Information Security and Privacy Advisory Board (ISPAB)

Summary of Meeting

West Parlor Dining Room,
George Washington University,
1918 F Street, NW, Dining Room Conference, Washington D.C. (1st)

George Washington University
Cafritz Conference Center
800 21st Street, Room 405
Washington DC (2nd and 3rd)

April 1-3, 2009

Wednesday April 1, 2009			
Started at 8:50 A.M. Ended at 4:00 P.M.	Present: Rebecca Leng Dan Chenok Fred Schneider Pauline Bowen Brian Gouker F. Lynn McNulty Joe Guirreri (telecom) Howard Schmidt Alexander Popowycz Jaren Doherty Lisa Schlosser Peter Weinberger	Absent: Ari Schwartz	Visitors, presenters, panelists: Matt Scholl, NIST, Computer Security Division

The Chair opened the Information Security and Privacy Advisory Board (ISPAB) meeting at 8:50 am. He went through the agenda and discussed the topics and speakers for the day.

He talked about the Snow/ NIST draft bill. The Chair went around the board for updates and initial comments.

Lisa mentioned the recovery.gov and reporting from a security perspective. She is glad to see this on the agenda. She said that she would like to get some good comments and suggestions from the public. Brian talked about running a symposium in Hawaii, the HICCS Conference, January 2010. Fred talked about how he would like to help out Melissa Hathaway and her research. Lynn talked about attending a conference on computer forensics and that he thought it was interesting and would like the board to look into this in the future.

Dan mentioned the CSIS Commission report and that the Blog for commissioners will be put up. He also mentioned the Einstein program and FISMA 2.1. Phil Reitegher will no longer be a part of the committee due to his move to DHS as director of NPPD.

Then Dan went over the minutes from the last meeting and Lynn thought it was a very fascinating session with very good speakers and topics. Lynn thinks that some of the topics deserve further investigation. Peter agreed with Lynn and he thinks the issues are about working out the details. Alex stated that the term cloud computing could mean a ton of different things to different people. He would like to have consistent discussions on this topic. Fred could see us writing a letter discussing the cloud to OMB about the inherit security and privacy issues that does not re-state current conclusions but rather highlights the hard decision trades offs in making decisions on using cloud technologies. Lisa would like to mention this to the group of people over the next few days to see if this could be a spoken topic on Friday. She feels like we would get some input. Matthew stated that NIST is working with OMB to try and speak the same language about this. He also said that Cloud Computing work is still pretty new and the privacy part is not being addressed as intently as technology yet from the NIST stand point. Donna is working at the CNSS worksite to try and collaborate with them to get the same terminology on this. Lisa thinks that it is a huge issue that the privacy part of cloud computing isn't being addressed fully and importantly.

Eric Cole—Director of Cyber Security oversight, DOE. Cole stated that he thinks cloud computing from a Privacy point of view needs to be addressed and asked questions about the technology available to sanitize data in the cloud.

Bran Neiman, EPA – He feels like this topic is moving ahead fast and people are not grasping it. He feels that the security concerns are passing by government middle management.   The questions to be asked are "is this worthwhile, what is the value and what are the issues?"

Dan thinks there is value in raising questions about this topic. Dan will send to the board a write up of the discussion in December about the cloud computing topic. Dan stressed the importance of timing with the issues of cloud computing and stressed that the board needs to say something that is new and of value.

FNS and Tools of CERT
Mike Smith, DHS

Mike provided a background of Federal Network Services (FNS) and its new location under NCSD as well as the new organization in DHS where NCSD now falls. Doug Andre leads FNS which is currently staffing up to meet its missions.

Requirements and Acquisitions Support, part of NCSD, currently has Tier II Training LOB, C&A LOB, SAIR Tier I and Tier II.

Network and Infrastructure Security is led by Sean Donovan and includes TIS, DNSSEC, NEWORX 2 and MTIPS.

Architecture and Standards group is just forming.

Alex asked how LOBs are selected. Mike responded that this is done through stakeholder input from the FSSGB, the CIO council and individual agencies.

There was discussion on compliance and oversight of TIC agencies and setting standards for NOC/SOC operations. This will mostly involve MOAs and SLAs with DHS NPPD and US-CERT and the TIC agencies for now.

Lisa asked if they were coordinating their work with the US army SOC/NOC to leverage their expertise and lessons learned. The US Army web portal has requirement, standards and evaluation criteria for SOC/NOC that they could use. Mike took this as an action to look at this information.

