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

October 22, 23 and 24, 2014

U.S. Access Board, 1331 F Street N.W. Suite 800, Washington, DC, 20004, (202) 898-4000
http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-10/october-2014.html

	Present	
Wednesday, October 22, 2014 8:38 A.M. – 5:23 P.M. Thursday, October 23, 2014 8:32 A.M. – 4:23 P.M. Friday, October 24, 2014 8:04 A.M. – 12:30 P.M.	**Board Members**	
	Present Matthew Thomlinson (Chair), Microsoft Chris Boyer, AT&T John R. Centafont, NSA Dave Cullinane, Security Starfish. LLC Kevin Fu, University of Michigan Greg Garcia, FSSCC Toby Levin (Retired) Edward Roback, US Department of Treasury Gale Stone, Social Security Administration Peter Weinberger, Google, Inc.	Board Secretariat and NIST staff Matt Scholl, DFO, NIST Annie Sokol, DFO, NIST Tatiana Laszczak, Exeter Government Services, LLC See Annex A for list of attendees

Wednesday, October 22, 2014

Welcome and Remarks
Matt Thomlinson, Chairman, ISPAB
Vice President, Microsoft Security

The ISPAB Chair, Matt Thomlinson, called the meeting to order at 8:38 A.M. He welcomed back the board members and asked them to provide a brief update of their activities since the last meeting.

The Chair announced to the board that due to his increased job responsibilities and requirements that he will be stepping down from being Chair and regrettably this will be his last board meeting.

The Chair began the first day's meeting by providing an overview of the agenda and introduced the first presenter.

Privacy and Civil Liberties Oversight Board (PCLOB) Updates

Report on the Surveillance Program Operated Pursuant to Section 702[1] of the Foreign Intelligence Surveillance Act
David Medine, Chairman, Privacy and Civil Liberties Oversight Board (PCLOB)

The Chair welcomed back Mr. David Medine, Chairman of the Privacy and Civil Liberties Oversight Board (PCLOB) to the board to discuss the Foreign Intelligence Surveillance Act (FISA) 702[i] program report on surveillance findings. Mr. Medine thanked the board for inviting him back and began his opening remarks by providing a brief background of the cause of report analysis of Section 215 Access to records and other items under the Foreign Intelligence Surveillance Act and Section 702. Mr. Medine stated in 2013 after the Snowden case regarding the initial leaks of Section 215 and Section 702 programs the PCLOB was commissioned by 13 Senators to conduct a study of both programs. Mr. Medine said that there were differences with the two programs; for instance, the 215 Metadata program, at the time, had already had a significant amount of leaks. Because of this, it was not difficult for the board to release an unclassified report to the public. In contrast, the 702 program was heavily classified which caused greater challenges for the PCLOB to release a report due to the highly classified nature of the program. However, the PCLOB was successful in identifying 100 facts about the program and were able to get the facts declassified to include in their report. In general, the 702 program consists of the National Security Agency (NSA) PRISM surveillance program that surveys:

1) Contents of email communications from various email providers.
2) Upstream communications such as tapping into live telecommunications and internet to obtain the contents.

Mr. Medine explained that the metadata 215 program focuses more on the number of occurrences a phone number is called, what time of day verses the actual content that the 702 program captures. In order for the government to utilize the 702 program to target and obtain content communications the following criteria must be met:

1) The person targeted must be a non-US citizen.
2) That person must not be in the US.
3) There has to be Foreign Intelligence value to the information.

The PCLOB analysis found that in order to target a person there has to be a 51% of certainty that the person is in fact a non-US citizen. The PCLOB worked closely with the Intelligence Community and concluded that it is difficult to determine with 100% accuracy that a candidate individual is a non-US citizen. Mr. Medine provided an example of a person who may be using VPN access from another country, and due to the IP address masking function of VPN – can look to be initiating internet traffic from within the United States. Mr. Medine continued by saying that a lot of rigor was put in to determine whether the person was a US or non-US citizen. After the PCLOB's evaluation, it was found that in 1% of cases the NSA was incorrect. Mr. Medine said that a lot of information is collected that is relevant to the counter terrorism mission; however, there is information that is not such as a non-US citizen communicating with an American that could be family. The government does have minimizing processes in place to remove non-counter terrorist communications; however, the report found that information is rarely deleted. The PCLOB report recommends that the 702 program should provide more efforts to the minimization process and delete irrelevant information when possible.

[1] The FISA Amendments Act of 2008 (also called the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, H.R. 6304, enacted 2008-07-10) is an Act of Congress that amended the Foreign Intelligence Surveillance Act

The PCLOB provided a three part analysis in their report addressing the following areas:

- Is it legal
- Is it constitutional and,
- Does it strike the right balance between privacy, civil liberties and national security

The PCLOB's oversight functions examine the legal compliance of government programs. In their analysis, they found that the 215 report was not legally authorized and should be discontinued. The Section 702 program was fully authorized. However, at the constitutional level, there is an application of the 4th Amendment that questions whether there is an exception to collecting Americans information in searching, collection, and using that information. There is a foreign intelligence exception for national security matters that has never been ruled on at the Supreme Court level and no cases in the Section 702 program context exist. Mr. Medine stated that this is an open question right now whether there is a foreign intelligence exception that would not require a warrant for information collected. The Section 702 program operates under the exception of foreign intelligence communication no warrant is needed. The PCLOB felt the assessment of the Section 702 program was right up to the line of constitutionality and called for added legal protections in searching US citizen communications. The PCLOB felt when searching a US citizen communications should require court approval.

Another question arose during this report questioning whether non-US people rights were being violated. The United States government states there is no territorial obligation to non-US persons; however, the board decided to defer this question to President Policy Directive (PPD) 28[2] that President Obama released January 2014 regarding *how intelligence forums address foreign individuals.* President Obama asked the board to oversee PPD 28 and use PPD 28 to address *what can be done to effect non-US people's rights*.

Mr. Medine concluded the PCLOB's assessment addressing policy issues with the 215 and 702 program. Since there were overall privacy issues and concerns on civil liberties, the PCLOB concluded that the 215 program was not effective in thwarting terrorists' efforts and added no unique value. In contrast, the PCLOB found the 702 program to have concrete evidence of terrorists efforts thwarted off and provided input into government decision making as well as supported counter terrorism. The PCLOB felt the 702 program did offer value and should go forward even though there were significant privacy concerns. The PCLOB recommended the following changes:

- Collecting foreign intelligence value; the PCLOB did not see rigor in the documentation collected and would like the process to be enhanced and reasons to why events occurred.

- There is some disconnect in the FISA court in what they thought were approving and what it actually was. There is not a way to follow-up. The PCLOB recommends a process to check via by sampling and querying the database. This would allow courts to check decisions and follow-up and ask questions if necessary.

[2] PRESIDENTIAL POLICY DIRECTIVE/PPD-28 Signal Intelligence Activities http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

- Recommend greater transparency in minimization and retention procedures that require the government to issue declassified procedures

As Mr. Medine, concluded his presentation, he said the next report assessment will be focused on the Executive Order 12333--United States intelligence activities[3].

Continuous Diagnostics and Mitigation (CDM) [4]- Phases of CDM and FedRAMP Baseline Security Controls
John Streufert, Director, Federal Network Resilience, U.S. Department of Homeland Security, National Protection & Programs Directorate

The Chair introduced and welcomed back Mr. John Streufert, and in response, Mr. Streufert thanked the board for inviting him back to speak. His opening remarks referenced two documents authored by *Franklin Reeder* on *Updating U.S. Federal Cybersecurity Policy and Guidance*[5] as well as a summary on the Threat to Cyber Infrastructure. These documents explain the importance of the urgency to invest widely in protecting against National Cyber threats and emphasizes that our defenses are not equal to threats and threats are constantly changing.

Mr. Streufert remarked that since the Office of Management and Budget (OMB) M-14-03[6] Enhancing the Security of Federal Information and Information Systems has been adopted; the CDM program has increased through agencies, and CDM uses it as a tool to augment the court capabilities on FISMA. Mr. Streufert offered the following Cybersecurity risk statistics (*Raising the Bar for Cybersecurity*[7]*, CSIS report dated February 12, 2013 by James A. Lewis included the following statistics*):

- 75% of cyber-attacks are known vulnerabilities
- 98% of cyber-attacks that are successful require only the most basic of techniques
- 96% of cyber-attack breaches that are successful can be avoided by simple or intermediate controls.

The OMB M-14-03 mandates that all government agencies have an operational federal policy. This provides near-to-real time results to fix the worst vulnerabilities and accelerate defense mechanisms that are relevant to cyber-attacks which will enable vendors to identify and mitigate laws closer to network speed.

The current CDM[8] program has been utilized by 98% of the civilian government agencies which have signed formal memorandum agreements and/or are in the process of signing an agreement in response to the OMB M-14-03. Since 2009 and on, the CDM contract award for civilian agencies resulted in a 30% reduction off of the GSA schedule and budget avoidance of $26M from GSA. The goal was to support those agencies that did not have a CDM procedure in place. For the agencies that did not have a process in place, the CDM program offered a good starting point. Some other agencies had a widely divergent

[3] http://www.archives.gov/federal-register/codification/executive-order/12333.html
[4] https://www.dhs.gov/blog/2013/08/13/major-step-forward-better-protecting-federal-state-and-local-cyber-networks
[5] http://csis.org/files/publication/121019_Reeder_A130_Web.pdf
[6] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf
[7] http://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf
[8] http://www.dhs.gov/cdm#

process approach. In comparing the agencies approaches there was a need to have standardization. When planning for the CDM program, the contract intentionally supported the federal government model of shared services such as cloud services. From the very beginning, contract was kept open so as to allow FedRAMP to provision CDM tools off the contract.

In response to the Board's question on CDM phases[9] and their status, Mr. Streufert described the four phases: Asset Management, Whitelisting, Vulnerability Configuration settings and Compliance. He emphasized that he and his team have their eyes on Phase 2 of the CDM program which focuses on managing privileges and perimeters for a common insider threats approach to incidents. An RFI was released in April 2014 and updated in July 2014[10]. Based on the RFI response, a draft Statement of Work (SOW) will be prepared which will also be provided to the executive branch to solicit questions before releasing it. Phase 3 (scheduled to occur after Phase 2), will focus on managing events that will match and coordinate with activities in the EINSTEIN program where intrusion detection occurs. Phase 4, will focus on putting sensors out to 4 million devices using SA FEDSIM as a source. There have been no awards for the dashboard CDM initiative process. The purpose of this process was for GSA to gather sensor input and 124 subcomponents of <dot>*gov* sensors that will use commercial off-the-self (COTS) packages to maintain data on a local level. This will support worst vulnerabilities reported first at the civilian agency. At the federal level, a summary of civilian agency information will provide an enterprise risk picture and awareness on the readiness of departments and agencies of emerging threats.

Mr. Streufert mentioned that the US Department of Homeland Security (DHS) worked closely with the FedRAMP program to establish a low baseline on asset controls which was represented from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4[11]. The discussion on security control or control enhancements on low, moderate, and high baselines are presented in Appendices F and G of SP 800-53 Rev. 4. CDM included 20 controls from SP 800-53 and 46 non-selected controls in deliberation with the Joint Advisory Board (JAB) from FedRAMP. In the effort to establish a high baseline for special cases is being coordinated between DHS National Protection and Programs Directorate[12] and FedRAMP. Projected activities for establishing the high baseline would be in 2015.

