Information Security and Privacy Advisory Board (ISPAB)
Summary of Meeting

Washington Marriott Wardman Park Hotel
2660 Woodley Rd., NW
Washington, DC 20008
April 7-9, 2010

Wednesday April 7, 2010		
Started at 8:35Am	Present:	Absent:
Ended at 4:35 Pm	Dan Chenok Gale Stone Matthew Thomlinson Ari Schwartz Fred Schneider Lynn McNulty Jaren Doherty Joe Guirreri Brian Gouker Alex Popowycz Matthew Scholl Pauline Bowen On the Phone: Donna Dodson	Lisa Schlosser Peter Weinberger

Dan Chenok, Chairman of the Board called the meeting to order at 8:45 am. He welcomed the new members of the Board, Matthew Thomlinson from Microsoft and Gale Stone from Social Security Agency (SSA). He then went over the agenda for the next 3 days.

The chairman of the Board started with information about the planned Health IT letter. He said that it has been sent out for review and has been approved. It will post on the ISPAB web site when completed. He also talked about Howard Schmidt, former ISPAB member, and his new position as the Cyber Security Advisor for the new administration.

The Board members went around the room and discussed any issues or upcoming events. Jaren Doherty mentioned that there are a lot of changes to the Veterans Administration (VA) network. He said they are also teaming up with the AirForce and the Food and Drug Administration (FDA), focusing on malicious software on biomedical devices and working with the manufacturers on these issues. Dan said that he would like to raise this issue again at a future meeting.

Brian Gouker talked about the Cyber Defense Exercise that the National Security Agency (NSA) will be hosting; he said that he could try to get some of the members of the Board set up for a VIP tour.

Ari Schwartz said he would like to get a review on the Comprehensive National Cyber Security Initiative (CNCI) 3 for the next meeting- the pilot of Einstein 3.

Matt Thomlinson and Gale Stone introduced themselves.

Cita Furlani had a quick announcement about Donna Dodson. Donna is now the Computer Security Division Chief for the Information Technology Laboratory at NIST.

NIST Issues- National Initiative on Cyber Education
Matthew Scholl Presenting for Donna Dodson.

Matthew Scholl is one of the Group Managers for Donna in the Computer Security Division at NIST. In the Division they work on outreach awareness training and education. He spoke about CNCI 8 and its 4 tracks. Matt said that he would send out a guideline of the tracks to the board. He said that this officially started on March 22nd and he is looking at opening it up on public web spaces and holding some workshops on it. They are calling the new initiate NICE (National Initiative on Cyber Education).

Dan mentioned that he would like to focus on the Civilian agency participation. Donna and Matt talked about the budget for this project. Donna said that she would like to talk more about this in the next meeting when it has progressed a little more.

Health IT
David McDaniel, Veterans Health Administration (VHA)
Adam Greene, Health and Human Services/Office of the National Coordinator (HHS/ONC)
Gail Belles, VA
Joy Pritts, HHS/ONC

Gail Belles, HIT Adoption.
The Board had a Health IT (HIT) panel discussion at an earlier meeting; the information struck them enough to request another discussion. Gail Belles from VA went over the goals for the VA Health Information Exchange (HIE). She discussed the operation and legal issues going on. She mentioned that they really need to address the security and confidentiality issues in order to meet stakeholder expectation and further HIT adoption.

Adam Greene, HIPAA legislation.
Mr. Greene talked about HIPAA and the HIE and the topics that HIPAA permits for use and disclosure. He went over the use and disclosure topics including Treatment, Payment, Health Care operations, Authorization vs. Consent, and Section 164.152.

Joy Pritts, Legal Issues.
Mrs. Pritts talked about the state laws regulating use and disclosure of health information. She went over the state laws and the significant areas of interest in state laws. She talked about the Disclosure restrictions and the promise for confidentiality to encourage testing and treatment. She spoke about medical record requirements and the issue with minors for Patient Access Laws. She mentioned

that congress consistently has not been inclined to fully preempt state law for the federal approach on this. She also talked a little about HITECH (2009).

