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

George Washington University
Cafritz Conference Center
800 21st Street, Room 405
Washington DC

July 29-31, 2009

Wednesday, July 29		
Started at 8:45am	Present:	Absent:
	Brian Gouker Jaren Doherty Ari Schwartz Howard Schmidt Dan Chenok Lynn McNulty Fred Schneider Alex Popowycz Joseph Guirreri Peter Weinberger Rebecca Leng	Lisa Schlosser Donna Dodson Pauline Bowen

Lynn McNulty opened the meeting at 8:45am since the chairman of the board had not arrived yet. They started with the board discussion. They talked about Phil Reitinger no longer being on the board. A few members asked if there would be a replacement for him, nothing certain yet. There was mention that OMB now has a new deputy for management. The board then discussed the agenda for the next 3 days, and mentioned the closed meeting for the next day. The chairman of the board arrived; he started to explain that Melissa Hathaway wanted the briefing. Donna Dodson talked about the ITL Reorganization. She mentioned that this is just a proposed change. She explained how the reorganization will be organized. She also mentioned that she was the acting deputy chief. Fred said that he would like a chart of the before and after of the organizational chart. Lynn and Peter believe that the reorganization is sending the wrong message and thinks this is diffusing the purpose of ITL or Computer Security.

Sean Donelan
Program Manager, Network and Infrastructure Security DHS
TIC External Connections

Mr. Donelan has addressed this board before but has changed jobs since then. He is now a federal employee working for DHS.
Mr. Donelan discussed the TIC glossary; he said that the TIC is the actual location of where the security hardware and software is. He talked about the TICAP, which is the access provider that manages the operation of TICs in support of customer requirements and policies; includes two or more TICs and he discussed the MTIPS- are the services sold by a network vendor. He showed a pictorial graph on how it works. Mr. Donelan discussed the mission of Network & Infrastructure Security. He also talked about the TIC Initiative, networx, and the architecture and standards of TIC. He said that OCIO operates the DHS TICs. He then began to discuss where the TIC requirements come from, including the Presidential Directive, CIO Council and Government Wide meetings. He talked about the 51 capabilities of the TIC and how the TIC document references a lot of NIST standards, sot they have not started any of their own. He went over the Definition of success for the TIC and he explained the success that they would like to achieve. He talked about the definitions of the different agencies. The board gave their suggestions on what they thought the TIC meant to the agencies. He said that he did not want to give the agencies regulations; he wanted the agencies to tell him what they want. He showed a chart on Notional TIC Architecture, this chart explained how the TIC works. He talked about the Conceptual TIC Trust Relationships and how this explained the TIC and the internet connection going in and out. He showed the external zone then the TIC zone and the Internal Zone. Mr. Donelan then explained the definition of external connections. He talked about the public cloud and the private cloud. Dan thought this might be a discussion that needs further explanation or discussion. Mr. Donelan then talked about the Einstein capabilities as part of TIC. The Board agreed that this was extremely educational and he did a good job explaining the TIC.

Break

Secure Software

Aneesh Chopra, Associate Director

and Chief Technology Officer, OSTP

Aneesh was Secretary of Technology in Virginia and is well known for his leadership in the IT community. Dan has been working with him for the past year.
He discussed what the 3 ambitions of the CTO responsibilities are. He talked about what is the CTO and how does it fit into the IT world. He said that the President wanted a Senior Advisor on IT security in the White House. The President wanted him/her to focus on three areas, Health IT; Education Technology and Job Creation. Mr. Chopra said that his goals are to embrace new technologies in open government, and make the government more transparent. He was focused on two things, long-term policies and 90 day milestones. With regards to Cyber Security, he said that the President would like to collaborate more with the private sector. He said they have been working with the banking sector and healthcare sector. He said that they should have an agreement on some sort of planned action and that it should be soon. He said that their R&D is high. Their number one in R&D priorities is Supply Chain. He said that collaboration is a key priority. He also said that he was pleased to be working closely with NIST, NSF and other agencies. Fred thought that smaller agencies should have an R&D mandate. Mr. Chopra then talked about the Standards of the agencies, including FACA and Smart