Security Management led by Antoine Morrison has the mission of evaluating new technologies and looking at Cyber Security strategic issues. Lynn asked if this includes classified information and are there judicial and legislative issues with sharing this information. Mike said yes it does include classified information and they are working out the legal issues to see what can be done.

Peter asked how they were planning to measure this activity to see if it is successful in improving security. Mike stated that he was not sure yet.

Upcoming FNS activities were discussed including C&A customer day, TIC working groups and finalizing compliance program processes. Mike offered to bring in DHS employees in the future to discuss TIC external connections if the board wanted that discussion.

Break

Work Plan/ Board Discussion
Board Members

The Board talked about the new presidential transition. Obama sent teams to go into various agencies and talk to them. Melissa was involved in the transition as well.

The board discussed Privacy Protection. Each agency has the same data but not the same policies on privacy protection against data. You need to have a consistent means for data security. It depends on writing a reasonable policy. There some questions, slightly sensitive, unsensitive, highly sensitive, what is the answer to disclosing this information? Brian stated that NSA recognized the issue with sharing threat data in a classified and unclassified mechanism. Fred suggested that this type of information classification issue might be served with a continuum of protection profiles designated by each agency that have different protection mechanisms for different C-I-A levels based on what was desired. Lynn discussed the need for this information to also be pushed down to state and local governments and first responders. Dan would like to reserve a classification discussion next meeting. The CSIS report came out with a recommendation about how information is treated (sensitive, non sensitive) something that the hill is picking up on. Dan believes that this is a major discussion and it importantly affects Einstein and FIMSA 2.

20 Most Important Controls for Continuous Cyber Security Enforcement:
Consensus Audit Guidelines
John Gilligan
Gilligan Group, Inc.

John worked with Dan before.
This topic is getting a lot of attention.

John discussed how the Federal Government is no different than Private Sector. They are all being subjected to attacks at a significant rate. He talked about Cyber Security today and how it is a 'New Ballgame'. He also discussed the government security environment and how we are in a cyber war and are losing badly. The IT industry has produced an inherently unsecure environment – total security is not achievable. John believes that CIO mandates exceed time and resources available and that Cyber security is an enormously complex. He believes that we cannot fix the technology over night, but can do a lot better. John discussed how FISMA was well intended, but, what is not working. He believes that the original content was good and was well written. He said that NIST has done a really good job and produced very good guidance, but, NIST general guidance became mandatory and there was no auditable basis for independent evaluation. John believes that the grading became overly focused on paperwork. He then went on to discuss the analogy of the current FIMSA implementation; he thinks this needs more importance. John thinks that to assess effective security we need to objectively measure the effectiveness of security controls and focus on the high payoff areas and to maximize automation.

He then began the discussion on the 20 most important security control options and the approach for developing the 20 most important security controls.

He believes that you need to engage in the best security experts, prioritize controls to match successful attacks, describe automation/verification methods, engage CIOs, CISOs, Auditors and Oversight organizations and that you will also need to coordinate with Congress regarding FISMA updates. John gave examples of Critical Controls. He then read off the list of the 20 Most Important Security controls from his point of view. He went over some of the comments that people have left regarding his list of 20 Most Important Security Controls.

He talked about what the next steps to get this going would be. Lynn believes there is nothing in the document that is different than what NIST has already discussed and handled, he says that NIST has taken some of these reports and used them in their own documents. Fred thinks that we should redo FISMA to provide some specificity to the audit community. Lisa thinks that we need to contact the group of auditors (PCIA) and suggest to them what to audit and hopefully they will pick it up. If the IGs and OMB use this type of methodology than that can, perhaps, move this to more meaningful audit methods.

Lunch

Open Government and Security
Michelle Hefner for Beth Noveck.
OSTP

Michelle Hefner filled in for Beth Noveck today. Michelle ran the CIO activities.
The Board went around and introduced themselves to Michelle.

Michelle said that she wanted her discussion to be an opportunity for suggestions. She stated that they have started a new website. She is working on a collaboration piece to

4

make the government more efficient on the technology side. She said that is would be issued by OMB in coordination with the whole community. She stated that it is still in the beginning stages and she is looking for more suggestions and comments. Ari suggested that her group publish some policies and concerns for this document. Michelle had suggested that they post something on their website about the issues and have people comment on them and add more suggestions. Ari thinks this was a great idea.