David McDaniel, VA work within the states.
Mr. McDaniel opened with a discussion of the complexity of the issues from legislation to policy to technology. He stated if this was easy, they would have likely done this long ago. He said they are still conducting requirements and gap analysis to understand what has not been identified which might be impactful. He talked about how VA wants to share their information with non HIPAA covered entities. He stated the Nation wide Health Information Network (NHIN) is somewhat less complicated since partners are HIPAA Covered Entities. He went over a list of Privacy Rights that may conflict with patient notification. He talked about the private and public sector difference and how they all come into play. He discussed a few case studies that they are currently working on.

Lunch Break

NIST Update on FY10 Activities
The Honorable Patrick Gallagher, NIST Director.

Dr. Gallagher mentioned that this Board was one of the critical advisory committees for NIST. Dr. Gallagher has been at NIST for 16 years. It has been a change for the secretary to recommend a nomination for someone who was within NIST. He said that he did not have to spend a lot of time learning about some of NIST, but still has learned a lot in the short time since his confirmation. One of his main focuses was on the structure of NIST and a proposed reorganization.

He said that the proposed reorganization at NIST has two parts. First being the people who directly report to the director. He said that wanted to give the director a core team. This will be critical for continuity to an organization that has appointed leadership. He would eliminate the Deputy Director position, and instead have 3 Associate Director positions. He is proposing that the 8 labs would be divided into 4.

Dr. Gallagher talked about the different new labs and how they will operate and their focus areas. He mentioned that these decisions have not gone through the full approval process and are currently being vetted. He said that he would like to keep working with the Board as they move forward with this. He said that within the new administration, a strong point for NIST is the high collaboration with the different agencies. The new administration wants the agencies to work well together. He said that Howard Schmidt and Vivek Kundra are working on how they can define roles and responsibilities for Cyber Security with out have a meeting for every issue. He talked about how a lot is happening with Cyber Security within the White House. He said there is an enormous amount of interest on the Hill for Cyber Security.

Dan Chenok, Chairman of the Board, said that he would like to keep the Board active in this new NIST reorganization as it was very active in the discussion of the ITL reorganization. Dr. Gallagher said that he will see a draft of the reorganization by the end of the week, but, it will be a while to be approved. He said that he has not had any complaints from the Hill and they are eager to move on with this.

OMB Update/ Metrics
Vivek Kundra, Federal CIO, OMB
Mr. Kundra said that across the government the focus has been demonstrating compliance with the FISMA requirements and now they have recognized a problem around the metrics previously asked by OMB. He acknowledged that the annual reporting requirements are driving some of this, and he plans to use new metrics to assist with driving agencies to re-focus on where they spend money for security. He said that NIST has been very helpful, and that OMB has brought in GAO as an observer to assist with creating new metrics and to build new threat models and questionnaires for agencies. He said they got feedback from a number of private sectors on what is working on there end and that he is working closely with Howard Schmidt. He talked about the big shift with Cyber Scope and the automated tools that OMB is using to exchange information with the agencies.

He said they are working on putting together a team to go to each agency and interview them on what their threats and threat profiles. They will customize profiles on every agency. Mr. Kundra said he is working with Dr. Gallagher to look at specific case studies. He talked about the May 20th event for an open workshop on Cloud Computing and how it is going to be very big for this administration. He mentioned to the Board that any involvement from the team at the May 20th event would be much appreciated.

Mr. Kundra said that he wants to leverage the open ID community and Create relationships in the digital space between services offered by the federal government and the citizens. He has put together a team, to work on the user interface and look at the associated requirements.

Mr. Kundra said that one thing he was disappointed in was lack of execution in security at the agencies. How do we move towards getting security done and this is one of the areas where he wants to spend a lot of energy.