grid. Rebecca says that she is glad to hear about next generation development, she thinks that it has been outdated; she thought that Intelligent transportation systems need to be updated. Mr. Chopra talked about the Research Agenda and the Public Document. He said that he would like to get public recommendations and comments on this. He talked about Vivek Kundra and how is he figuring out public policy decision and answers. He said that Vivek, Melissa Hathaway and he get together regularly.
He gave examples of the cloud and the budget for the cloud, he explained that he is very interested in Cloud and he is pushing lots of people into that direction. Dan talked about the collaboration issues; Mr. Chopra says to solve them with target intervention.
Dan said that he is looking forward to working with Mr. Chopra in the future.

Lunch

Earl Crane
Chief Information Security Architect
Acting Director, Cyber Security Strategy, DHS
Brian Burns,
Deputy Chief Information Officer for Emerging Technology,
U.S. Department of the Navy Chief Information Officer, (DON CIO)

Cloud /Social Media Panel

The board has been looking at the issues with Cloud Computing. Mr. Crane had been working for the CIO's office he is the Co-chair federal CIO community for Cloud Computing. The Board introduced themselves to them. Mr. Crane said that he was please to see industry and education on the board.
Mr. Crane had been with DHS for about 4 years. He said that his presentation was on social media. He mentioned Infrastructure, social media technologies, and cloud computing. He said that a white paper that DHS has produced is a little more up to date than what his slides cover. He mentioned that he could make the draft white paper available to the board for comments and suggestions. He explained what web 2.0 is and what the main issue was, he showed a diagram of the differences between web 1.0 and 2.0. He went through the Web 2.0 terminology including Government 2.0 and Social Media.
He talked about Spear Phishing and the definition of it: An attack targeting a specific user or group of users that attempts to trick a user to perform an action that launched an attack, such as opening a document or clicking a link. He said that Phishing emails don't seem that common anymore. Howard asked why this was being looked at so closely. Mr. Crane said that in the US it would be uncommon, but, with newer users to the internet in other countries it is still growing. He then discussed Social Engineering and how Social Networks give an easier chance to get attacked. He said that we need to figure out how to start working with the social media administrators, there is a discussion going around about mutual authentications. Fred said that he believes something should be included in the browser authenticating and approving the website that you search. Mr. Crane said that he would take that into consideration. He gave examples of social engineering issues. He then talked about Web Application Security. He explained what procurement means from his standpoint.
Mr. Burns said that wanted to talk more about the management issues. He talked about FISMA. He said that he would like to start a policy. He talked about some issues, including personal use of government equipment. Then the issue of what is external

cloud and what is internal cloud. He mentioned the question, Can we write a policy that is general enough? He said that there was not a web2.0 policy.
Mr. Crane said that they had a discussion on cloud computing with feds, he said that had a good range of information from people, but, not so many people showed up, and he is wondered why not more people we there.

Small break

Patrick Stingley,

Chief Technology Officer, BLM, DOI

Mary Ellen Condon,

Principle, Assurance & Resilience, Booz Allen Hamilton

Frank Reeder,
President, The Reeder Group

Data.Gov Panel

The Data.Gov panel went of the Identification of data, If there is information that should not be public; it is manually reviewed on the data.gov website. They based it on the Dublin Core and FGDC Plus PII & DQ.
They talked about some new cool features of data.gov; a new website. They explained the catalogs and the various things to search on the website. They also mentioned that data.gov is using cloud hosting.
Mrs. Condon thought that there should be the same databases for all communities, including government, private sector and so on. Mr. Reeder explained that this was the beginning of a continuum; he said that authentication of data is a huge problem, but they are working on this. He said that he fears that they are establishing a standard.
They talked about hashing of the data on the website they said that part of the goal is to promote repackaging; helping people find information within the government easier.

