bit hash and128 bits resistance. Around 2004 due to new attacks and new insights into structures, there were new techniques and hash functions, which led to a competition modeled after the AES. The requirements for SHA3 were to have 128-bits and 256 pre-image resistances. A public competition was organized that included five public workshops. In 2012, a winner was selected – Keccak submitted an innovative solution called the sponge function. This capacity parameter allowed a tradeoff between performance and security. We are giving up a lot of performance to have more security. This is in order to have a fixed length hash function, and to allow users (cryptographers) not have to think about the properties.

Ms. Dodson explained that the requirements were set up front for the collision and pre-image resistances. No other security feature of the hash has a higher security at NIST. Some comments about SHA3 seemed to show that it was not clear people really understood the environment. Also, any change you make after the competition is not good and will generates comments. There are areas where NIST have a lot of work but do not have the resources. Ms. Dodson explained that if there is an area that they are particularly interested in or have personal contacts, they are always looking to broaden their pool and to increase the department competitiveness. With regards to International Cryptography Regulations (ICR), NIST did participate only in euro-crypto workshops.

Mr. Moody presented on NIST Curves. When Elliptical Curve Cryptography was proposed in 1985, NIST recommended 15 curves that could be used. There was a lot of research over the years and the concerns were in two areas: efficiency and security. A greater concern is that there a hidden weakness. The curves were chosen with ten pseudo and random, and another five special curves. NIST developed the pseudo curves. Random curves do not have special curves. Special curves do not allow you to select your curve. In theory, someone could generate a lot of curves and pick the one that has a weakness too. NIST worked closely with and received the curves from NSA, but there is no specific documentation to detail how those curves were developed. There are known security attacks on NIST curves.

The Board suggested that NIST to consider new curves for performance. Also, NIST panel to address the selection process and that it was insufficiently documented. The Board commented that there are gaps in the process even though it might seem that people are not confused about the process. NIST believes there does need to be an adjustment in the decision, communication, and durability of the process, so it is about the details being communicated not necessarily the process. Developing standards and communicating NIST standards to the public are both equally important, and NIST is considering writing up a draft to provide to the public. The Board cautioned that this draft could be misunderstood, and how it will be used. The Board also asked NIST to be careful using this draft on existing publications.

Additional suggestions from the Board:

- Encourage NIST to draft a written record of community concerns and engage the community to raise the concern
- Reflect on document and public concerns and incorporate a statement such as "this is how we do it now"
- Discuss NIST's workshops and other ways to get engaged with stakeholders
- Be clear about NIST's principles, not standards, and that the process upholds your principles
- Before addressing and distributing to the public, wait until the process and gaps are addressed

Ms. Dodson explained that NIST strives to make our standards as practical as possible and believe in open transparency, not only for cryptography but for all areas. However, since cryptography is in question, NIST is focusing on that first. The Board mentioned that they could get some people together to make some additional recommendations to NIST, perhaps a sub-set of ISPAB.

Public Participation

No request was received.

Regulatory updates of Embedded Software Security

Kevin Fu, (Moderator, participated via teleconference), Associate Professor, EECS Department, The University of Michigan
Brian Fitzgerald, Deputy Director, Division of Electrical and Software Engineering, FDA CDRH OSEL

Dr. Fu joined us via telephone as the moderator and introduced the presenter, Mr. Fitzgerald. Mr. Fitzgerald who had previously presented on this topic, will be providing an update on embedded software security, specifically relates to medical devices. FDA issued some cybersecurity guidance for manufactures. Dr. Fu emphasized that this is the first document he is aware of that addresses cybersecurity integrated not just into the implementation of a medical device but also in the design phases of the device and risk management. Mr. Fitzgerald confirmed that they have published draft guidance[26] on medical devices since the last time he presented to the Board. Since this is considered a guidance document, there are more dynamic capabilities of adding or changing guidelines. In this guidance document, there are several steps of guidance that are being addressed in the design cycle of medical devices, through external and internal steps. For example, one of the first external steps is to assist manufactures with knowing FDA's expectation. It is mainly addressed to the premarket medical device industry. The FDA does see a select portion of the premarket medical devices but, not all, and only if vulnerabilities

[26] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm356186.htm;

have been identified. The premarket industry tends to notify the FDA for guidance when vulnerabilities are found. The medical device companies that do not come to the FDA for guidance can still follow our guidelines and understand the expectations being addressed. Mr. Fitzgerald stated that this is FDA's initial step for publishing this guidance document specifically for medical device manufacturers to gain awareness of the guidelines and expectations moving forward in designing a medical device that also addresses cyber vulnerability mitigation. This publication is still in progress but is the foundation of the guidance document.