OpenID
Elaine Newton, NIST
Don Thibeau, Executive Director, The OpenID Foundation (on the phone)
Eric Sachs, Google (on the phone)

Matthew Scholl mentioned that Mary Theofanos from NIST helped to get this panel together. Ms. Newton talked about the 4 levels of assurance in OMB memorandum 04-04 and specified in SP 800-63 and how OpenID maps to this. Their biggest issue is trying to figure out what the levels of assurance are and how OpenID can work in this space.

Mr. Thibeau talked about the OpenID Foundation, that it is a non-profit organization and its collaborative work by market competitors who come together to work on interoperable identity management issues. He said that just over a year ago they were invited to speak with Vivek Kundra about working on technical interoperability for identity credentials. Then a year later, the OpenID Exchange was launched.

Eric Sachs, Google
Mr. Sachs talked about how two years ago, Google, Yahoo, and Facebook got involved in the OpenID foundation. He talked about how people need to get away from password 'confetti', using the same password for all applications. This has a vulnerability issue if the one password is weak that can be used for multiple access points. Mr. Sachs discussed the ability to use other credentials at different levels for different purposes.

Meeting adjourned at 4:35pm

Information Security and Privacy Advisory Board (ISPAB)
Summary of Meeting

Washington Marriott Wardman Park Hotel
2660 Woodley Rd., NW
Washington, DC 20008
April 7-9, 2010

Thursday April 8, 2010		
Started at 9:15Am	Present:	Absent:
Ended at 4:56 Pm	Dan Chenok, Chairman Gale Stone Matthew Thomlinson Ari Schwartz Fred Schneider Lynn McNulty Jaren Doherty Joe Guirreri Brian Gouker Peter Weinberger Alex Popowycz Matthew Scholl Pauline Bowen Lisa Schlosser (on the phone)	Donna Dodson

Chairman of the Board called the meeting to order at 9:15am.

Minutes:
January 20, 2010 Meeting Minutes were approved by the ISPAB after a few amendments were added.

Review of Day one of the Meeting
The Board did a review of what they thought of the first day, including the Initiative 8, NICE project, and agreed to draft a letter with Board observations for a vote.

Cloud Computing Implementations
Earl Crane, DHS
Daniel Burton, Senior Vice President, Global Public Policy, Salesforce.com
Dave Miracle, Google

Earl Crane has been with DHS for about 5 years. He said he was giving presentation as the chair of the web 2.0 working group. He is an associate professor at Carnegie Melon as well. Mr. Crane talked about how they would like to develop a set of guidelines that would provide a framework to help Federal Departments and Agencies make risk based security decisions about how to securely embrace cloud computing. He talked about how this paper would support FedRAMP effort for cloud authorization. Dan Chenok mentioned that the Board might want a briefing on FedRAMP in the future.

Dan Burton has been with SalesForce for 4 years; they work close with public sector and legal and policy teams to ensure their offerings are secure and meet policy and legal requirements. He wants to make sure that people not only in government but around the world can use their Cloud technologies. He said that he is working with individual agencies with their security requirements as they look at SalesForce to assist with their mission needs. Mr. Burton explained the Six Use Cases that they came up with and their various deployment and delivery models based on the NIST Cloud Computing definitions. He went over Private Cloud vs. Community Cloud and how it breaks down into 16 Security Domains. He then discussed the 16 Security Domains.

Dave Mihalchik has been working with the government and Google apps for quite some time. He said that after numerous conversations with several federal government agencies, Google has conducted a government based certification for Google apps. He said there was a Certification and Accreditation (C&A) package submitted to GSA in March of 2009. He said that they already have comments coming back about the C&A package and are actively working with GSA.

Office of Science and Technology Policy (OSTP) R&D
Chris Greer, OSTP

Mr Greer talked about the President's strategy for Science and Innovation. He talked about how he wanted to develop an Advanced Information Technology Ecosystem. He discussed the Comprehensive National Cyber Security Initiative. He talked about Tailored Trustworthy Spaces and gave examples of the research challenges. He talked about the National Cyber Leap Year and its planned phases.