Board discussion

The Board talked with Donna about the reorganization of the Computer Security Division. The Proposal is getting ready to be put forward. She said she would like comments from the board. She talked about how some other divisions in the laboratory were doing Computer Security as well. The Board said they believe that the reorganization is a step backwards instead of forwards with Computer Security. Donna explained to the board why this is happening. Donna said that she would check to see if Cita Furlani would come and speak to the board to explain what her goals were. The Board wanted to let Cita Furlani know that the board takes the reorganization very seriously and it was their responsibility to weigh in on this.
The Board discussed the classified meeting with Melissa on Friday. Fred said that he did not like the idea to have a classified meeting with not all of the board there.

Meeting adjourned 5:10

Thursday July 30		
Started at 8:45am	Present:	Absent:
	Brian Gouker Jaren Doherty Ari Schwartz Howard Schmidt Dan Chenok Lynn McNulty Fred Schneider Alex Popowycz Joe Guirreri Peter Weinberger Rebecca Leng	Lisa Schlosser Jaren Doherty Donna Dodson Pauline Bowen

Meeting opened at 8:45am by Lynn McNulty. Mr. McNulty asked the Board members if there were any thoughts or questions about yesterday. Peter Weinberger mentioned that it was a very interesting day yesterday. Everyone thought Aneesh Chopra was impressive. Fred Schneider said that the TIC and cloud stuff suggests that there is a higher level problem. The Board members talked about minutes, and made some suggestions for changes or corrections.

CNSS/IC/DOD/NIST Harmonization (SP 800-53, Rev 3)

Ron Ross

Project Leader, FISMA Implementation Project, Computer Security Division, NIST

Jennifer Fabius Greene
IC CIO IA Senior Risk Advisor
Integrated Enterprise-wide Risk Management

Mr. Ross said that he was concerned about losing capability of the systems. He talked about the threat situation and how the intelligence community is coming together. He said that this was going to help everyone in the federal government, especially the contractors. He went over the unconventional wisdom and the new rule: boundary protection is no longer sufficient against high-end threats capable of launching sophisticated cyber attacks. He said that boundary protection is the current strategy, but, is not working as well anymore. He mentioned that they were moving from a check-based compliance to a risk-based compliance. He talked about ITAEF. Lynn McNulty mentioned that Cyber Command is being used as a trademark blurb. Mr. Ross said that he needs to fix that. He also mentioned that NIST SP800-53 was coming out tomorrow. He talked about the transformation goals of the information security transformation. He said that reciprocity is a big issue. He mentioned that common security roles were going to come out in SP 800-53. He said that the purpose of the framework is not to force everyone to collaborate together. Rebecca Leng asked if the goal was to adopt a new FIPS 199 or was it to update it. Mr. Ross said, yes and no, because it will take a long time to do that. He said that he thought that it was just going to be a transition; it was just a process at this point. He went over the transformation goals. He talked about the unified framework; he showed a generalized model of what he thought it would look like.

He went over the strategic initiatives and the tactical initiatives; he showed where these are in the NIST Special Publication. He said that risk management hierarchy was going to be the central concept. He went over 'the central question': security capability perspective and threat capability perspective. He said that cyber prep started at MITRE. He talked about the five different controls for the security capability perspective. Security control selection—cyber preparedness, there will be a description of the different threat levels and then there will be a set of controls that you can chose from. Lynn McNulty wanted to make sure it wasn't just focusing on external threat, and not internal threat. Mr. Ross assured him that they were focusing on all threat. Ari Schwartz mentioned that the chart on cyber preparedness should be in prism order. Mr. Ross mentioned that this was supposed to be a starting point with boundary protection and that agile defense is a more robust solution to boundary protection. He explained the examples of agile defense measures. Peter Weinberger was worried about corrupted data and why it wasn't on the agile defense list, Mr. Ross said that there was nothing you can really do at this point about corrupted data, that's why it was not on the list. He talked about how new documents such as SP800-53, SP 800-37 (new C&A process) show the path to convergence. He then went over the new key risk management publications that were out.