Mr. Fitzgerald continued, by addressing the way FDA views the cybersecurity community. For example, the FDA has had some interface with other agencies but up until this point not much related to cybersecurity. Mr. Fitzgerald stated that his department within FDA reached out to the U.S. CERT to assist with building processes, but they seemed more interested in the IT-related risks whereas FDA focus is more on the clinical risk management. Mr. Fitzgerald indicated that it seemed that U.S. CERT was wary of the patient clinical risks posed by cybersecurity. As the FDA moves forward with publishing the guidance document, they would also like to expand their cyber community outreach.

One of their major accomplishments in drafting the guidance document was identifying internal processes related to medical devices. They used functions like record, recall and correct to see if they translated into cybersecurity for medical devices. For example, the FDA's document 883 references that a manufacturer, medical device or a user must report an incident if there is an adversarial incident. The FDA has always thought of this occurrence as a clinical incident instead of cybersecurity. Also, not every incident is considered a clinical incident. Mr. Fitzgerald explained that the FDA would like to craft a post-market approach so that they can understand how these cyber events fit into what they have traditionally managed as design phases and reportable incidents. Their goal is not to force every cybersecurity vulnerability requirement nor do they want every cyber event to be considered a reportable incident. FDA would like to achieve a careful balance of the two.

The plan is to have a 1- to 3-year rollout plan. Medical device regulators are more aggressive than others and some are contracted out to third parties. Those third parties were contracted long before this became an article. Post-market guidance[27] will be released in October 2014.

National Infrastructure Protection Plan - EO 13636 Improving Critical Infrastructure Cybersecurity

Robert Kolasky, US Department of Homeland Security
Jenny Menna, Director, Stakeholder Engagement and Cyber Infrastructure Resilience Division, US Department of Homeland Security

Mr. Kolasky stated that the National Cybersecurity Services staff was asked to update the National Infrastructure Protection Plan[28] (NIPP), which was due to be released that day. The

27 http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

2828 https://www.dhs.gov/national-infrastructure-protection-plan

fundamental plan is how DHS will execute the policy that is laid out in Presidential Policy Directive 21[29]. The plan is a basic concept risk management plan for public private partnership to make progress with cybersecurity critical infrastructure. The NIPP is largely known to have a lot of collaboration between public and industry. NIPP is trying to bring in partners to share information as well as R&D, understanding previous NIPPs were built on security resilience. There are structures at the sector levels and cross-sector levels. There are five goals and seven core tenets (which include infrastructure, information sharing, trusted relationships, mitigate and management consequences, sector partnerships, international relationships, standard processes). Finally, the NIPP lays out twelve calls to action (which include set joint national priorities for security, state and local planning, thinking account incentives, information sharing front, response and recovery for owners and users, recovery framework, updates how we are going to measure). Working with NIST Cybersecurity Framework, restructuring the NIPP was very helpful. DHS circulated three drafts of the NIPP under the federal register notice.

DHS also leveraged partnerships and supported the adoption of the Framework. The Cybersecurity Framework gives DHS the opportunity to take the program and promote cyber resilience through 800-53. Ms. Menna stated that the voluntary program to advance adoption of the Cybersecurity Framework is through outreach and leveraging partnership relationships with other agencies. DHS would also like to reach out to engage the insurance companies and audit communities to small, medium, or large business. The Framework and the Voluntary Program gives DHS a chance to focus on the programs currently held and refresh them. DHS would often point to 800-53 and now DHS can point to the Framework. DHS also wants to look at programs that were designed for Federal civilian and government practices for industry partners.

Board Discussion

Action items:

The Board suggested that a letter[30] be submitted to the Office of Management and Budget and the NIST Director commending the NIST Computer Security Division staff on their excellent processes and procedures in developing the Cybersecurity Framework. A vote was initiated and the motion was passed that a letter would be drafted up and recirculated to the Board members for final approval.

The Board also commended NIST for their historical involvement and community outreach in cryptography and recommended sending another letter[31] recognizing NIST cryptographic standards. Key points to mention would be:

1. Recognize and compliment NIST cryptography expertise to develop in the private sector

[29] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[30] http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab_ltr_on_cybersec-framework_jan2014.pdf

[31] http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab_ltr_on_crypto-stds-process_jan2014.pdf

2. Recognize the process at arriving and updating those standards and ongoing efforts
3. Encourage NIST to continue to partner with academic and public stakeholders and industry and international

The Board motioned to approve both letters as discussed above and the motion was passed unanimously. The letters will be drafted and circulated to all Board members for review. Board members will have to vote and approve the final drafts before they are sent out.

The Board's next action item was approving the June 2013 meeting minutes. A motion was proposed to approve the minutes. The motion was approved unanimously.

Annie Sokol, Designated Federal Officer, updated the Board on the following:

1. Charter renewal for 2014-16
   Annie Sokol is in the process of working with NIST legal to finalize the documents for submission to US Department of Commerce. The proposed charter 2014-2016 includes a new role of vice chairperson. The current charter expires March 9, 2014. If and when the charter is approved with added text for vice chairperson, a vice chairperson can be appointed.