DHS is taking steps to analyze NIST's Framework for Improving Critical Infrastructure Cybersecurity v1.0[13], published February 12, 2014, regarding the emerging activity and conversion related to Executive Order 16636 (Improving Critical Infrastructure). Currently the OMB M-14-03[14] *Enhancing the Security of Federal Information and Information Systems* and the NIST Framework are complementary of one another.

The CDM staff is intently watching the deliberations of DHS and cybersecurity hiring authorities. The CDM program would like to offer training needs for cybersecurity that will assist with assembling a recruitment and retention effort appropriate under OPM. This will allow government personnel to man their cybersecurity departments internally and receive proper training that will support continuity in an agency. The training effort is based on the outcome of the deliberations.

[9] http://www.dhs.gov/cdm-implementation
[10] https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=4758aa0a7a98466b9d11d862e858993b
[11] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[12] http://www.dhs.gov/about-national-protection-and-programs-directorate
[13] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
[14] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

Looking to the future, the Leap-Ahead[15] program is one in which DHS has partnered with a support organization to have a location that will provide developments of technologies that could be reviewed in a systematic way. The intent would be to apply the results and findings in a new CDM service contract which would allow vendors to be aware of emerging new technologies while also monitoring updates of existing software and previously adopted. DHS is also beginning to review a program called Dedicated Systems Reliance[16]. The scope of this program is focused on networks across federal agencies that require cybersecurity protection. Lastly, Mr. Streufert, stated that in FY17 DHS would like to create a program office to establish classes for CDM customer training focusing on protecting software, hardware, websites, databases etc.

The Board inquired that given the way threats evolve, are we gaining or falling behind on threats?
Mr. Streufert commented that the previously known threats where there are no flaws particularly in the core capabilities there has been steady progress. As well as the government agencies that have committed to CDM memorandum agreements. In terms of zero days, the newspapers suggest, that the problems are not small and decreasing but increasing. Threats will continue to increase but having companies invest in cybersecurity and risk management will help. All the companies that have come under attack should consider CDM. Mr. Streufert remarked that the pace of urgency is getting it fully implemented.

FedRAMP Updates

Matt Goodrich, Acting Director, FedRAMP, Federal Cloud Computing Initiatives, GSA (PPT Slides provided)

Mr. Matt Goodrich began by providing an overall statistics of the FedRAMP[17] program and agency involvement.

The numbers in each area of authorization and processes are anticipated to double in the next month. Mr. Goodrich said the FedRAMP program has been operational for two years; however, there has been a bit of a grace period for agencies to become FedRAMP compliant which has been slightly stretched. As of June 2014 agencies are reporting 40% compliant although based on information obtained by the FedRAMP PMO realistically assesses the agencies at more of 25%. In terms of the PMO use, 22 out of the 24 Chief Financial Officer (CFO) Act agencies are using the security assessment packages. The review process consists of over 500 active reviewers at the agencies. Mr. Goodrich mentioned there have been 50 other government entities that are interested in the FedRAMP program; however, the PMO only supports government agencies at the federal level not state or local government since they do not qualify for Federal Information Security Management Act (FISMA) reporting. The authorization cost is about a quarter to a million dollars based on the 2012 FISMA reporting which was the last time a cost breakout has been done on the program.

[15] http://www.dhs.gov/csd-leap-ahead

[16] http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf ; The White House, Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, accessed September 24, 2013

[17] http://cloud.cio.gov/fedramp

Mr. Goodrich said the PMO is working on 500 contracts which is a conservative number although it is believed to be more across the government. *The board inquired how the PMO measures the number of contracts FedRAMP touches.* Mr. Goodrich said that every time a Cloud Service Provider (CSP) is authorized "their success is our success" our PMO office reaches out to the providers' customers to give them information on the FedRAMP program "on what it is" and "how it can be leveraged" which provides insight into the number of contracts reported. The FedRAMP PMO office said they can typically work with 10 – 12 CSPs consecutively; however, they are currently 50% over capacity. Mr. Goodrich mentioned that despite their extended resources the PMO office continues to work actively with the CSPs to earn ATO as quickly and effectively as possible. Foremost, to assist the current CSPs in process and to assist with the supply and demand need of other CSPs waiting in line for authorization.

As of late October, the FedRAMP PMO office released a new program known as FedRAMP Ready[18] Systems. This program is listed on the cloud.cio.gov website as a way "for potential agency customers and authorizing officials a starting point to initiate an authorization". Mr. Goodrich explained in order to be FedRAMP Ready, at a minimum the PMO office requires the potential CSP to go through the FedRAMP Readiness Review. The initial review, at the PMO level, consists of a documentation review of the providers System Security Plan, Incident Response Plan, Configuration Management Plan, Contingency Plan, and any documentation referencing policies and procedures. As the next initial review step, the potential CSP goes through a completeness check to ensure all boxes in the forms are filled out properly. *The board asked how large the documents being reviewed are.* Usually, Mr. Goodrich stated, the documentation provided is between 800 – 1000+ pages on average. He went on to say that the FedRAMP template is about 400 pages but to keep in mind that the template covers all security control from NIST publications as a courtesy to have everything in one document. The PMO office ensures that all boxes within the forms have been filled out properly. If they pass, the PMO reviewers will send the potential CSP's System Security Plan to the FedRAMP PMO. The role of the JAB is to perform a holistic review of 15 – 25 security controls at a minimum and, should they pass are considered FedRAMP Ready. The benefit of the FedRAMP Ready program will allow a faster authorizations process for both JAB and CSPs.

Mr. Goodrich outlined benefits agencies could use to leverage the use of open source. He explained that since open source is "open to all", the security implementation documentation typically required within agencies is no longer considered proprietary and therefore not needed. The FedRAMP PMO office is working on providing open source code documentation on "how to implement open source" for government agencies use. *The board inquired who would be providing and validating the government open source code.* Mr. Goodrich stated that the open source code would be validated through another government entity accompanying a government level review before published.

Mr. Goodrich provided an update of the Third-Party Assessor Organization (3PAO) in that it is privatized and currently has 31 organizations mostly consisting of small businesses. The FedRAMP PMO office owns the list of accreditation and can remove an organization from the list if inefficiencies are found. Mr. Goodrich noted that no organization has needed to be removed to date.

Also, based on the recent NIST SP 800-53- Rev 3 & 4 updates related to security controls; the FedRAMP PMO updated their documents to incorporate the adjustments. Mr. Goodrich also mentioned that the NIST Appendix J regarding privacy controls is also part of the FedRAMP baseline.

[18] http://cloud.cio.gov/site-page/fedramp-ready-systems

Mr. Goodrich provided the board with a 2 year road map[19] of where FedRAMP will be applying their resources and energy. The FedRAMP PMO would like to maintain transparency when possible with their partners and agencies. The PMO office would like to increase FedRAMP program awareness and increase agencies that are actively engaged in the process. *The board asked why the FedRAMP mandatory due date has not been followed.* Mr. Goodrich explained that there is not enough money to meet every IT policy that OMB releases; however, if an agency cannot meet the mandatory deadline required by OMB, then they must provide detailed documentation that demonstrates why they cannot and a course of action to correct it.

Mr. Goodrich said the FedRAMP PMO office would like to increase training and education of the FedRAMP Program and process. The PMO office will be redoing their website and rebranding to a <dot>.gov. The PMO office is planning to finalize and release their goals mid-November 2014.

Mobile Devices and Protection of Sensitive Information

Michael Cassidy, Cyber Security Architect, Information Technology Security Staff (ITSS) Justice
Management Division (JMD), US Department of Justice
Tom Karygiannis, Senior Computer Scientist, Computer Security Division, NIST
Troy Lange, Chief, Systems & Technologies Analysis, NSA (PPT provided)
Gregory F. Youst, DISA Chief Mobility Engineer, CTO (PPT provided)

Mr. Troy Lange, Chief of Systems and Technologies Analysis from the National Security Agency (NSA) provided a security overview of how NSA addressed technologies that evolved into the mobile device discussions of "why mobility". Mr. Lange mentioned that in the past when technology issues were identified, NSA primarily used crypto resources to solve their technology problems or when there was a need for a device, they worked with industry to build it. Mr. Lange provided an example of his office authorizing the build for a "Secure Mobile Device" with security functions that met NSA requirements. Once built, NSA would perform a security evaluation (including testing); however, 3 or 4 years later the mobile device is complete but obsolete to emerging new technologies.

Mr. Lange emphasized, "How do we keep pace with new technologies when the government has no control, design, manufacture and package over it". The question discussed is whether there is a way to build a system to protect information sharing and use parts/devices that may not be completely trustworthy. Mr. Lange said this concept coined our commercial strategy for classified solutions program. In theory, this would involve a higher liability system that would compensate if a device or part failed. The security element would be added to the system so if vulnerability occurs that is unknown it is mitigated by having another device or part that performs the same function. Although there has to be some confidence in devices, Mr. Lange, referenced using the Common Criteria Protection Profile for assistance in testing security requirements for devices (Samsung for example is currently being tested). Mr. Lange said the system would be independent from the mobile device and capability package and there are still mitigation risks that are known. For example, if classified information is stored on mobile devices when a person accepts the device our risk assessment may only protect data up to 15 years. There is a balance between opportunity risk and the risk that the end-user accepts. For example, taking a classified call on your mobile device in public where another person can overhear versus losing your

[19] http://cloud.cio.gov/sites/default/files/documents/files/FedRAMP%20Forward%202%20Year%20Priorities.pdf

device. Mr. Lange and his colleagues at NSA are discussing the idea of embracing Cloud Services. This concept supports removing as much data as possible on the device and pushing it to the Cloud enterprise. *The board asked who creates the capability packages*. Mr. Lange said they are developed internally by NSA protection profiles[20]. *The board asked about over the air updates in this context.* Mr. Lange said there is still a lot of ongoing discussion.

Mr. Youst, Chief Mobility Engineer from DISA (Defense Information Systems Agency[21]), began his presentation by outlining the US Department of Defense (DoD) Mobility Vision Enterprise. The program consists of joint information datacenters that are in the process of being consolidated and collapsing the 8 current layers to 4. DISA is looking to simplify their networks while still maintaining a secure network and "on the edge" mobile device data. Mr. Youst highlighted that DISA is headed towards a Cloud infrastructure that has the potential to become a consolidated enterprise. There are three key areas and strategies DISA is focused on as outlined in the presentation provided a rollout plan of the (PPT slide page 4):

- Information Enterprise Infrastructure to support mobile devices
- Mobile device policies and standards
- Promoting the development of DoD Mobile and Web-Enabled Applications

According to the projected timelines, DISA in FY17 would like to be able to routinely serve DoD on a wireless network. In Mr. Youst's opinion Government has to move at the speed of technology. There are not a lot of agencies that have government Wi-Fi so Mr. Youst said, "we have to trust the carriers". However when taking the proper security precautions and setting up controls, on the phone, data in transit and accessing the network should all be in place. DISA would like the wireless capability to be at the unclassified level as well as classified (TS and TS SCI levels[22]). DISA is waiting for guidance from NSA on what levels can be implemented. Furthermore, DISA is looking for mobile device provisions to be more scalable. Currently, the process needs to improve with only 500 mobile devices approved for classified use[23], and there is an estimated need of 25K mobile devices needed to be provisioned. DISA is working with Public Key Infrastructure (PKI) to increase the provisioning efforts.