Jennifer Greene
Mrs. Greene said that Ron covered a lot of the stuff about the Intelligence Community. She said that she would be talking more from a national standpoint. She talked about how the national community can move forward. She said that mission fulfillment is critical and they need to have a more secure foundation. She said that they needed to understand what and where the risks were. She said that they needed a broader transformation process. When they came to that realization, they came up with seven roles. She said that ICO and DOD worked closely together to come up with new documents, and the intelligence community came to the shift a little earlier. She said that overall they found that the broader national security community was making a huge shift. Long term goals are SP 800-37 and even though they have not finished the document, just working on it just showed that they had potential. She talked about how ICD503 came out in the intelligence community and that this was the only policy document that was required to implement the seven developmental goals. She mentioned the NIST SP 800-47. She said that the reciprocity memo was made because they had different documentation memos. She said that in March 2009 at the CNSS annual conference, one of the outcomes was how long it could take sometimes to get people together; maybe it was time to adopt something more, and that was where SP 800-53 came out. She talked about how, if we don't take the time to understand the other partners in this effort, it will cause more problems. She said that convergence has been an educational experience for the national community. She mentioned that the openness to new ideas that NIST has, has been wonderful. Lynn McNulty mentioned that they had done a great job. Ari Schwartz wondered if there was a big concern when it comes to convergence. She said that most of the civil agencies are so tired of having to go to three different publications, so this is good for them.

Break

Donna Dodson informed everyone that Cita Furlani would be joining them tomorrow morning. Mrs. Furlani mentioned that she was happy to hear the Board's thoughts and comments.

Work plan discussion: Dan Chenok called in and wanted to talk about the things that were discussed yesterday. From what Lynn McNulty heard from Jennifer Greene, there is some commitment on NIST part to provide leadership, because of this, ITL should be kept together. Ari Schwartz asked if, from the discussion about Cloud yesterday, if the Board get someone from OMB to talk about the pilots? Fred Schneider wondered if Peter Mell could come and talk to the Board about Cloud. Donna Dodson said that she would like to invite Peter Mell and Tim Grance. Ari Schwartz said that he thought The Smart Grid seemed like a good topic. Donna Dodson said there is some trusted communications work that needs to be covered. Lynn McNulty asked if there was any interest in bringing someone in from legislation, Ari Schwartz said that cyber security bills will be mashed together and he will know in September, he said that some bills have not even been introduced yet. Consensus was to maintain work on the cloud, and bring in the principle people from NIST. Bring in NIST people and find out what they are telling people about the cloud.

Lunch

Software Assurance/Supply Chain

Joe Jarzombek,
Director for Software Assurance
National Cyber Security Division, DHS CSSLP

Mr. Jarzombek talked about the DHS NCSD Software Assurance Program. He said they started addressing it as software assurance and not software quality assurance. They do this through forums and working groups. When people would come into the working groups, the different agencies would work together. Everything is non-guidance and non-policy. He explained that the FAR changed in Sept. 2005. He then explained the vulnerable software and its exploitation. He said they are looking at functional correctness and making sure that it functions under hostile conditions. He talked about the software assurance “end state” objectives. He went over the DHS Software Assurance Program. He talked about the Software Assurance FORUM and Working Groups and how everyone agrees that Common Criteria has to change. He showed the Board the Software Assurance Pocket Guide Series and gave everyone a copy. He went over the SWA concern categories. He mentioned that the next tool expo is going to be Nov. 2-6. He showed the different publications that they came out with recently. He talked more about the document that he handed out. He said that they would be coming out with a series of pocket guides and that open source is going to help get this out. He explained how the pocket guide works. He said that the next working group will work with cloud computing. He said that software supply chain management is a national Security Issue.