2. The Board agreed to have the following three meetings in 2014:
   a. March 12, 13, and 14
   b. June 11, 12, and 13
   c. October 22, 23, and 24

   Annie Sokol will look for room availabilities based on those dates.

3. Annie Sokol provided to the Board the latest Annual Report for NIST Computer Security Division. During the meeting, pictures were taken of ISPAB for inclusion for the following year NIST CSD Annual Report.

4. The Board agreed on the following list of topics/activities for 2014-2015. The list will be used to update ISPAB Activities http://csrc.nist.gov/groups/SMA/ispab/activities.html:

   - Updates from the Executive Office
   - Updates on OMB A130
   - Data Report information for unsupported software
   - Cybersecurity Framework regarding technical transfer and implementation/adoption and sector-specific agencies focusing on CIPPS
   - PCLOB (including more information on the annual report PCLOB)
   - NIST Updates on basic cryptographic properties transition and new crypto work
   - Embedded software security information
   - Medical devices and relating challenges such as security
   - Status on protecting the federal Einstein Program - TIC is a goal
   - Use of the Framework for procurement for DOD requirements on supply chain
   - FISMA and FISMA report

- CAP GOAL status 15-16 along with the metrics (pull report)
- Information Sharing/FBI – Follow-up
- Updates from federal agencies re. implementing Appendix J / 800-53 (privacy section)
- DHS CVM Program integration services follow-up
- FEDRAMP briefing
- NSA, DHS to talk about privacy
- General legislative updates

The meeting adjourned at 4:10 P.M., Friday, December 20, 2013.

Annex A

LAST	FIRST	AFFILIATION	
Ayiotis	Christina	GWU	Visitor
Barker	Elaine	NIST	Visitor
Beauchamp	Brian	Booz Allen Hamilton	Visitor
Boyens	Jon	NIST	Presenter
Burch	Ashley	Advanced Government Solutions (AGS), Inc.	Visitor
Carnahan	Lisa	NIST	Visitor/Presenter
Chen	Lily	NIST	Presenter
Chenok	Dan	IBM	Visitor
Cooper	Michael	NIST	Visitor/Presenter
Cressey	Roger	Liberty Group Ventures	Visitor
Cuello	Veronica	eGlobalTech	Visitor
Curran	John	Telecom Reports	Visitor/ Media
Dodson	Donna	NIST	Presenter/Staff
Dworkin	Morris	NIST	Visitor/Presenter
Fitzgerald	Brian	FDA	Presenter
Hogan	Mike	NIST	Visitor
Huergo	Jennifer	NIST (PBA)	Visitor
Jones	William	FBI	Presenter
Kelsey	John	NIST	Visitor/Presenter
Kolasky	Robert	DHS	Presenter
Lefkovitz	Naomi	NIST	Presenter
Marshall-Johnson	Gina	The Johns Hopkins University Applied Physics Laboratory	Visitor
Medine	David	PCLOB	Presenter
Menna	Jenny	DHS	Presenter
Michalek	John Conor	Liberty Group Ventures	Visitor
Mitchell	Charlie	InsideCybersecurity	Visitor /Media
Moody	Dustin	NIST	Presenter

LAST	FIRST	AFFILIATION	
Nelson	Michael	Microsoft	Visitor
Newhouse	William D.	NIST	Visitor
Ozment	Andy	The White House	Presenter
Pillitteri	Victoria	NIST	Presenter
Polk	Tim	The White House	Visitor
Qian	Michael	DHS	Visitor
Regenscheid	Andrew	NIST	Presenter
Rogers	Susan	Yale	Visitor
Royster	Kristin	Global Information Security	Visitor
Scanlon	Jonathan	Booz Allen Hamilton	Visitor
Scholl	Matt	NIST	Presenter/Staff
Schwartz	Ari	The White House	Visitor
Scurlock	Antonio	DHS	Presenter
Sedgewick	Adam	NIST	Presenter
Sepeta	Arthur	US DHS	Visitor
Sharpe	Emily	Facebook	Visitor
Smith	Matthew	G2-Inc.	Visitor
Smith	Phil	Trustwave Federal Solutions	Visitor
Smith	Michael	CCSi	Visitor
Stine	Kevin	NIST	Presenter
Suh	Paul	Booz Allen Hamilton	Visitor
Taylor Moore	Debbie	CyberZephyr	Visitor
Todt	Kiersten	liberty group ventures	Visitor
Toler	Danny	DHS	Visitor
Weber	Rick	InsideCybersecurity	Visitor /Media
Withnell	Elizabeth	Advanced Government Solutions, Inc.	Visitor
Williams	Timothy	RSI	Visitor