Break

NIST Issues- Key Management and Key Transition
Matt Scholl, NIST, in place of Donna Dodson, Elaine Barker and Allen Roginsky from NIST

Mr. Scholl talked about the Transitioning of Cryptographic Algorithms and Key Sizes. This is specified in Draft SP 800-131. He said that the issue was how to transition in terms of interoperability and getting things in and out of enterprises, signatures and verifications, the discussion started in 2003 and was specified in 800-57.

Encryption: AES 128 is still good for the future. After Dec. 2010 algorithms no longer approved will be SKIPJACK, and two key triple DES.
Digital Signatures specified in FIPS186-2. SHA 1 is going to be an issue, they are going to allow it in some cases and some not.

There will be transitions in the spaces of key management specifically in:

Random Number Generation,
Key Derivation Functions, and
Key Agreement Schemes.

Dan asked whether the HSPD12 guidance is still premises on generation of SHA 1 and what is the impact to the current federal ID cards? Curt Barker answered said, yes PIV uses SHA 1. After Dec will agencies have a new set of guidance to generate HSPD12 credentials?

NIST SP 800-79 is taking a look at the requirements for the PIV cards; transition plans for PIV are not yet developed. As series of issues versus impact and implementation discussions was conducted. NIST was asked if there were metrics used in loss of security on these algorithms that drove the date of December, 2010. Curt Barker replied that, yes those metrics are open in SP 800-57 and that estimated transition time needed. When they discovered that DES was not secured, it took 15 years to work it out of our infrastructures.

Lynn recommended that NIST needs to develop an outreach program to ensure that this is more known and understood by a larger community. Lynn also asked when the draft of 800-131 will go final.

Matt agreed that they need more outreach and significantly recommend that NIST look at this for a long reach on the strength of algorithms to not have to transition again for a time frame measured in decades, if possible.

Ari recommended that the board spend time looking over the documents before they consider a letter asking for either more outreach or a changed transition date.

Dan recommended a subcommittee form to read over the documents.

The board agreed not to write a letter but to read the publications. This is a potential agenda item at the next meeting to revisit.

There was no Public Participation

Board Discussion

The Board agreed that getting the Minutes edited a week or so after the meeting would keep topics fresh in everyone’s mind.

The Board discussed the interviews that Vivek Kundra wanted to start. Everyone on the Board agreed that this was a good idea but going on the interviews would be time consuming. Dan Chenok said that he would talk with Mr. Kundra about what exactly he expects from the Board. Brian Gouker would like to talk more about Initiative 8 and what the specific tracks entail.

Fred discussed the need for NSF CISE effort to be included as well as the education directorate and STEP.

Jaren expressed the need for a balance from agencies that do not have a security mission.

The board expressed interest in a formal communication on more involvement from the civilian agencies in track 4 or in the initiative in general.

Pending Cyber Security Legislation

Adam Sedgewick, Professional Staff Member, Senate Committee on Homeland Security and Governmental Affairs
Bruce Andrews, General Council for the Commerce Committee

Adam Sedgewick is a Professional Staff member and has been with community for a few years and E-gov and Federal IT for a few years.
Bruce is a General council for commerce community and is part of team working on Cyber Security. He helps manage from the community side.
Adam said they are still in the midst of drafting a bill that they would like to have within the next few weeks. He talked about the Senator Carper Bill that was passed.

Bruce said that Senator Rockefeller and Senator Snowe came to them with strong views about the bill and issues of scope of the committee, and reconciling issues with other pieces of legislation that occur in Cyber Security. He said they are working on identifying areas of critical infrastructure (CIP) and security for these areas. He said they need increased awareness of what is CIP and the importance of these issues. He added that the critical infrastructure access to classified information is hugely important in order to ensure appropriate protection. He said they would like to get NIST involved in working with the private sector on risk management and best practices. He said they are looking at provisions on added Continuous Training to the bill. He mentioned having independent audit companies to go out and audit critical infrastructures to provide public acknowledgement of CIP who is doing the right things and incentive others and assist the markets to reward those who are doing good things in security.