Metrics

Suzanne Lightman, Lead Policy Analyst, OMB

Dan Chenok, Board Chairman

This was the first time Mrs. Lightman had address the ISPAB. She has had a long career in security with GAO and when she was on detail through the committee, is when she first met Dan Chenok. She started with OMB in October. She said that she got to this

point because of Vivek Kundra asking what he thought should go into Metrics. She has been involved with FISMA for about 10 years. She said that changes were only additions on privacy to the annual FISMA; the main thing that OMB collects is the annual and quarterly statistics. She said that the statement that is required to report on in FISMA is basically compliance metrics. She mentioned that the reporting has been kind of static. This is what she told Vivek Kundra and she would like a standard report for compliance and performance statistics. She stated that she didn't want to put it into a spreadsheet, so she thought of making a system or database to enter this information. This is an enormous contract issue because it wasn't in their original contract. She said that now they have an automated reporting tool/ database, but the metrics really didn't change because it was already too late in the year. She said that it was tough to come up with a metric that you could actually use. She stated that, what OMB would like to do is put together a working group, they want to have a collaborative-wide discussion to talk about these metrics. She said they need to come up with a balanced score card of reporting metrics that included performance and compliance together. She said that's where OMB is now. She is looking for input and discussion, and help in determining a good way to look at metrics. She said that the best bet is to not say anything about your security because you will still be attacked if you say it is good or if it sucks. She mentioned that the only metrics that they really gather is FISMA. She talked about the TIC a little bit and how that is another area that they can implement. She did not think that this was isolated to FISMA. She talked about patch monitoring, and how publishing a patch is equivalent to publishing he attack. She said that she would like to start preparing the other agencies because she sees this is becoming a phase process. She thought that when people think about FISMA they are only thinking about the big agencies. She would like to help the smaller agencies build up to report on metrics. She said that OMB made the decision at some point to concentrate on the C&A. She talked about how agencies like compliance and they understand it and moving them to something other that compliance is going to be difficult. The board members asked her what OMB thought of continuous monitoring and she said that OMB hasn't really defined this yet. She thinks that is what this new process is going to flesh out. Peter Weinberger wanted to know what she meant by continuous, does she mean continuously or a couple times a year. She said that she did not think that OMB meant to do this continuously, and that this word may be misleading to some people. She said they don't want to prejudge anything and that it has to be measureable and meaningful and it has to have consistency over time and it also has to be economically feasible. It needs to be scalable. She said that she would like to start this within 2010, but, did not think there will ever be a final set of metrics. She said that she will start sending out formal invitations to the working groups. Since the Board usually does not meet in working groups, she said that she would probably ask the board to send two representatives from the board instead of having the whole board go to a working group.

Privacy Report Briefing

Ari Schwartz, Board Member

Lynn McNulty, Board Member

Alex Popowycz, Board Member

Mary Ellen Callahan, Chief Privacy Officer, DHS

Mrs. Callahan is officially the co-chair of the CIO councils' Privacy Committee. The Board asked her to give a different perspective on what happened after the Board sent