The next steps are moving to a cloud environment. Some challenges will be to have better asset controls if mobile devices will be located in all parts of the world. Mr. Youst said improved information access will need to be determined based on location and "what one needs to do their job" while making the information available in real time and the key should be able to reach back to get the information securely. Another thought that need to ponder is what impact do you have on cloud and the impact of cloud have on us. There are a lot of challenges with mobility devices that DISA is analyzing to protect and secure data that will need to be addressed before building a cloud infrastructure.

DISA is anticipating the release of the final publication of NIST 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credential[24] as DISA is exploring development of an over-the-air provisioning system using PKI and/or Derived Credentials.

[20] https://www.nsa.gov/ia/business_research/partnerships_with_industry/niap_and_cots_product_evaluations.shtmlc
[21] http://www.disa.mil/
[22] http://en.wikipedia.org/wiki/List_of_U.S._security_clearance_terms
[23] http://fcw.com/Articles/2014/10/22/DISA-classified-mobile-phone.aspx
[24] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf; http://csrc.nist.gov/publications/nistbul/itlbul2014_12.pdf

Mr. Youst presented challenges based on tactical environment considerations to using mobile devices such as when sever terrain and environments do not allow traditional battery charging of devices or service. Mobile devices may have to evolve in some cases and allow solar energy to charge mobile devices, and a number of vendors will be offering phones that will remain operational when dropped in water. It is important to deal with authentication on-the-edge and non-traditional operational environments.

Mr. Cassidy, Cyber Security Architect from the US Department of Justice (DOJ), said his main focus has been on commercial mobile applications and security. He and his office have developed internal government applications for procurement and other internal services or programs. He emphasized that the current commercial mobile applications are projected to fail basic security requirements. The reason behind this is that application providers are more concerned with bugs and defects than investing in security settings. Most enterprises are inexperienced in mobile application security and tend to be done casually by developers mostly looking for defects. From a security stand point, applications face challenges in the following areas:

- Mobile Device Platforms – Do not support platforms such as Apple, Android, Blackberry etc.
- Mobile Application Data Tools – These are highly recommended. Before selecting a tool, review a pilot program. Even if the tools architecture looks good often times the tool does not function the way it was intended or the overall tool quality could be lacking during the testing phases.
- Out of 250 applications that were embedded, 10% required a deeper dive and a majority had very few security permissions in place.
- Mobile Application functionality and user liability is outlined in NIST SP 800-157 and highly recommended
- Each Mobile Application requires roughly 4.5 updates a year (multiply that by each application downloaded)

Mr. Cassidy said he would recommend a deeper dive analysis on enterprise and supply chain mobile applications in the development areas that also address security.

Mr. Tom Karygiannis, Senior Computer Scientist from the Computer Security Division at NIST, mentioned that he gained his expertise in mobile device applications by initially testing and analyzing palm pilots and working with DARPA (Defense Advanced Research Projects Agency)[25] on a program called Transformative Apps[26] Program (TransApps) which includes providing smartphones to soldiers in Afghanistan that had applications that could translate the local dialect to English and vice versa. Questions arose on how these applications can be verified and perform as intended, and they could present many risks based on networks connections. Mr. Karygiannis said he began using open source tools and working with NIST researchers to develop new test capabilities, and since had received enquiries from many agencies requesting for guidance in testing mobile applications.

Since NIST, NSA, and DISA were all developing a set of guidelines related to mobile applications, they worked together to develop NIST SP 800-163 *Vetting the Security of Mobile Applications*[27]. The

[25] http://www.darpa.mil/default.aspx
[26] http://www.darpa.mil/Our_Work/I2O/Programs/Transformative_Apps.aspx
[27] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf; http://www.nist.gov/itl/csd/20150126_sp800163.cfm

document provides guidance to agencies on assessing risks and testing. It is not meant to provide strict parameters to agencies but to provide information on what should be tested. Since each agency has a different level of security, it is up to the agency to determine the appropriate level for their requirements.

Various banking and financial services were considered when testing applications. The findings were that the financial institution applications tested had hard coded security keys programed inside. However, in some cases, the application failed and unlocked a database but was not able to gain access or export data. The NIST Computer Security Division office reached out to agencies to look for other ways that agencies can manage without having a Mobile Application Engineer or expertise on staff. Mr. Karygiannis explained that independent labs test on mobile applications can be conducted and results provided to agencies.

Cloud Geolocation and Privacy

David Cullinane, (Moderator), Chairman, Board of Cloud Security Alliance
Jerry Archer, Senior Vice President & Chief Security Officer, SallieMae
Michael Bartock, IT Specialist, Computer Security Division, ITL, NIST (PPT provided)
Thomas Finneran, Principal Consultant – IDennedy Project (PPT provided)
Jim Reavis, Co-founder and Chief Executive Officer, Cloud Security Alliance

Mr. David Cullinane, Chairman of the Board of Cloud Security Alliance (CSA) and ISPAB Board Member, introduced the Cloud Geolocation and Privacy discussion panel.

Mr. Finneran, Principal Consultant – IDennedy Project and Co-Author of *The Privacy Engineer's Manifesto*, presented a "How To" guide of what principles to think about when migrated to a Cloud and how to incorporate privacy requirements (PPT, page 2 & 3).

- How does Cloud Provider handle encryption and encrypted data?
- Does our user have exclusive access to his or her data?
- Does our data get commingled with other people's data? Is the commingling managed effectively?
- Can our user access all of his or her data whenever needed?
- Does the cloud provider satisfy all compliance requirements including OEDC, FIPPS, GAPP, specific statutory regulations for all jurisdictions, or all enterprise privacy policies?
- Is data stored so as to be physically protected?
- Can data be transferred without the knowledge of the cloud provider or the data manager/owner?
- Are the laws and regulations of all relevant jurisdictions satisfied?

(More guidance outlined in the PPT)

Mr. Finneran emphasized that these are basic business and privacy requirements applied to a cloud enterprise. The next steps include incorporating the privacy components that rely heavily on data stewardships. He continued by stating there are three different steward roles: Producer, Usage and Administrative that govern the data. All stewards take into account the requirements and processes. The Board remarked that the presentation provides a good outline and similar to the Federal Information Processing Standards (FIPS).

Michael Bartock, IT Specialist, Computer Security Division, ITL from NIST, spoke on the NIST IR7904[28], *Trusted Geolocation in the Cloud: Proof of Concept Implementation* (Draft) which he has been working on in collaboration with CSD and the NCCoE (National Cybersecurity Center of Excellence)[29]. The concept behind this publication was to provide hardware and define geolocation that we can trust in a cloud environment.

Mr. Bartock mentioned that there are a lot of benefits to migrating to a Cloud environment like agility, flexibility, dynamic resources, and leveraging CSP services. It has been challenging to get people to adopt cloud computing. One issue that Mr. Finneran mentioned, multiple customers can share the same physical environment in the cloud but there is also a lack of boarders. CSPs may tell their CSCs (Cloud Service Customer) that their workload is running in the US but no clear visibility available or mechanism to support the statement. The other potential issue is the integrity of the hosted environment. If CSC does not know what hardware the workload is running on top of, there is no way to verify what CSP is asserting. In addition, there is the issue with data protection and whether the workload is encrypted.

Mr. Bartock worked with the NCCoE in conducting a use case as a building block to tackle some of these issues. He explained that some security requirements already have a trusted resource pool in place such as a physical environment that performs measurements on firmware while software runs over top of it. A hardware root of trust is stored in the measurements values if updates or tampering of the environment occurs, the measurement values would change. Mr. Bartock explained this happens by tagging each server allowing one to make decisions based on geolocation of the physical environment. Moving towards, Mr. Bartock provided insight into how data protection of workload on a virtual machine can be encrypted or decrypted. If CSPs wanted to migrate the workload and a technical mechanism is in place (such as a migration policy that states Cloud service provided must stay in the US), the CSP would have to contact the CSC if there are plan to migrate to another country. The proof of concept for any CSC is to have a technical mechanism in place to enforce the server and datacenter trust values have been unchanged since the last validations. *The board asked who would be responsible for auditing and providing the proof of concept mechanisms.* Mr. Bartock's response is for the CSP to provide the capabilities to deliver proof of concept mechanisms to ensure CSCs that they have security policy criteria that must be met.

Mr. Jerry Archer, Senior Vice President and Chief Security Officer of Sallie Mae, began by saying that "What drives us to the Cloud" is overall IT cost reductions. The savings will allow government agencies to invest more money into IT staff, privacy, and security. Mr. Archer explained that there are CSP challenges that are being analyzed that consist of: Unintended expectations/consequences, integration and the importance of Service Level Agreements (SLAs), CSP's level of operations meets the recipients standard of operations, compliance of requirements, use of strong encryption (the CSPs do not have ownership of the data), lawyers and security CISOs (understanding risk liability), and, lastly, assumed cyber liability verses security transparency (if CSPs assume all liability of data less transparency is needed although if they do not, more transparency is required for the recipient) .

Mr. Jim Reavis, Co-founder and Chief Executive Officer, Cloud Security Alliance, added that there are cloud trends that are focused on the intermediary of the CSPs and CSCs. There are smaller companies that actually come in-between the two that are able to encrypt the data so that the CSP cannot have access to it. In some cases, CSPs are not pleased with the encryption process because it interferes with their

[28] http://csrc.nist.gov/publications/drafts/ir7904/draft_nistir_7904.pdf
[29] http://nccoe.nist.gov/content/trusted-geolocation-cloud; http://nccoe.nist.gov/content/building-blocks

marketing business models in that they would like to use some of that information. However, Mr. Reavis emphasized that there are companies that are providing this encryption service so the information is secure. Presently, this does not pose a problem but this could problematic if this approach becomes popular and more companies adopt it. As the market competition heats up, large CSPs would find a way to produce this service themselves. There are other solutions that are being conducted in this space such as cloud application controls in building a database and advising the organization on policies they can implement.

Mr. Reavis reiterated discussion points from Mr. Finneran and Mr. Bartock that the security mechanisms should be built in to include: encryption, privacy and security features. The future of assurance in cloud is to continue audits. It will be necessary to have legal requirements scoped in and there may be different solutions for each cloud service. CSA Security, Trust & Assurance Registry (STAR)[30] focuses to have a cloud control matrix of security controls with all the other requirements known and to work with other countries and industry that are moving towards regulating a cloud service standard. Ultimately, customers would map in their requirements without changing the control. *The board remarked that they are pleased with the work that is being put into this space in developing regulations. FEDRAMP was the beginning predecessors to regulating CSPs and offered a lot of information that will be helpful to moving forward in establishing a standard.*

NIST Updates on Cryptography Program Process
Matt Scholl, Chief, Computer Security Division (CSD), ITL, NIST
Andrew Regenscheid, Computer Scientist, Computer Security Division, NIST (PPT provided)

Mr. Matt Scholl, Chief, Computer Security Division, ITL, NIST, provided a background of the Visiting Committee on Advanced Technology[31] (VCAT) which is a Federal Advisory Committee Act (FACA) board that reviews and makes recommendations regarding general policy for the NIST, its organization, its budget, and its programs, within the framework of applicable national policies as set forth by the President and the Congress. The VCAT put together a sub-committee called the Committee of Visitors[32] (COV) of leading industry and academic experts to review NIST's balance between research and development and engineering with a focus on the cryptography division (see NIST IR 7977[33]).
Mr. Scholl stated that since the last ISPAB meeting in June 2014, the VCAT received the COV's recommendations[34], have begun acting on the recommendations and prioritizing future actions.