Michelle stated the goal of getting information out to the public and allowing the public to participate in the discussions. She stated that OpenGov@OSTP.gov is where comments should be submitted for suggestions on how to accomplish this. Dan asked what the specifics of the Jan 21st directive were. Michelle answered:

- Dive to put more information out and have it available,
- Promote civil engagement working with industry to have informed decisions,
- Make government more efficient. How to use technology to achieve this goal and not use technology for its own sake,
- Still meet the needs of underserved communities.

Alex asked if this two way dialog could sway policy and how do you know who is participating and if they are citizens? This is currently unknown.

Dan asked about risks in providing large data sets that could be data harmed and aggregated to provide potentially sensitive information. This will be looked into. Dan also discussed the policy regimes within each agency and how they need to standardize on data classifications to allow for such aggregation. It could start within communities such as VA and DOD for example.

Ari discussed the issues of de-identification in data sets that are made public and the questions that at some point data sets become so large that de-identification is no longer feasible. Ari then asked if they can publish the list of privacy and security concerns collected for public viewing and participation.

DNSSEC and the Authoritative Root Zone
Fiona Alexander, NTIA
Timothy Polk, NIST

The board went around the room and introduced themselves to Fiona and Tim. They talked about the Internet Domain Name System. They discussed the topological view of DNS. They gave an example of the DNS query. The DOC role is the authoritative root zone. The authoritative root zone is the top of the DNS hierarchy. They discussed the current root zone management process and showed a detailed chart. Fiona and Tim talked about Security and the Internet Domain Name System. They then went on to discuss the Cache Poisoning Attacks such as inserting false data into a resolver's cache. They also talked about the Kaminsky Cache poisoning. They mentioned that Dan Kaminsky refined Cache poisoning attacks into an art form, with this, patches were developed and have been widely implemented. They went over the summary of the Kaminsky attack. They then discussed the Implications of Security Attacks on the Domain Name System.

They talked about the DNS Security Extensions and the DNSSEC standards including

the DNS Referral + DNSSEC; DNS + DNSSEC; and DNSSEC Query. Tim and Fiona shared the services provided by DNSSEC, which includes, Source Authentication; Integrity Protection; and Authenticated Denial of Existence which is all aimed to protect the end user system. They also talked about the services not provided by DNSSEC. They said that DNSSEC relies on Public Key Cryptography and Key Management. They shared a chart showing the Chaining of Keys in DNSSEC. They discussed why DNSSEC is and Opt-in technology, why we need DNNSEC at the root and how to deploy DNNSEC in the Authoritative Root Zone.

Dan Chenok closed the meeting at 4:00 pm.

Information Security and Privacy Advisory Board (ISPAB)

Summary of Meeting

George Washington University
Cafritz Conference Center
800 21st Street, Room 405
Washington DC (2nd and 3rd)

April 1-3, 2009

Thursday April 2, 2009			
Started at 8:52 A.M. Ended at 5:15 P.M.	Present: Ari Schwartz Rebecca Leng Dan Chenok Fred Schneider Pauline Bowen Brian Gouker F. Lynn McNulty Joe Guirreri Howard Schmidt Alexander Popowycz Jaren Doherty Lisa Schlosser Peter Weinberger	Absent:	Visitors, presenters, panelists: Matt Scholl, NIST, Computer Security Division

The Chair opened the Information Security and Privacy Advisory Board (ISPAB) meeting at 8:52 am. He discussed that NIST has extended him on the board for another year and that we will need to replace Phil. Fred mentioned that he would like someone with good technical background on the board and who could participate in technical discussions. The board discussed maybe asking Marianne Swanson to join. Lynn thinks that maybe someone from Semantic. Fred said that Matt Scholl mentioned something about Steve Lipner from Microsoft who had a candidate. The Board will discuss this at the next meeting.