Peter Weinberger had concerns with where these audit companies come from and who will set the standards for the auditors and what standards or measurements will be used by the auditors to assess correctness.
Adjourned at 4:56pm

Information Security and Privacy Advisory Board (ISPAB)
Summary of Meeting

Washington Marriott Wardman Park Hotel
2660 Woodley Rd., NW
Washington, DC 20008
April 7-9, 2010

Friday April 8, 2010		
Started at 8:30 Am	Present:	Absent:
Ended at 4:35 Pm	Dan Chenok, Chairman Gale Stone Matthew Thomlinson Ari Schwartz Fred Schneider Lynn McNulty Jaren Doherty Joe Guirreri Brian Gouker Alex Popowycz Matthew Scholl Pauline Bowen Donna Dodson	Lisa Schlosser

Friday April 7, 2010

Chairman of the Board called the meeting into place at 8:30 am.

NIST Issues- SCAP- Security Automation and Vulnerability
John Banghart

John Banghart has been with NIST for about a year as a NIST employee. He began by talking about the challenges with Security Automation. He talked about how this is like the "Tower of Babel", very costly, and error prone. He said that the problem is how do they communicate security requirements? He discussed some of the solutions, including Standardization and Automation. He wants to get everyone speaking the 'same language'. He talked about what they are achieving with Security Automation. They are minimizing effort and increasing standardization and interoperability. He talked about the relationships between malware protection and SCAP, and DNS Cash Poisoning and SCAP. Matt Scholl said that they have met with the Einstein project lead and DHS wants to follow up on this.

Mr. Banghart talked about the partners they have with this project including the US Government, Foreign Governments, and the Private Sector. He talked about the NVD, National Vulnerability Database. He said that they are releasing something called eSCAPe that is an SCAP editor. He does not have a link for it yet because it is still new, but, will send out something once is has been created. He also said that the Cloud people at NIST are utilizing SCAP in many ways.

Dan asked how the board could assist with NIST in S-CAP and Mr. Banghart said that he would like them to encourage other government agencies to continue to use S-CAP and extend its use in other areas besides the Federal Desktop Core Configuration He said that the awareness of S-CAP is pretty good but the message could be sent out more.

Work Plan Discussion
The Board discussed the webcast from the second day. Matt Scholl was generally pleased with the product. They talked about how it would have been beneficial to have wireless microphones. Apart from some logistical issues, it worked out well. He would like to get the word out earlier to get more people to watch.

The Board agreed that they liked the new location of the meeting more.

Potential Agenda Items for Next Meeting:
-Issues of embedded software in biomedical devices- refocus on this
-FISMA Guidance- would like to get a panel of IGs in to talk to the board about their perspective
-Ernest McDuffy to come in and discuss NICE
-Key priorities for NIST in the next 2-3 years in cyber security
-Would like to have another discussion on what Vivek said about agency interviews and threat vectors
- A discussion on FedRAMP.
-Session with Howard Schmidt
-Session with Phil Reitenger
-Security Roadmap, Invite Matt Coose from DHS
-Initiative 3 exercise
-OMB update, NIST update
-Placeholder for GAO to come and talk about the FDCC and Agency Security Implementation at Agencies reports coming out.
-Authentication and trust framework secure online transaction work and assurance of legitimate government outbound email
- Issue of the uptake in the civilian community about SCAP, should we bring in civilian agencies to talk about SCAP? This would be useful to John Banghart. Matt Scholl and John Banghart can work on finding a civilian agency.
-Ari suggested bringing in Howard Schmidt for a discussion on Authentication and Trust framework.
-Commerce Department has 4 working groups, the one Curt is leading. They will have a Notice of Inquiry out, can we have Curt come out and talk about this?