Mr. Andrew Regenscheid, Computer Scientist, Computer Security Division, NIST, continued the discussion and provided the Board with the COV/VCAT recommendations. He also wanted to commend and acknowledge the COV for their insight and assistance in this process. The COV panel members[35] consisted of leading industry and academic professionals that reviewed extensive NIST materials

[30] https://cloudsecurityalliance.org/star/
[31] http://www.nist.gov/director/vcat/
[32] http://www.nist.gov/director/vcat/vcat-051414.cfm
[33] http://csrc.nist.gov/publications/drafts/nistir-7977/nistir_7977_draft.pdf
[34] VCAT report: NIST Cryptographic Standards and Guidelines Development Process
http://www.nist.gov/director/vcat/cryptographic-standards-guidelines-process.cfm
[35] Vint Cerf of Google; Edward Felten of Princeton University; Steve Lipner of Microsoft Corporation; Bart Preneel of Katholieke Universiteit Leuven; Ellen Richey of Visa Inc.; Ron Rivest of the Massachusetts Institute of Technology (MIT); and Fran Schrotter of the American National Standards Institute (ANSI)

surrounding NIST's Cryptographic standards, how they were developed and who contributed to them. NIST also provided the COV with the background information on cryptography related to Dual EC DRGB and Elliptic Curves. NIST provided the COV with a general overview of its processes and transparency standards; in addition, to face-to-face meetings and discussions. All NIST COV materials are posted on NIST's website[36] and are open to the public.

Mr. Regenscheid provided a walk-through to the Board of the VCAT recommendations (see slide 3). The recommendations were broken out into four sections:

- Openness and Transparency: Develop and implement a plan to further increase the involvement of the cryptographic community, including academia and industry.
- Independent Strength/Capability: Strive to increase the number of technical staff.
- Clarification of Relationship with NSA: NIST may seek the advice of the NSA on cryptographic matters but it must be in a position to assess and reject it when warranted.
- Technical Work, Development and Processes: NIST work openly with the cryptographic community to determine how best to address the number of specific technical recommendations.

Based on these areas, NIST has taken action in increasing their cryptography group (see slide 5) as well as publishing NIST IR 7977, *NIST Cryptographic Standards and Guidelines Development Process*. NIST is having open discussions with stakeholders and publically providing all documentation of the VCAT report and COV materials for overall awareness and input from the community on their website. *Examples Include:* IETF, ISO, ANSI, X9, IEEE, US Congressional Staff, US Industry, Industry Associations, And Foreign Governments. Moving forward, all NIST contributors of authoring a document even if it is in conjunction with National Security Agency (NSA) will be acknowledged. In the past, there have been contributors but not all have been identified as authors. Mr. Regenscheid stated that NIST has removed the Dual EC DRGB from NIST SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*[37].
NIST acknowledged that the ISPAB has offered an invaluable service to them and would like to continue to provide regular updates of their activities as well as welcome the advice of the Board in monitoring their activities and transparent process.

Mr. Chris Boyer, Mr. Greg Garcia and Mr. Edward Roback participated remotely today. The meeting recessed at 5:37 P.M.

[36] http://csrc.nist.gov/groups/ST/crypto-review/index.html
[37] http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf

Thursday, October 23, 2014

The meeting resumed at 8:30 A.M.

Update on Mutual Legal Assistance Treaty in Relation to Intelligence and Communication Technologies

Nathaniel J. Gleicher, Director for Cybersecurity Policy and Law, National Security Council, The White House
Mary Rodriguez, Principal Deputy Director of International Affairs, US Department of Justice

The Chair began the session and stated that this session is a follow-up presentation on Mutual Legal Assistance Treaty (MLAT[38]) by Mr. Ari Schwartz in relation to intelligence and communication technologies at the last ISPAB meeting in June 2014.

Mr. Nathaniel Gleicher, Director for Cybersecurity Policy and Law, National Security Council from The White House began the session. He stated that the President announced in January 2014[39] that the MLAT modernization is a priority. In order to improve this process, the National Security Council (NSC) made a budget request on behalf of the International Affairs of US Department of Justice (DOJ) to revamp the outdated computer systems and assist with the overall improvement of this process. The MLAT process was developed in the 80s to promote law enforcement information exchange internationally for court prosecution. This process is used if evidence is being stored oversees through the internet as an example. For a foreign country to obtain access to that evidence and present it in court, they must go through the MLAT process. MLAT; however, is not the dominate process when sharing information. This process is related to international courts and their law enforcement procedures in gathering evidence.

Ms. Mary Rodriguez, Principal Deputy Director of International Affairs of US Department of Justice, mentioned that her office's role is to be the central authority for all MLAT requests from foreign countries pursuing treaties or agreements on the exchange of information particularly related to cyber-crime and cyber information. The vast majority of requests are internet crime which has increased to 110% in the past ten years. She continued, as an example, the requests range from preserving records in the U.S., internet service provider data and communication content. Her office is responsible for reviewing those requests and determining whether the evidence requested has proved probable cause for the information requested. This is based on a series factors:

1) Foreign law enforcement must present evidence to the U.S. that is relevant to the investigation.
2) Requests of content data are hard to meet due to the U.S. high standards.
3) The probable cause standard, if met, requires a search warrant.

The board asked in terms of the requests for relevant information received; do the requests target certain individuals or general information? In response, Ms. Rodriguez stated that her office's mission is not engaged in large data sharing. It could be an email or an account that has been identified. If they prove relevancy, Ms. Rodriguez and her colleagues must review the content of the data and under the 4th Amendment remove all irrelevant information. Since they have to put everything through legal; the process is time consuming.

[38] http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm
[39] http://www.whitehouse.gov/the-press-office/2014/01/17/fact-sheet-review-us-signals-intelligence

The International Affairs, DOJ, services all federal, state and local, and overseas government agencies and organizations. Ms. Rodriguez said her office is manned by 46 attorneys and 14 para-legal on staff but the overall MLAT process is rigorous. Some of the foreign government partners are good at corresponding regularly and others are not, and providing training for this process might be helpful.

Privacy Engineering Workshop (PPT provided)
Naomi Lefkovitz, Senior Privacy Policy Advisor, ITL, NIST
Sean Brooks, Privacy Engineer, ITL, NIST

Mr. Sean Brooks, Privacy Engineer ITL from NIST, mentioned that NIST has held a series of Privacy Engineering workshops[40] beginning in April 2014 to gather feedback from the government and private sector related to how to build privacy into products and systems. Privacy is a challenging subject that spans a number of domains, including law, policy and technology. Notwithstanding numerous sets of principles, including the foundational Fair Information Practice Principles (FIPPs), that seek to address the handling of individuals' personal information, many concerns exist about the future of privacy in the face of rapidly evolving technologies. Process-oriented principles (such as FIPPs) are an important component of an overall privacy framework, but on their own they have not achieved consistent and measurable results in privacy protection. In the security field, risk management models, along with technical standards and best practices, are key components of improving security. Similarly, the safety risk management field also has well-developed models, technical standards and best practices. To date, the privacy field has lagged behind in the development of analogous components.

To address this gap, NIST has begun the Privacy Engineering initiative. Privacy Engineering focuses on providing guidance to information system users, owners, developers and designers that handle personal information. Such guidance can be used to decrease risks related to privacy harms, and to make purposeful decisions about resource allocation and effective implementation of controls. Both presenters assisted with developing a draft risk model that was presented at the 2nd Privacy Engineering Workshop, September 2014.

Ms. Lefkovitz mentioned the goal was to have risk engineering objectives that focus on privacy policies. The risk objectives thought process was “how will we analyze risks”. Ms. Lefkovitz explained that they narrowed it down to three objectives: Predictability, Manageability and Confidentiality. The risk model is intended to be correctable. Thinking in terms of system administrators, the intent is to give them control to correct a problem and end-users should be able to make reliable assumptions if inaccuracy occurs. These three objectives can essentially support the assessment of any issues that may become problematic. The risk model is also intended to include individuals.

The Board commented that there does not seem to be a mechanism in place in the current risk management model that would allow prioritizing and scoring the risk based on importance. The Chair noted that the engineering architecture component is lacking in understanding and may pose implementation concerns. Ms. Levin, ISPAB Board Member, thought this might be more of an interpretation for organizations to follow a risk management framework that builds in privacy objectives that apply to each organization unique privacy and security requirements.

[40] http://www.nist.gov/itl/csd/privacy-engineering-workshop.cfm; http://www.nist.gov/itl/csd/privacy-engineering-workshop-september-15-16-2014.cfm

The goal is to have the risk management model provide support in assessing a risk management framework that can be applied to a multitude of situations. A NISTIR (NIST Internal Report) on the risk management model is anticipated to be released in 2015.

Industry Perspectives (CSRIC) on the NIST Cybersecurity Framework

Chris Boyer, (Moderator) Assistant VP – Global Public Policy, AT&T Services Inc.
Danielle Kriz, Director, Global Cybersecurity Policy, Information Technology Industry Council (ITI) (PPT provided)
Robert H. Mayer, Vice President, Industry and State Affairs, USTelecom Association (PPT provided)
Melanie Seader, Senior Cyber & Infrastructure Security Analyst, Edison Electric Institute (PPT provided)

Chris Boyer, (Moderator) Assistant VP – Global Public Policy, AT&T Services Inc and ISPAB Board member, explained that this session main focus is to provide an industry perspective on the NIST Cybersecurity Framework and invited experts that have implemented the cybersecurity framework. As NIST released a Request for Information (RFI)[41] asking for feedback the experience with the Cybersecurity Framework[42], this session will also update the Board on "*how does industry view the framework*" and *how is it being used outside of government"?*

Ms. Melanie Seader, Senior Cyber & Infrastructure Security Analyst from Edison Electric Institute (EEI) began with some background information on EEI which consists of three business models companies (see PPT slides): Investors, Owners and Utilities. Ms. Seader works for the EEI utility company that provides 70% of the U.S. power. The company has a number of committees, and the NIST Framework engaged the committee members in other disciplines. Many of these committees are focused on policies. Within these committees the organization as a whole came up with ten threats from industry and developed mitigation strategies for each threat. She said the next steps are focused on risk management, legal policies, supply chain and cybersecurity.