NIST Computer Security Division
Donna Dodson, NIST

Donna talked about NRC coming in. She said that NIST talks about the goals and projects that are coming up. She said that she presented very similar slides to the NRC. She feels that the NRC panel is similar to ISPAB. She talked about the Current events going on with NIST CSD including the American Recovery and Reinvestment act, the Omnibus Bill, Executive and Congressional Activities, ITL Programs, and the CSD Reorganization. She talked about how NIST received funding from the recovery act and that they are going to go out and get grants- money for some building improvement

7

projects on the campus and there was some money set aside for the health IT and the technology side. She mentioned that under the recovery act they received funding for work on Smartgrid. Dan thinks that Smartgrid is something that he would like to add to the agenda for next meeting. She said that there are many organizational units at NIST that are looking at the Smartgrid. She mentioned that NIST is trying to get something together, maybe a write up about the system wide security issues that are slipping through the electric power control modes. She talked about how CSD is going to be looking at key management issues working with Cloud. She went over the new reorganization chart with CSD. She stated that CSD has a new mission statement. Dan made some comments on the statement and what he thinks needs to be changed. Donna said she would take these comments into consideration. She discussed the different groups within CSD (the Cryptographic Technology Group; the Systems and Emerging Technologies Security Research Group; and the Security Management and Assurance Group) and major projects that they have going on.

Identity Management Framework
Alex

Alex brought up that Identity Management was discussed at the December 2008 ISPAB meeting.
He mentioned that Elaine Newton from NIST described several activities underway touching upon Identity Management. There was a lot of discussion about work in biometrics and biometrics analysis. He discussed what he thought Identity Management meant in his eyes. He talked about NIST and Identity Management and how NIST has already produced a few bodies of work on identity issues such as SP 800-63. Alex mentioned the gap between NIST and other agencies and explained how he would assess the gap. Donna mentioned that NIST attempted to come up with a generalized framework but couldn't figure out what needed to be included; she thinks too many people are working on it. Fred thinks that we need to advocate a survey paper instead of a framework. Dan believes that Elaine needs to be part of this discussion. The Board then went into a discussion on how they think this should be addressed.

Lunch

NIST Participation in the Comprehensive National CyberSecurity Initiative11:
Supply Chain Risk Management
Marianne Swanson, NIST

Marianne went through a list of what she was going to be talking about. She introduced the Comprehensive National Cyber Security Initiative 11: Supply Chain Risk Management. She stated that it is still in the planning stages. She talked about and explained the working groups within the Initiative 11 including Senior Steering Group, Threat Information Sharing Acquisition Policy and Legal Analysis and Lifecycle Processes and Standards. She discussed the Identification of High Priority Systems with a chart. She showed the committee an organizational chart on the Pilot Program Organization. She said that DoD will have a huge part in the SCRM and mentioned that there are a few other interested organizations.

Developing a Cyber Supply Chain Assurance Reference Model
Hart Rossman, SAIC
University of Maryland

Hart discussed the project's overview that he is working on and the project's milestones. He says that it has been a collaborative research project. He went through the different phases that the project has gone through so far. He talked about the project rational and that the current threat landscape requires a convergence between "Defense In Depth" and "Defense in Breadth." He showed some charts that explained this process. He also showed a chart on the Study Participant Demographics and stated that 30 participants were interviewed. He showed a chart that explained the SDLC/ Supply Chain Ecosystem, which is a common reference model for what a supply chain looks like. He discussed SDLC/Supply Chain Interdependencies.

Board Discussion

Dan stated that he would like to further discuss key management issues with Donna and thinks that would be a good future agenda item. He also thinks that Lee Badger should come back and talk to the committee about metrics. He talked about maybe doing an Einstein II follow up in a future meeting.

Privacy Report Briefing
Ari Schwartz

Ari would like to take a look at the law and policy of this new framework. He drafted a white paper about this and would like the board to review and comment on it and decide if they would like this to be published. He discussed the four basic parts of the paper. The board gave comments and suggestions as Ari changed what he liked.

 Meeting adjourned at 5:15pm

Information Security and Privacy Advisory Board (ISPAB)

Summary of Meeting

George Washington University
Cafritz Conference Center
800 21st Street, Room 405
Washington DC (2nd and 3rd)

April 1-3, 2009

Friday April 3, 2009			
Started at 8:15 A.M. Ended at 12:20 P.M.	<u>Present:</u> Ari Schwartz Rebecca Leng Dan Chenok Fred Schneider Pauline Bowen Brian Gouker F. Lynn McNulty Joe Guirreri Howard Schmidt Alexander Popowycz Jaren Doherty Lisa Schlosser Peter Weinberger	<u>Absent:</u>	<u>Visitors, presenters, panelists:</u> Matt Scholl, NIST, Computer Security Division

The Chair opened the Information Security and Privacy Advisory Board (ISPAB) meeting at 8:15 am. He went over the agenda for the last day of the meeting. He mentioned that he talked to Rob Casey and he is going to come out to talk with the Board about Cloud Computing. The board discussed having an ISPAB networking site and all agreed that this would be a good idea.