-The Board discussed the letter that Dan Chenok put together on NICE.
Lynn McNulty and Peter Weinberger approved it. Brian Gouker believes they should learn more about the understanding of Track 4. He also does not think that having a

civilian agency as a lead would be the right step. Dan suggested taking about the reference to DOD and DNI and make the recommendations for the effort overall rather then just Track 4. The Board agreed that the letter seems to be better to go to OMB and NIST rather than Dr. Gallagher. The letter will go out to Dr. Orizag, coping Dr. Gallagher, Howard Schmidt and Vivek Kundra. Board motioned to send the letter, all voted in favor.
-Brian Gouker talked about the Cyber Defense Exercise at NSA and will work by email about getting VIP tour set up.

The next ISPAB meeting will be held July21-23rd, 2010.

Security Issues in Broadband Plan
Ari Schwartz, Board Member
Blair Levin, Federal Communication Center (FCC)

Blair Levin, FCC: Security Issues in Broadband.
Congress asked FCC to make broadband available, used and useful. Initially the filings were very FCC centric. Affordability, adoption and utilization are directly impacted by cyber attacks. In the future he thinks the report on national utilization of expanded broadband will be very impactful and is where many national priorities can be accomplished.
FCC started to study why people did not adopt broadband. 60% believed that it is very easy to steal identity on line, 40% of current users are concerned about identity theft and this will hamper usage. In contrast personal data is the most underutilized item on the internet such as healthcare information.
The most important thing is to address personal data and privacy in order to gain confidence of the user base.

FCC and NON-FCC parts of the security plans. Access, voluntary incentives, recognition of international part of the issue, broadband infrastructure are the main themes for both parts of the security plans. Non-FCC related issues include information exchanges, executive branch and regulatory agencies to develop an operational mechanism to identify users and abilities to prevent and react to attack. An increased emphasis in education in cyber security is also part of the plan. International issues include participation in international organizations and the development of a foreign county cyber security assistance program.
OMB can assist in accelerating technical actions to secure federal networks.

FCC is planning on issuing a cyber security road map in 180 days to identify the 5 most important issues that need to be addressed. They are actively seeking input on this road map and have planned a workshop. FCC recognizes that they are not the cyber security leader but there are areas to play in this important space. No one is collecting info on network operators, this is being done by FCC for telecom and one place they are looking at is reporting requirements for broadband providers. Impact and outages are not as clear for broadband as with telecom for measurements and tracking.

FCC is looking at voluntary incentives for providers. A network advisory committee was formed to identify some best practices. They are forming a NOI to see if there is interest in seeking a voluntary certification for a network to gain a public stamp of approval.

Network and Broadband Infrastructure: Focus is on inquiry proceedings. Looking a broadband resilience and preparedness. Exploring standards for broadband reliability and resilience. Working with NCS to explore potential for priority access for wireless, and exploring this concept as well for broadband and routing.

Fred wants to be sure there is parity of security between wireless and wired, not from the technology but from the requirements. This will be difficulty due to the legacy issues of the existing infrastructures and their capabilities. FCC is looking at this issue through the NOIs and attempting to be as technology neutral as possible in the results. The country needs both fixed and mobile infrastructures and both need addressing. Rules should be based on service instead of nomenclature of the infrastructure.

The worst use of spectrum is to do nothing with it. If we can get competitive pricing in 4G as a model then we can get the low grade offerings to lower price or upgrade quality. We hope this will be a helpful driver for adoption.

If the county has 97% coverage by mobile, how does this fit into the plan? FCC did not define broadband but believes that the needed qualities for broadband qualification can not be met by 3G and 4G will probably qualify. Current plans for 4 meg down 1 meg up is based on estimates for current needs and some planned expectations for future use as a base requirement to meet the qualification.

FCC takes a position that the consumer should have the most information possible to make good decisions.

Adjourned at 12pm