Mr. Robert H. Mayer, Vice President, Industry and State Affairs from the US Telecom Association thanked the board for inviting him. He described his company represents small to midsize businesses. Mr. Mayer talked about the initiative that he co-chair under the CSRIC – FCC (The Communications Security, Reliability and Interoperability Council) and related to the evolution of the NIST cybersecurity framework and to the communication industry. Referring to the presentation slides, Mr. Mayer mentioned the importance of synchronicity in regards to the timeline of events surrounding the NIST cybersecurity framework. The CSRIC under the FCC initiated a new charter focused on the areas that CSRIC engages in. CSRIC was in the process, and they will start working with CSRIC WG4 to develop the CSRIC best practice when the framework is complete. He also mentioned that CSRIC is developing studies and reports that will lead to the ability to provide assurances. It is noted that these assurances map well to the NIST cybersecurity framework. It is essential to consider useful and effective measurements to define security core indicators and then risk management measurements. There are 22 categories and 98 subcategories that assist industry with selecting the correct controls based on their security efforts during the critical infrastructure scoping efforts.

Ms. Danielle Kriz, Director of Global Cybersecurity Policy from the Information Technology Industry Council (ITI) thanked the Board for inviting her. She provided a an overview of her organization which consists of 60 U.S. based companies that represent hardware, software and IT services companies and

[41] http://www.nist.gov/cyberframework/cybersecurity-framework-rfi.cfm
[42] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

approximately 30% of that are not based in the U.S.

Most of Ms. Kriz's responsibilities are international in nature and she spends large amount of her time every day on cybersecurity proposals and policies from other countries like China, EU, India, Brazil, besides the U.S. It is her organization's perspective that government should do a lot to boost cybersecurity and industry can and does a lot too and they need to work together. It is important to have successful government policies that improve security. By her experience, she attested that there are policy proposals that would actually decrease security or harm innovation and trade. With that being said, Ms. Kriz, called attention to the ITI principles on page 3 of her presentation:

To be effective, any efforts to improve cybersecurity must:

- Leverage public-private partnerships and build upon existing initiatives and resource commitments;
- Reflect the borderless, interconnected, and global nature of today's cyber environment;
- Be able to adapt rapidly to emerging threats, technologies, and business models;
- Be based on effective risk management;
- Focus on raising public awareness; and
- More directly focus on bad actors and their threats.

Ms. Kriz pointed out the similarities of the ITI Principles to the NIST cybersecurity framework which demonstrate that this is the correct approach to cybersecurity. Ms. Kriz and her organization participated in the development of the Framework and participated in all workshops. She stated that a regulatory static approach is not the correct policy for cybersecurity. Now that the NIST had released Cybersecurity Framework V1.0, the ITI has proceeded to raise awareness to use this approach. Ms. Kriz also emphasized the importance that the NIST cybersecurity framework is presented globally because cybersecurity and threats are global concerns, and IT companies and non-tech companies require cybersecurity protection.

Ms. Kriz praised the NIST cybersecurity framework and NIST's commitment to providing best practices and standards. She is confident that the easy and simplified steps laid out in the cybersecurity framework offer entities essentially the more approachable way of thinking about cybersecurity. The ITI will continue to raise awareness and adoption industry and government. Cybersecurity has to be embedded in "what we do". The U.S. government is watched very closely around the world. NIST's open transparent process that is workable and reasonable enforces that this is the correct approach.

After lunch and before the start of the next session, the Board took a picture to be included in NIST Annual Report.

Update on Federal Implementation of Identity Management
Update on Federal Cyber Workforce Efforts and the National Initiative for Cyber Education (NICE)

Cheri Caddy, National Security Council, The White House
Tim Polk, Office of Science and Technology Policy (OSTP), The White House

Mr. Polk opened with an update on NICE workforce challenges and the steps developed through NICE to address them. The NICE[43] program was founded five years ago by the Comprehensive National

[43] http://csrc.nist.gov/nice/

Cybersecurity Initiative (CNCI). Progress that includes raising job awareness and the importance of cybersecurity, and improvements have continued to evolve; however, the demand for cybersecurity professionals are expanding more rapidly than the government can train the workforce. With the increased demand, agencies are cannibalizing each other's workforce and the private sector is cannibalizing the government's workforce and vice versa.

Mr. Polk mentioned that his department does a lot of work on workforce analysis driven much to the question of whether the current workforce have a quantity or quality gap. There is a quantity gap but there may also be a quality gap in some areas. It is difficult to determine due to a lack of insight into those areas, and more work is necessary to get a better idea of what the workforce is, such as:

- What is the workforce we have?
- What is the workforce we need?
- What skills do those people need to do their job?

The NICE program developed a Workforce Framework[44] consisting of seven categories with each comprising several specialty areas, and 31 common types of cybersecurity work areas[45]. But there are no job postings for computer security within the federal government. Over the last year, the NICE program has been working to apply the workforce framework to the entire federal workforce to better assess the government's needs. There is not enough good data to assess the workforce in its entirety to date or to determine what information is not being captured. The key is to obtain the metrics and measure the effectiveness of our workforce. Tim Polk emphasized the importance of reaching out to Middle/High Schools and engaging them in cybersecurity.

Ms. Cheri Caddy, National Security Council (NSC) from The White House, explained that her office framed their work in five broad categories starting with: Critical Infrastructure, Protecting Federal Networks, Incident Response, Information Sharing, and Developing a National Policy on Cybersecurity. Overall Security and Privacy is the main focus; the NSC is promoting the NIST Framework and receives feedback from industry and government.

Drones and Privacy – Panel Discussion

Jeffrey Kosseff, Privacy and Communications Associate, Covington & Burling, LLP (Washington DC) (PPT provided)
Christopher Lee, Directorate Privacy Officer, Science & Technology Directorate, US Department of Homeland Security (PPT provided)
Mario D. Mairena, Senior Government Relations Manager, Association for Unmanned Vehicle Systems International (PPT provided)

Mr. Christopher Lee, Directorate Privacy Officer, Science & Technology Directorate from the US Department of Homeland Security began the presentation by providing an overview of Unmanned Aerial Program (See PPT slides). An Unmanned Aerial Vehicle (UAV) is defined as:

- More than 20 – 30 lbs.
- Monitoring devices

[44] http://niccs.us-cert.gov/sites/default/files/documents/files/NICEWorkforceFrameworkSlickSheet-Final.pdf
[45] http://niccs.us-cert.gov/training/tc/framework; http://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework

- Limited Uses
- Location restricted

Mr. Lee continued by saying that there are controls in place that restricts their capabilities. There are not substantial differences between a model airplane and a UAS (Unmanned Aircraft Systems), but Federal Aviation Administration (FAA) requires the UAS operator to have an authentication of use certificate known as a Certification of Authentication (COA). Mr. Lee's office was the first to publish *Privacy Impact Assessment (PIA) use of Robotic Aircraft for Public Safety (RAPS)*[46] for testing SUAS (Small Unmanned Aircraft Systems) based on FAA Advisory Circular (AC) 91-57[47] (slide 4): Applying what conditions and scenarios that UAS could be deployed in and used. The goal was to develop a consumer report for UAS for state and local government agencies with plans to purchase UAS's for law enforcement, and search and rescue operations (such as the Coast Guard operations) etc. He explained that the thought was to have a report available that would help identify the government's needs. In the search and rescue example, Mr. Lee explained, that UAS technology could increase their search range and help find the person lost quicker which would be similar in cases such as disasters (chemical spills, forest fires etc.).

The Board asked if these are just private non-DHS uses of UAS. Mr. Lee responded that these are not just DHS uses. He continued by stating that in 2012 Congress passed the FAA Modernization and Reform Act[48] which triggered a lot of current activity regarding UAS industry. Essentially, congress opened up UAS airspace to take effect in 2015. The Act passed required six test sites within the U.S. Instead of an operator getting a COA they could use these test sites that would not interfere with other airspace and would allow special designated areas people can test their UASs.

For areas if used for surveillance, it is necessary to review these questions based on FIPPs[49] (Fair Information Practice Principles): what data was being collected, how long the data is being stored, notifying the public of the UAS use, and providing public demonstrations of the operations.

Mr. Mario D. Mairena, Senior Government Relations Manager from the Association for Unmanned Vehicle Systems International (AUVSI) began his presentation by providing a brief overview of AUVSI and the direction that UAS technology is heading. The AUVSI is represented by 7500 individual members, 600 corporate members, 25 National Chapters on Development, academia and civil and defense members. He noted that UASs do not have the capacity to be used 24/7. Usually, they can be used in 50-90 minute intervals. He stated that due to portrayal in popular media in movies and theater, UASs have received negative public perspectives.

His presentation explained additional uses for this technology and provided projected market research growth in the UAS industry. The UAS industry estimated at $11.3 billion and expected to grow to $140 billion as a global market industry with the capability to create 103,000 jobs. A majority of the market place identified for UAS and particularly for agriculture needs which are projected to be 80%.

[46] https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_st_raps_nov2012.pdf

[47] http://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentid/22425; http://www.faa.gov/documentLibrary/media/Advisory_Circular/91-57.pdf

[48] https://www.congress.gov/bill/112th-congress/house-bill/658; http://www.gpo.gov/fdsys/pkg/BILLS-112hr658enr/pdf/BILLS-112hr658enr.pdf

[49] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

He stated that in the FAA Privacy and Reform Act, provisions on public safety that include first responders, firefighters, and law enforcement to be used under these conditions:

- Fly below 400 feet
- Only fly during the day
- Operator must obtain line of sight with the UAS at all times.
- Weigh less than 25 lbs.

Public entities have been utilizing UAS for the past two or three years. Hobbyists are required to follow these guidelines as well. Mr. Mairena said at the time the 2012 FAA Privacy and Reform Act that his organization was focused more on security and safety and were unaware of the legislation introducing privacy concerns. He stated that there seems to be a distinction between an unmanned and manned system where a manned asset does not require a warrant but an unmanned UAS does. He added that there also seems to be a legal and social premise that surveillance systems should be illegal under any circumstances. Mr. Mairena remarked that there is a lot of useful information that could benefit law enforcement from the use of UAS systems. Lastly, he stated that he would like to work with FAA and he believes that the industry be regulated in safety and security.

In response to *the Board's question on whether there have been any Federal legislation regarding UAS,* Mr. Mairena said that no efforts have been made for a Federal law but is unsure whether there are proposed bills that have the technical expertise to address the UAS industry.

Mr. Jeffrey Kosseff, Privacy and Communications Associate from Covington & Burling, LLP began by stating that there are great benefits in having the UAS technology while acknowledging that there are very real privacy concerns. He provided some insight into current baseline state / local laws. Most of the state legislation is proposing privacy laws that focus on government surveillance for the privacy sector which in some states would exclude a journalist using a UAS surveillance system on individual property.

The Board inquired as what protections for a private citizen to limit a journalist from surveying. Mr. Jeffrey Kosseff explained that under common law intrusion upon seclusion it would be illegal, e.g. 1) if someone intentionally intruded on a citizen, they can be held liable; 2) if information was wrongfully published, someone could be held liable; 3) if one is flying above a private citizen's private property; the operator can be liable for trespassing, and finally, 4) if the UAS is flying above 83 feet on private property, the private citizen could destroy the UAS and not be held liable.

Mr. Kosseff mentioned that as a privacy lawyer; he is more concerned with hobbyists knowing the UAS regulations. Mr. Mairena remarked that regulations should be provided upon purchase of a private UAS. In closing the panel asked the Board to keep asking questions on commercial use vs. personnel use, for community standards about the privacy protections, culture and pressing on neutral legislation.