NIST Standards and Guidelines
The Board
Donna Dodson, NIST
Bruce McConnell, Independent Consultant

Bruce served at OMB with Dan, and left in 2000 and has been running a few consulting companies since then.

The Board talked about the Consensus Audit guidelines that Bruce had been working on. 'The NIST framework for civilian agencies'. Bruce mentioned that there were a lot of reasons for the separation of the facilities; they didn't want military agencies involved too closely with private agencies. He thinks that NIST needs to be better resourced in this.

He also thinks that FISMA requires a risk based approach and that risks cannot be eliminated but only managed. The board then went through a discussion on what they thought would work and gave comments and suggestions.

Stimulus and Cyber Security CIO Panel
John Streufert, CISO, State Department
Mike Carleton, CIO, HHS
Dan Galik, CISO, HHS

This is the first time that they have addressed the board.
John discussed that it should be considered to build on the strengths of FISMA 1.0. He said that some of the same techniques had been applied at the state department and now they are a higher stage. He believes that major changes can occur in different time zones. The solution cannot occur with out ongoing support and finding out who is responsible for every device.

Mike discussed some of the conditions to get the funding to operate. He mentioned that he talked to the Recovery Act group with HHS. He talked a lot about what HHS is doing with the budget money and where they were going to be applying it.

United States Information and Communications Enhancement (ICE) Act of 2009
Erik Hopkins, Professional Staff Member
Senate Committee on Homeland Security and Governmental Affairs
Subcommittee on Federal Financial Management, Government Information,
Federal Services, and International Security

Erik Hopkins has presented the Board before about the FIRRE act.

He discussed the FIMSA 2002 strengths and weaknesses. He explained the state of cyber space today including the global information infrastructure and that the US is the greatest benefactor, yet the most at risk. He talked about the state of government information and that the bottom line is that we need to balance information sharing and information security. He discussed what FISMA 2.0 does and gave two quotes, one from Tom Davis and one from Karen Evans on their thoughts on the need for an improvement in the legislation. He went over the ICE points and how it established accountability with CISO, and it recognized interconnected nature of 'systems'. He also talked about U.S. ICE and where he thinks it will take us and the difference between ICE and FIRRE. He mentioned that the public draft of ICE will come out on Tuesday. He said that the biggest difference between the bills is going to come down to the operational level. The board asked what they can do to help; he said that he would like to wait until the public draft comes out.

Board Discussion

Dan went back to the Consensus Guidelines and mentioned that he would not call it an audit and would consider changing the name. He would also like to issue communication with OMB about this, the Board agreed. The Board agrees that the top 20 issue is good, but, still need to decide on what to call it. Lynn thinks there should be an internal government imbedding of the list. The board motioned to draft this letter/bill. The Board brought up the discussion on the Privacy paper and agreed on some questions and

concerns for it and they have decided to amend a few areas of the privacy paper to make it simpler.

OMB Update
Vivek Kundra, Federal CIO, OMB

Vivek is the first federal CIO for the new presidency. He is looking to get advice from the board. When he first came on board at the white house he felt like he moved back a decade from the technology stand point and he believed that one of the major reasons was privacy and security. He wanted to hear from the board what we can do about this. He mentioned that one of the big areas is Cloud Computing. Another big area is delivering services and how he would like to connect the American people to services, not to agencies. How can we deliver these services in a comprehensive manner that does not stove pipe them into their respective agencies? He said that he would like to keep the laws that we have now, and then further down the line change them as needed. Rebecca believes that the issues over the last several years haven't really been budget issues but more of guidance and awareness issues. Vivek says that he is working closely with Melissa on the 60 day review. Vivek believes that even the laptop will be out of date within the next few years and that is why he is very interested in the Cloud. Vivek agrees with the Board that there needs to be set Security classes. He says that he would like to turn to the Board as much as possible as a sounding board and for advice on directions.

Board Discussion
The Board talked more on the Privacy paper and the board gave some more suggestions on what they think Ari should do so that he can publish.

The Board has not issued a white paper in a while as a FACA. When the paper is finalized, the Board will let everyone know, and have NIST post it on the web. Donna thinks that it should be marked with headers. Everyone motioned to send the white paper out.

Meeting concluded at 12:20 pm

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting.

Daniel Chenok
ISPAB Board Chairman