the report. The Board went around and introduced themselves. Lynn McNulty talked about what he observed at the meeting in June. He said that it was well attended. He said that it was a very well done meeting with a lot of enthusiasm. Ari Schwartz passed out the latest draft of the privacy report. The Board members were provided with a draft of the bill in their packets. Ari Schwartz said that the idea was to try to take every recommendation that ISPAB offered. He said that he did not have as much on commercial privacy issues, so he put it up as a wiki and had lots of good suggestions. He said that there were some very good edits form the wiki. He said that they were able to get in some hooks on the commercial issues, the hooks are there, but, they will need some leadership to implement them in the right way. OMB has not been engaged in this issue. They have been following it, but there is no one actually working with it. Mrs. Callahan said that on the House side there was more of the issue of how much the Administration can do without making a bill. They said that they also briefed Melissa Hathaway and she wasn't really engaged. Ms. Hathaway came in to the meeting with the report really marked up and a lot of questions. They said they briefed Vivek Kundra and he was interested in the metrics part. Ari Schwartz said that the wiki is still up and they will have their last meeting about it. Mrs. Callahan said that she did have some observations and that she had been thinking about the report and how she saw it at the House. She said that she was trying to work together to get the policy side together. She said that the conversations at the CDT meetings have been very helpful. She said that GAO has been participating along the way also. She said that at least they are making an expressed statement, it may not fix everything but it is a start. The Board agreed to take a look back at this at the December meeting. The Board would like to stay active with her.

The Meeting was recessed by the Board Chairman at 5:00 P.M.

Friday July 31		
Started at 8:45am Ended at 12pm	Present: Brian Gouker Jaren Doherty Ari Schwartz Dan Chenok Lynn McNulty Fred Schneider Alex Popowycz Joe Guirreri Peter Weinberger Rebecca Leng Howard Schmidt	Absent: Lisa Schlosser Donna Dodson Pauline Bowen

Board Discussion

TIC and Cloud – No suitable defenses. Small groups looking at cloud. Cloud insights will not be useful. TIC may be useful to pursue. Understand where cloud fits into the bigger picture. There should be discussion between the two groups (TIC and Cloud). The levels of privacy and security should be addressed.

Web 2.0, the cloud and other concepts need to be addressed in context. How can I do Certification and Accreditation(C&A)? Every agency will have to address this. Should we do a Federal level C & A on cloud and every agency can use it if they want to? There is a new BPA on cloud services from GSA. The Board wanted to know how they are incorporating the security.

Joe Guirreri, Jaren Doherty, and Ari Schwartz will form a subcommittee to talk to GSA and OMB about this issue. They will report back at the December meeting. We will send email to keep the board members informed on this issue.

We should have a periodic update from NIST on the work that Ron Ross is doing with the DOD, IC, and CNSS. Continuous monitoring needs to be clarified.

We should invite Phil Reitinger back for 1 ½ hour or 2 hours to speak to us.

Metrics working group with OMB should be formed as a subcommittee. Joe and Jaren volunteered to serve. Dan will shadow the work and backup. Jaren will serve after clearing with his management. We need a long-term look at Health IT. Jaren will volunteer for doing that.

Bruce McConnell's question: What can we do for our own systems and other questions? Do we want to talk with Phil Reitinger about this? Ari Schwartz will respond to Bruce

McConnell on privacy questions. What can we do for identity management? Dan Chenok will let Bruce McConnell know about what Board members are doing.

NIST held workshop a few years ago on PKI and authentication that addresses his identity management concerns. We should support NIST talking to Bruce McConnell about what NIST is doing on identity management and Biometrics. We need practical examples. Internal government use is what he is concerned about.

E-FACA is an open-government initiative. What activities are not as open as they should be? FACA is one of these activities. We need to work with NIST to see what we can do on-line for the public. GSA has a pilot program on video. They are looking for advisory committees. We need to contact them. Ari Schwartz would like to do a wiki for the board. Dan Chenok will work with NIST on this to get something started. Alex Popowycz asked about social media sites use. We would like to use the NIST website. Ari Schwartz would serve as editor of the on-line activities. Maybe we could have a town council. NIST has contracted some of these services that we may be able to use. GSA has some help with this. It will work if it is in place, in time on our schedule. We may do a video feed.

How do we get more engaged with Tony Sager's Group? NIST is working with the committees, doing automated tools, cloud computing, and ISMC projects. Dan Chenok proposed getting what the CISO's are getting – the information from vulnerabilities, etc. We need a panel of CISO's to speak to the board.

Dan Chenok adjourned the open session of the board at 12:00 pm.