Presentation on Drones and Privacy

Harley Geiger, Senior Counsel and Deputy Director, Freedom, Security and Technology Project, Center for Democracy & Technology (CDT) (PPT provided)

Ms. Toby Levin, ISPAB member, introduced Mr. Harley Geiger, Senior Counsel and Deputy Director, Freedom from the Security and Technology Project, Center for Democracy & Technology (CDT).
Mr. Geiger thanked Ms. Levin and the Board for inviting him to speak on the UAS topic. He began his

presentation by mentioning that the CDT is a global non-profit organization that is primarily focused on preserving privacy, free speech, and other civil liberties while enabling technologies to grow companies and government agencies in the security space. He also pointed out that the CDT is covering similar topics to the boards meeting agenda and would welcome the board to invite other members of his organizations to speak on health data, cybersecurity geolocation and many others.

Mr. Geiger's presentation was broken up into three parts:

1) Uses of UAS/drones, privacy issues and public trust,
2) Legal protections for privacy or lack thereof,
3) CDT's recommendations for UAS and privacy.

He stated that CDT recognizes the importance of unmanned aerial systems (UAS) and they believe it is a valuable technology that has lots of positive uses, such as: hazardous circumstances, farming, and law enforcement. It is an inaccurate perception that policy holders want to hold back this technology, and policy holders do want to see this technology used for science, ecommerce, disasters, law enforcement and security. He emphasized that despite these beneficial uses, there is potential for UAS technology to degrade civil liberties. As an example, UAS surveillance capabilities far exceed other current systems in places which pose a larger impact on civilian privacy than older technologies. He explained that UAS are less expensive compared to older surveillance technologies (helicopters) which will make them more accessible to the public and state/local government. A UAS can quietly monitor a wider range for an extended amount of time without refueling. Mr. Geiger provided the Board with an example of current surveillance technologies such as red-light cameras that have a limited reach and asked the Board to think of a surveillance technology that has the capability to follow anyone unlike a red-light camera that only follow the person within the range of the stationery camera. UAS can also add on capabilities, such as, facial recognition cameras, thermal imaging and other sensors which will make the technology more intrusive. As military efforts wind down, military UAS/drones are being distributed to state /local governments which will be biggest market initially.

From a policy perspective, Mr. Geiger said the idea is to not make the UAS surveillance illegal but to have a policy in place that addresses privacy concerns. Currently, the public has an unfair image of UAS system technology capabilities accompanied by a lack of privacy protection make the public relation message negative. He continued by saying that the public want protection from the troubling capabilities of this technology.

Mr. Geiger emphasized that if the UAS industry want broad public acceptance then it will need to address civil liberty issues. The alternative would be to risk a regulatory back-lash among consumers. There have been a number of surveys and public comments expressing alarm and hostility in UAS. He continued by stating that the reason why the UAS industry does not have a good public relations message is due to the privacy concerns. He mentioned that there are 16 states that have laws regarding the use of UAS. These laws focus on law enforcement from a state/local perspective. The CDT encourages a uniform federal regulation that would address privacy protection concerns and help establish public trust.

At present, Mr. Geiger, said there are very few nationwide restrictions of law enforcement using UAS to monitor outside citizen homes. The FAA law for regulating the integration of UAS/drones in the U.S. airspace mentions privacy and transparency zero times. This oversight has affected the UAS integration effort. Currently, no federal stature provides privacy protection or describes a process of government use of drones for surveillance of the public.

He continued his presentation by mentioning that the 4th Amendment of the U.S. Constitution protects Americans from unreasonable search surveillance (see slides for examples). He mentioned that there are no laws protecting a citizen outside of their home from surveillance and privacy issues. CDT provided recommendations for policy holders and asks for industry support with the following:

- Recommends federal legislation for emergency, farming, and commercial assets.
- Recommends federal legislation that should establish due process for law enforcement to use the UAS systems for surveillance, a process that provides transparency.
- Legislation should establish a minimum threshold for private industry.
- Band lethal weapon capabilities on UAS / drones. (FAA prohibited this but there is still opposition regarding weapons).
- Commercial use of UAS/drones should have privacy transparency requirements and technical specifications.
- Government use of UAS/drones should have applicants submit a data collection statement to the Department of Transportation (DOT) that outlines collection retention and uses of data.
- Lastly, the government should establish a public assessable database website of government / private authorized UAS/drone operators.

In conclusion, Mr. Geiger said that UAS / drone technology has positive benefits and potential abuse. The CDT's goal is to protect civilian privacy while preserving the technology.

The meeting recessed at 4:10 P.M.

Friday, October 24, 2014

The Chair opened the meeting at 8:00 A.M.

NIST Updates & National Cybersecurity Center of Excellence (NCCoE) Updates

Donna Dodson, Associate Director, Chief Cybersecurity Advisor, Information Technology Laboratory, NIST, and Director, NCCoE
Matt Scholl, Acting Chief, Computer Security Division, NIST

Ms. Donna Dodson, Associate Director, Chief Cybersecurity Advisor, Information Technology Laboratory, NIST, and Director, NCCoE announced to the Board that Dr. Romine could not be here today but wanted to take a moment to thank the Board for their continued support and acknowledge their invaluable efforts. Ms. Dodson heartily echoed Dr. Romine's words.

Ms. Dodson reported that NIST is in the process of hiring a new Chief of the Security Division (the largest Division at NIST) which should be completed before year end. She explained briefly the process that goes into hiring a Division Chief. Beginning with the release of the vacancy position description to the public to return of postings, a small group of designated NIST staff members reviewed the candidates and conducted phone interviews. If selected, the candidate will be asked to spend an entire day at NIST meeting senior NIST officials as well as to present on strategic direction on cybersecurity.

Ms. Dodson continued with updates on NIST programs and focused work such as: National Strategy for Trusted Identities in Cyberspace (NSTIC), National Initiative on Cybersecurity Education (NICE) and National Cybersecurity Center of Excellence (NCCoE) and lastly, Cybersecurity Framework. One of the two focuses for NSTIC was to setup the Identity Ecosystem Steering Group[50] (IDESG) which was developed two years ago to work specifically with an identity management focus. Two pilot programs were awarded this year. NIST was pleased with Executive Order 13681[51]—Improving the Security of Consumer Financial Transaction that recognizes the guidance set in 2011 NSTIC on the use of multiple factors of authentication and an effective identity proofing process. There are two separate pieces related to chip and pin authentication. Without the strong authentication credentials consumers tend to be very concerned with identity theft. As a whole, bringing these two authentication pieces together demonstrates the government's commitment to strong authentication.

Ms. Dodson expressed great excitement in latest development of NCCoE[52] facility up and running. The program is currently moving into Phase I of getting the facility actionable. One of NIST's big actions items was to have a Federally Funded Research and Development Center (FFRDC) to support the NCCoE. Ms. Dodson highlighted that the NCCoE's FFRDC is the nation's only FFRDC that is entirely focused on cybersecurity – security of the nation's information systems. The Indefinite Delivery, Indefinite Quantity (IDIQ) contract was awarded to the Mitre Corporation[53], a not-for-profit organization that operates six other FFRDCs. The award marks a new phase for the NCCoE, which was established in partnership with the state of Maryland and Montgomery County, MD including academia institutions to assist in building out cybersecurity infrastructure use cases as well as looking at the fundamental

[50] https://www.idecosystem.org/
[51] http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions
[52] http://nccoe.nist.gov/
[53] http://www.nist.gov/itl/nccoe-092414.cfm

capabilities to support security measures such as asset management, authentication, and mobile. Also, applying NIST's standards and best practices basing on use cases built into security infrastructure that becomes actionable for products and services. Each use case is different and depends on the companies requirements. NIST oversees the day-to-day functions working with Mitre and federal people. She also emphasized that NIST strongly values working with new technology and being a part of the development instead of subcontracting work.

NCCoE has set-up a program to have interns help with building those use cases based on NIST's best practices and processes and provide demonstrations. Donna Dodson said it was a great experience listening to the way the interns interpret NIST guidelines. Every quarter the NCCoE holds an Open House to invite interest in participating in NCCoE work, and often a number of partners participated actively with the students at these events. NIST's work at the NCCoE is developing a new publication series to compliment NIST SP 800 series updates.

Mr. Scholl briefed the Board on the NICE program that has extended across agencies. In the past year there were discussions to transfer the NICE program from NIST leadership. After months of discussions between NIST, DHS, NSC, the decision was settled to keep NICE at NIST which means NIST will continue to serve in a coordinating function for education awareness on pieces of cybersecurity across agencies. It is not NIST's role or authority under the NICE program to bring cybersecurity awareness across agencies but to assists in aligning job driven training programs and develop mechanisms that will extend NICE's ability to coordinate outside of government on a larger scale to help people find cybersecurity jobs. Some data has been collected but not on a national scale. The purpose of this would be to identify jobs for government (link back to OPM website[54]) so that private industry will understand the needs.

Ms. Dodson added that while NIST works within the NICE program and moving into the next phase of the NCCoE, it would be helpful if the Board could help address any high level questions regarding the NICE program for the next ISPAB meeting. Mr. Scholl offered details of NICE annual conference, November 5-6, 2014, which will be looking to share and de-conflict, build jobs, and training.

Mr. Scholl listed successful events including a SHA3 workshop in Santa Barbra, CA, August 22, 2014. NIST is working towards finalizing SHA3[55] as a federal standard while making some adjustments to SHA2 as two separate options. The projected timeline for SHA3 to be released is next quarter.

NIST and Health and Human Services (HHS) have had a joint effort on Health Insurance Portability and Accountability Act (HIPAA) security measures regarding special publications for the government on authorizations and technical guidance. Basing on OMB M-14-04, NIST guidance[56] for continued ongoing authorizations was added and an interim publication was released highlighting the changes.

Mr. Scholl asked the Board for feedback on how impactful and/or how relevant a few areas of NIST research is, particularly NIST's Crypto validation program processes and research development areas. NIST will be testing programs and citations that will be used for requirements. The NIST Cryptography Technology Group has established Quantum Information Program with UMD and in collaboration with

[54] http://www.fiercegovernmentit.com/story/opm-nice-work-define-cybersecurity-workforce-problems/2010-08-16; https://www.chcoc.gov/transmittals/TransmittalDetails.aspx?TransmittalID=5716; http://www.fedtechmagazine.com/article/2014/08/opms-agenda-building-federal-cybersecurity-workforce
[55] http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_standardization.html
[56] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

National Security Agency (NSA). Ms. Dodson stated that Board could assist in providing feedback to NIST specifically of when NIST needs to be heavily engaged in this area.

The Board noted that the Quantum Information Program as a bigger issue in what would support e-commerce when these technologies become more available. The economic front is why NIST is heavily interested in this area and have invested resources to research more deeply. The Board suggested that NIST would need techniques to apply to this area and work back into a schedule as well as take into consideration for all current activities and timelines. Mr. Scholl mentioned NIST will be holding workshops in August 2015 about Cloud Provider Services (CPS) security focusing on the following: GPS tracking and timing security, infrastructure, identity on mechanisms, certificate browsers, and security automation.

Updates on Embedded Device Cybersecurity: Medical Devices[57] *to Automobiles*

Kevin Fu, (Moderator), Associate Professor, University of Michigan
Ken Hoyme, Distinguished Scientist, Adventium Labs
Gary McGraw, Chief Technology Officer, Cigital
Suzanne Schwartz, Director, Emergency Preparedness/Operations & Medical Countermeasures – CDRH, Office of the Center Director

Mr. Kevin Fu, (Moderator), Associate Professor at the University of Michigan and ISPAB member introduced the panel. He began by mentioning that there have been several meetings with the Association for the Advancement of Medical Instrumentation[58] (AAMI) which is an independent body that discusses medical and embedded device security.

Ms. Suzanne Schwartz, Director of Emergency Preparedness/Operations & Medical Countermeasures within the Office of the Center Director (CDRH) reported that Food and Drug Administration (FDA) recently hosted a public workshop – *Collaborative Approaches for Medical Device and Healthcare Cybersecurity*[59] where 1100 people reported participated online alone. FDA decided months ago that it would be appropriate to host a meeting to bring together the entire public health sector stakeholders in the area to discuss cybersecurity. FDA is a regulatory agency; but the authority of the Center for Devices and Radiological Health[60] (CDRH) is solely confined to medical devices. In particular, the area of medical devices and cybersecurity at large that connects with the other components of the healthcare system – beyond the medical device manufacture – which means the scope of broadening outreach with all appropriate healthcare partners is critical. She continued by mentioning that the decision to host a workshop aligns with the Executive Order and work being done on the NIST Cybersecurity Framework. The forward posture of the CDRH is to evaluate policy on medical devices and how they evolve and advance in technology and function in the through the entire healthcare ecosystem. The CDRH has been collaborating and leveraging its efforts that are being made through the Federal and private sector. *The Board asked if the focus was on the whole life of the medical device verses just the design and manufacture of the device.* Ms. Schwartz said that the focus is the Total Product Lifecycle[61] (TPLC). She also explained that the efforts are focused on first setting FDA regulations and then communicating to the

[58] http://www.aami.org/
[59] http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm412979.htm
[60] http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/
[61] http://www.fda.gov/aboutfda/centersoffices/officeofmedicalproductsandtobacco/cdrh/cdrhtransparency/ucm199906.htm

medical communities, and to have medical device manufacturers submit their devices designs to CDRH to be evaluated from a holistic perspective.

Dr. Fu pointed that when considering cybersecurity, Mr. Gary McGraw from Cigital may have more insight into medical device manufacturers and the changes that they are making. Mr. McGraw stated that he and his company have been performing analysis on different kinds of systems including Smartcard technology for many years. He further presented a brief background of Cigital and the company's focuses on cybersecurity particularly in the design and development of the physical build-out efforts. Cigital has analyzed systems all over the world. The medical device manufacturers have recently approached Cigital to evaluate their devices in considering cybersecurity with the implicit requirement to secure these devices. He explained that people using devices do not fully understand how to secure devices and are often misguided as well. Cigital is helping the discussion of some of the security problems that are designed into these devices. The uses of the operating systems are not secure due to poor encryption error and debugging. Mr. McGraw said that they do not broadcast the issues found but instead work directly with the manufacturers to improve their understanding of cybersecurity. In his opinion, medical devices are 5 to 7 years behind security engineering technology although cybersecurity issues in general are still being worked on. The medical community is asking for devices to react appropriately when under an adversary attack which means they are expecting the device will not fail from any attack. Mr. McGraw followed up with an example of an emergency room environment using the Internet of Things (IOT) where a number of different devices communicating with each other that resulted in a heavily saturated environment of information sharing. Traditional functions of password protection would not be appropriate in this environment due to the harm that could occur if a doctor cannot access a medical device quickly. Therefore, it is critical to find a way to make security invisible in this environment.

Ms. Schwartz added in the medical device guidance[62] that was released on October 2, 2014, regarding risk management for medical device manufacturers to define a cybersecurity risk management plan and provide documentation which is part of the design, controls, and quality assurance regulation. The CDRH is holding a webinar with medical device manufacturers on October 29, 2014 to give the device manufacturers the opportunity to ask questions, for example: What is the CDRH looking for in device designs? What does that mean to the manufactures?

Mr. McGraw commented that although policy and regulations are important, the physical engineering of these devices is even more important. He stated that engineering moves faster than policy and getting security changes recognized in the real-world will be challenging.

Mr. Ken Hoyme who is a Scientist from Adventium Labs added there are overlaps on how devices are designed in this space. The draft medical device guidance on the pre-market asks for the company to perform security risk management on their devices. Basically, perform an analysis of risks on their devices and accept any risks the company is willing to accept. Once the company accepts the risks, the device will then be submitted to FDA for approval before any hospital would purchase the medical device and integrate it with other devices from different manufacturers. Obviously, more research would need to be developed on usability and security not just for devices but requirements for device approval from the manufacture and validation process in order to validate the devices function effectively in the

[62] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff, October 2, 2014, http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf

environment. The major challenge is in the Emergency Room (ER) or Intensive Care Unit (ICU) of a hospital where there will be at least ten other devices that are manufactured differently. The risk presented is that although the devices are individually secure, collectively they are out of sync with each other. This area is part of the safety and security risk that can cause harm from a holistic perspective and not just a security business risk like HIPAA. Mr. Hoyme continued by saying that Advertium is working with the AAMI committee to help guide device manufacturers on how to apply safety and security risks.

In order to help regulate hospital devices it would also be beneficial to designate a senior hospital decision maker to review manufactured devices and risks because in some cases there is not a decision maker in charge. Ms. Schwartz mentioned that this community is at an interesting stage and she would like to process more of the data coming in between the federal and private sector. She added that outreach and education are going to be key areas for healthcare security.

No Public Participation Scheduled

Discussion on Safeguarding Health Information [63]

Julie Chua, Office of National Coordinator for Health IT, HHS
Rachel Seeger, Senior Advisor for Public Affairs and Outreach, HHS/OCR
Kevin Stine, Group Manager, Computer Security Division, NIST

Mr. Kevin Stine provided the Board with the following discussion points for this panel:

1) To provide insight into the recent NIST Safeguarding Health Information conference, and
2) To provide an overview of the stakeholder views from the Office of National Coordinator for Health IT within Health and Human Services (HHS).

Mr. Stine continued with an overview of the Safeguarding Health Information program. The first two years of the program, NIST and Medicaid Services mainly concentrated on delegating the HIPAA Security Rule and the enforcement functions. However, within the last five years, the focus has been on working with the Office of the National Coordinator for Health Information Technology[64] (ONC) which has been leveraging the strengths of NIST and Office for Civil Rights, HHS[65] (OCR), from the angle of requirement and reinforcement while NIST provides the technical expertise and guidance perspective. The objective has been to focus on the healthcare community and the broader cybersecurity space in general. The annual conference held to address policies and security issues regarding the healthcare industry has grown every year. Mr. Stine mentioned that there were 600 participants this year. In addition, the number of participants accessing the webcast exceeded the number of official registrants which suggested that information was disseminated within organizations. The conference was engaging with participants in a meaningful way based on the questions and feedback. The purpose of the conference was to explore the current Health IT security landscape with a focus on practical strategies, tips and techniques to help manage risks. There were two keynotes: Mr. Darren Dworkin from Cedars

[63] Safeguarding Health Information: Building Assurance through HIPAA Security – 2014, September 23-24, 2014 http://www.nist.gov/itl/csd/safeguarding-health-information-building-assurance-through-hipaa-security-2014.cfm
Agenda with links to presentations http://www.nist.gov/itl/csd/upload/Agenda-Safeguarding-Health-Info-092214.pdf

[64] http://www.healthit.gov/newsroom/about-onc

[65] http://www.hhs.gov/ocr/office/

Sinai Health Systems in Los Angeles, California and Mr. Daniel Solove from George Washington School of Law. Mr. Stine also mentioned that the clientele that are connected to Mr. Dworkin's organization is probably most publically recognizable people around the world. Mr. Daniel Solove's presentation focused on security and privacy from the health IT space. The agenda was a balance between policy and a "boots on the ground" operations perspective of safeguarding health information and challenges that the health IT space is facing – from large health systems and providers to government for both state and federal involvement. The conference covered updates on the NIST Cybersecurity Framework and how that could be applied to a broader healthcare perspective while reviewing it from a HIPAA security rule perspective. Other topics at the conference were: HHS updates on policy and data breach reports. Ms. Rachel Seeger, Senior Advisor for Public Affairs and Outreach from HHS/OCR spoke on medical device security and FDA activities and announced a workshop coming up the end of October or early November. Lastly, Mr. Stein touched on enforcement activities. He provided some observations regarding the conference in general that it seemed the most technical sessions were the most engaging; such as NIST representatives deep dived into cryptography technology to help provide some understanding to the healthcare community. He also stated that due to this feedback there may be a need to provide specific technologies to health IT listing the technologies, how they can be applied and how do the NIST standards mean to the healthcare community for organizations of all sizes and on the usable implementation function on these areas.

Ms. Rachel Seeger, Senior Advisor for Public Affairs and Outreach within HHS/OCR commented that the most popular conference session seemed to be on business associates (third party providers), who have a new element of liability under the HIPAA Security Rule. This liability focuses on accountability for HIPAA's security rule and breach requirements. The High Tech Act Rule within HIPAA also increases the OCR's enforcement strength because now there are significant penalties for not complying with these regulations. Ms. Seeger mentioned that recent settlements have been getting a lot of press because they have been multimillion dollar settlements (referencing the last 4.3 million dollar settlement between Presbyterian Hospital and Columbia University). She emphasized that there was a lot of focus on this during the workshop session. There is strong emphasis for education and outreach in the healthcare community regarding these regulations.

Ms. Julie Chua, Office of National Coordinator for Health IT, HHS participated in the session on OCR and NIST regarding the Cybersecurity Framework. One of the concerns from stakeholders was the challenges with performing a risk assessment and applying relevance of the cybersecurity framework to healthcare providers within their environment. This is the key to foster a culture of privacy and security within the OCR's legal authority. Healthcare IT systems are a high priority along with adoption and optimization of healthcare standards. Ultimately, addressing these issues and providing privacy and security will result in better healthcare services, lower costs, and better health for the American people. Ms. Chua also mentioned that this is a big culture change for the government and stakeholders to understand the privacy and security components in order to have a better healthcare system.

Mr. Stine mentioned that in addition to the conference he asked Ms. Seeger and Ms. Chua to discuss the activities and efforts among offices in HHS. Ms. Seeger began by stating that there is a balance between regulation and integration that her office is focusing on and that all sizes of healthcare organizations are affected no matter large or small. The HIPAA rules are scalable and flexible depending on the size of the organization.

Ms. Seeger stated that a major concern is healthcare breaches. The number of breaches occurring in the healthcare industry is growing in regards to information sharing, patient identities and business associates. She emphasized that it is not about whether breaches are going to occur, it is when as healthcare best practices have been low within the industry. She went on to explain that firewall and safeguards in doctors' offices are minimal and doctors are most likely not informed of the HIPAA rules. Mr. Stine added that the NIST cybersecurity framework has begun dialog with healthcare representatives but definitely more needs to be done.

The ONC's concern is looking at the needs of a large healthcare provider such as Kaiser Permanente and then looking at smaller doctor practices which have more vulnerability. The types of breaches within the industry include people using bio-sharing services and user error. ONC is trying to determine how to reach out to smaller doctor practices and have them follow the HIPAA rules. If a breach occurs, patients ultimately lose trust with not only their doctors but the healthcare delivery system. Ms. Chua mentioned that ONC does have educational information but it is inadequate. Ms. Seeger added that they have released a clip on YouTube, titled "HIPAA for Dummies"[66] to help explain the security rule. *The board suggested that the ONC's educational efforts to include what providers can do versus what they are not allowed to do.* Ms. Seeger stated that ONC is releasing some HIPAA guidance in a form of a manual to provide awareness and scenarios; for example, in the event of a cyber-attack that might take down networks throughout the nation. This information will be important if a major disaster occurs as well. No date was mentioned on when the manual will be released but it is currently being worked on.

Board Discussion

The Board reviewed each session on the agenda and to evaluate any follow-up action is necessary. Annie Sokol, DFO, had advised the Chair to raise discussion on FY 15 Work Plan for ISPAB. The Chair asked the Board for a motion to approve the minutes from the last meeting. Mr. Centafont motioned to approve the minutes and Mr. Garcia seconded the motion. The Meeting Minutes for June 11-13, 2014, was approved.

The Board's Review of the meeting:

Privacy and Civil Liberties Oversight Board (PCLOB) Updates

- The Board finds the presentation on Title VII, Section 702 interesting.
- The Board would like to invite Mr. Medine to present the report on the review of Executive Order 12333 as and when it is released ~ Spring 2015.

Continuous Diagnostics and Mitigation (CDM)

- The program is lacking progress in delivering back to the agencies.
- There is not enough progress with only signing up agreements - 98% of the 23 have signed agreements.
- The proposal is to invite another speaker to discuss the issues
- To continue follow-up on the progress and this topic – perhaps a representative from NSC or Ari Schwartz to share thoughts on CDM's progress
- To understand where "real" progress is being made and if agencies actually use and implement this program.
- Another perspective is to get the CIO perspective regarding this topic.

[66] https://www.youtube.com/watch?v=UWGojMPtiUA

FedRAMP Updates

- Re-authorization issue is interesting, 6-7 weeks update, making progress
- FEDRAMP is moving in the right direction
- To reevaluate in 2015 with no immediate updated for the next meeting.

Mobile Devices and Protection of Sensitive Information

- The board remarked that the panel had different perspectives on the issue.
- Board thoughts:
  - How would NSA use commercial devices?
  - Should there be app vetting solution across agencies?
  - NIST SP 800-163 and NIST SP 800-157, OMB M-06-16[67] -- ability to use devices as an authenticator (will be ready in a few weeks) and OMB requirement will need to update their publication(s):
  - Is there value targeting the OMB requirement between publications; Update the technology based on this new technology.
  - The Board approved to send a letter of recommendation to address the following issues:
    - Current situation of derived credentials in light of OMB publication 157
    - Recommend OMB to update M-06-16 siting the use case for PIV and CAC to incorporate derived credentials to be allowed
    - The OMB M-06-16 states that the device should be separate from – ones agency authentication CAC.

Cloud Geolocation and Privacy

- There is no plan for a follow-up discussion on this topic.

NIST Updates on Cryptographic Standards Program

- NIST asked the Board's feedback and to assist with continuous quality assurance in NIST cryptographic processes
- The Board agreed to continue monitoring the cryptography process and to get periodic updates from NIST at each meeting.

Update on Mutual Legal Assistance Treaty in relation to intelligence and communication technologies

- MLAT presentation was well done and the Board has no further comments or follow-up needed at this time.

Privacy Engineering Workshop

- The Board agrees to have ongoing updates
  - Current focus Appendix J that map to controls specifications
- The Board would like to rework the presented program plan, and narrow down the specific issues. The Board made the following comments:

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

  - Privacy did not translate well to engineers.
  - Require more information on the Appendix J test cases
  - To request Dr. Ron Ross to join Naomi Lefkowitz for the next updates

Industry Perspectives on the NIST Cybersecurity Framework

- To have a panel similar to this session every year as the Framework evolves.
- The Board is interested in the following topics:
  - More outreach and awareness and connection with business risk
  - Adopting regulatory agencies; evaluating compliancy
- The Board is considering writing a letter to OMB to harmonize the direction of the agency regulators in regards to the Cyber Security Framework:
  - To return to this topic after the next CSRIC workshop.
  - To have an update on this topic in the spring 2015.

Update on Federal Implementation of Identity Management

Update on Federal Cyber Workforce Efforts and the National Initiative for Cyber Education (NICE)

- The Board has the following questions:
  - Can we understand the size of the cybersecurity gap?
  - Will this program train people for a career?
  - Or, can this be adopted into High School curriculums?
- To follow up on this topic but has not specified a timeframe.

Discussion on Drones and Privacy

- The presentations were interesting but the focus on regulations and technology should remain neutral
  - The Board discusses the necessity to write a letter to OMB to encourage members of congress to address the use of drones and privacy, specifically to address any imbalance between privacy and technology - in order to address new technology for federal law enforcement use.
- To set up another panel for next meeting with different perspectives.

NIST Updates & NCCoE Updates

- NCCoE will hosting ISPAB in June 2015at its new facility
- NIST has asked the Board’s thoughts/perspective on how critical and when Quantum Cybersecurity should be addressed.
  - The Board is to follow-up in 2015 but remarked that the transition is going to call for a lot of changes in the current cyberspace ecosystem.

Updates on Embedded Device Cybersecurity: Medical Devices[68] to Automobiles

- The Board acknowledged that a lot of progress has happened in a short period of time in this

[68] The FDA takes steps to strengthen cybersecurity of medical devices
http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm416809.htm

space.

- The Board is interested to hear the CISO perspective/ insight in this area. No update requested for the next meeting at this time but to follow-up sometime in 2015.

Discussion on Safeguarding Health Information

- The board has no further comments or update requests at this time.

Work plan for 2015

- NIST (crypto and R&D space) regular updates
- FFRDC what goes on internally and externally and how do you balance the control of each.
    - The board thought it would be useful to have speakers (executive officials) of how to measure security (outcomes) and privacy.
        - Might be a good idea to have a coherent security position on how useful the reports are.
        - Measuring outcomes from info sharing , such as:
            - How does one measure information shared that resulted in mitigating corrective actions. For example, identifying the categories that should be in the gap analysis.
            - The board felt this would be a good area to dig into deeper.
- To assist NIST in: - Public Trust in NIST, accountability
- Quantum cybersecurity issue should stay on the ISPAB radar and have regular updates
- Privacy and Identity – (such as derived credentials) is very important to the ISPAB Board especially for the use by implementers to test derived credentials
- Medical device updates
- FISMA – CDM and FEDRAMP. Specific Board areas of interest:
    - CDM – automated side; DHS of the next generation of CSTICS (end of the year) next meeting would like to hear from DHS.
- Key ESCROW update and background history

Matt Thomlinson resigned from the Board and as the Chair. He was appointed as a member of ISPAB on March 25, 2010 by Dr. Patrick Gallagher, NIST Director. Ms. Rebecca M Blank, Deputy Secretary of Commerce, officially appointed Matt Thomlinson as the Chair, ISPAB, February 28, 2013. In 2014, Matt Thomlinson was one of FED 100[69] award recipients. Matt was most appreciative of his fellow members. He thanked NIST for the opportunities to serve as a member and the Chair.

Dr. Peter Weinberger has agreed to set up as the next Chair, ISPAB. Annie Sokol will begin the approval process after the meeting in time for the next meeting in February 2015.

The meeting adjourned at 12:37 P.M., Friday, October 24, 2014.

[69] http://fcw.com/articles/2014/03/10/fed100_thomlinson-matt.aspx

ANNEX A

List of Attendees

LAST	FIRST	AFFILIATION	ROLE
Abott	Richard	Defense Daily	Media
Curran	John	Telecom Reports	Media
Konkel	Frank	Atlantic Media	Media
Mazmanian	Adam	Federal Computer Week	Media
Miller	Jason	Federal News Radio	Media
Otto	Greg	FedScoop	Media
Perera	David	Politico	Media
Ruoff	Alex	Bloomberg BNA	Media
Stemstein	Aliya	Government Executive	Media
Archer	Jerry	SallieMae	Presenter
Bartock	Michael	NIST	Presenter
Brooks	Sean	NIST	Presenter
Caddy	Cheri	The White House	Presenter
Cassidy	Michael	US Department of Justice	Presenter
Chua	Julie	HHS	Presenter
Dodson	Donna	NIST	Presenter
Finneran	Tom	Idennedy Project	Presenter
Geiger	Harley	CDT	Presenter
Gleicher	Nathaniel	The White House	Presenter
Goodrich	Matt	GSA	Presenter
Hoyme	Ken	Adventium Labs	Presenter
Karygiannis	Tom	NIST	Presenter
Kosseff	Jeffrey	Covington & Burling	Presenter
Kriz	Danielle	ITI	Presenter
Lange	Troy	NSA	Presenter
Lee	Chris	US Department of Homeland Security	Presenter
Lefkovitz	Naomi	NIST	Presenter
Mairena	Mario	AUVSI	Presenter
Mayer	Robert	USTelecom	Presenter
McGraw	Gary	Cigital	Presenter
Medine	David	PCLOB	Presenter
Polk	Tim	The White House	Presenter
Reavis	Jim	CSA	Presenter
Regenscheid	Andrew	NIST	Presenter
Rodriguez	Mary	US Department of Justice	Presenter
Scholl	Matt	NIST	Presenter
Schwartz	Suzanne	CDRH	Presenter
Seader	Melanie	Edison Electric Institute	Presenter
Stine	Kevin	NIST	Presenter
Streufert	John	DHS	Presenter
Youst	Gregory	DISA	Presenter

LAST	FIRST	AFFILIATION	ROLE
Abrens	Nick	RILA	Visitor
Barrett	Matt	NIST	Visitor
Brennan	Duckett	Retail Industry Leaders Association (RILA)	Visitor
Brown	Evelyn	NIST	Visitor
Bruggemen	David	ACM	Visitor
Church	Al	Mitre - VA OCS	Visitor
Corrington	William	CSA	Visitor
Donelan	Sean	US Department of Treatsury	Visitor
Eisgrau	Adam	American Library Association	Visitor
Flynn	Michael	Application Developers Alliance	Visitor
Greene	Robyn	Open Technology Institute	Visitor
Herndon	W	Mitre	Visitor
Josey	Herb	DHS	Visitor
Lease	Michelle	Application Developers Alliance	Visitor
LeDuc	David	SIIA	Visitor
Mitnick	Drew	Access (AccessNow)	Visitor
Moore	Debbie	Cyberzephyr	Visitor
Moore	Jack	Nextgen/Government Execution	Visitor
Musella	Anne	US Department of Treatsury	Visitor
Nadeau	Ellen	NIST	Visitor
Olson	Eric	Mitre	Visitor
Rogers	Susan	Cyberwise CP - EMC	Visitor
Serban	Jason	US Department of State	Visitor
Siemon	Rita	The Constitution Project	Visitor
Suh	Paul	DHS	Visitor
Lightman	Suzanne	NIST	Visitor