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

March 2, 3, and 4, 2011

Homewood Suites by Hilton D.C.
1475 Massachusetts Avenue, NW
Washington, DC 20005

	Present:	
	Board Members	Non-Board members
Wednesday, March 2, 2011 8:40 A.M. – 4:47 P.M. Thursday, March 3, 2011 8:30 A.M. – 5:30 P.M. Friday, March 4, 2010 8:10 A.M. – 12:18 P.M.	Dan Chenok (Chair) Brian Gouker Joe Guirreri Lynn McNulty Alex Popowycz Phyllis Schneck Gale Stone Fred Schneider Matthew Thomlinson Peter Weinberger	Julie Boughn Donna Dodson Cita M. Furlani Ed Roback Matthew Scholl Annie Sokol (DFO) See Annex A for record of presenters and visitors

Wednesday, March 2, 2011

Lynn McNulty called the meeting to order at 8:40 A.M., Wednesday, March 2, 2011, as the chairman of the board had another commitment.

The Chair, Dan Chenok, joined the meeting and began the meeting with introduction of the potential new members, Ed Roback and Julie Boughn. The approval process should be completed by the next meeting. As the usual practice, each board member provided their updates and recent activities. Dan Chenok informed the board that the letter re. NICE was approved and sent to Jeffrey Zients. The letter re. NSTIC was being reviewed by the NIST Director. The Chair then discussed the status of the NSTIC National Program office (NPO) which was set up as a part of DOC and NIST. Dr. Fred Schneider announced that he is a new member of the National Academy of Engineers. The Chair, Dan Chenok, representing the board congratulated Donna Dodson on her selection to the FED 100, and he also expressed his appreciation to Annie Sokol for her good work in organizing this meeting.

NIST Update

Donna Dodson
Division Chief, Computer Security Division (CSD), NIST

Donna Dodson announced that in addition to her present responsibilities as Division Chief, Computer Security Division, and Deputy Cyber Security Advisor at the National Institute of Standards and Technology (NIST), she is also the Acting Division Chief, Advanced Network Technologies Division, NIST. She is impressed with the on-going work in that division. She informed the board of the current activities in Information Technology Laboratory and especially in Computer Security Division namely – 1) Tim Polk took over the leadership as the Group Manager for Cryptographic Technology Group as Bill Burr had retired end 2010, 2) CSD will be reorganized from three groups to five groups. The five groups will cover work in cryptographic, Security Testing, Metrics and CMVP, Information and Communications Infrastructure, Mobile

Devices and Censors from a Security Standpoint, and domain perspective like Health IT and SmartGrid. Since NIST is still operating under a continuing resolution, the reorganization has not taken effect. Donna Dodson assured the board that she will share mission statement and conceptual plan with the board for comments. She was confident that she will have the managers/leaders to step forward to meet the plan. She updated the board on her recent attendance at the RSA conference in San Francisco, with the NIST Director, Patrick Gallagher. Dr. Patrick Gallagher has a new title - Under Secretary of Commerce for Standards and Technology, Director, National Institute of Standards and Technology. In wrapping up, she went over CSD's publications that were published during the past few months as well as any upcoming workshops.

Direct Hiring Panel

Ernest McDuffie, Leader of NICE, NIST
Maureen Higgins, Assistant Director, Agency Support & Technical Assistance, OPM
Peggy Maxon, Director, National Cyber Security Education Strategy, DHS
[PowerPoint presentation provided]

Ernest McDuffie provided the status of the NICE Initiative, which NIST was officially designated as the lead. He said that they are getting great support from the White House. This is the year to establish the baseline so as to make information available. The structure and funding are in place with a number of on-going outreach activities. Presently, the strategic plan and goals are still under review and will be distributed at a later date. He stated that they have had some contact with international companies and agencies but that they will keep them at arms length until the national questions are answered.

Maureen Higgins is the lead for Track 3 of the NICE initiative. She stated that the new strategic plan is going to enhance the structure of the tracks. She briefly explained the Cybersecurity workforce plan and the objective is to ensure Federal agencies have HR tools needed to attract, hire and retain a skilled cybersecurity workforce. To achieve this goal, they have created a 4-Phased approach. She explained the phases and the challenges of the phases. For direct hiring, certain authority is required, while direct hiring for group 2210 starts at level 9. She stated that there is still a lot of work to be done, and it is necessary to continue collaboration with other agencies.

Peggy Maxon is the lead for Track 4 of the NICE initiative, and she is the lead person behind the creation of the document that established NICE. She explained this track and how it is not only the driving force for the Federal Government but also for the public space. Track 4 divides the population into four different groups. Peggy Maxon also shared a rough draft of the IT Infrastructure Operations and Maintenance Worksheet, which explained the different groups under Track 4 with the different functional roles. There is a gap between curriculum, and training and qualification of students.

NSTIC

Andy Ozment, Director for Federal Information Security Policy, National Security Staff (NSS)
Ari Schwartz, Internet Policy Advisor, NIST
Jeremy Grant, Senior Executive Advisor, NIST

Dan Chenok introduced Jeremy Grant who is now the Senior Executive Advisor to manage the establishment of the National Program Office at NIST. He will be taking over the lead from Andy Ozment who has been the project lead for NSTIC since last July. They talked about the issues of privacy and trust faced by most people on the internet, and the possibility of an ecosystem for both private and public sectors. The initiative is right for the maturity of the space especially with the development of mobile devices and health information.

Ari Schwartz talked about four main concerns - Governance, Privacy, Liability and Usability. He explained that this is a national project and with the private sector leading. He is impressed with the support from a number of industry leaders and hopes that the project will be fully usable in the near future. The chairman invited the panel to provide an update in the July meeting. They readily agreed that they would have more information when they return.

Jeremy Grant agreed to return at the next meeting to discuss governance and provide an update.

Science of Security

Fred Schneider, Professor, Cornell University
Peter Weinberger, Computer Scientist, Google [PowerPoint presentation provided]

Fred Schneider introduced his topic with the 'History' of the term Science of Security. As attacks are worsening, it is difficult to predict and adoption of prevention is not effective. He does not believe that prevention is the only answer. He gave an analogy of Art vs. Craft- Art is known, Craft is taught. He stated that Science was a moving target. In his presentation, Science of Security means Body of Laws that is predictive; they transcend specific systems, attacks and defenses. There is no map to predict how things should work. He presented the expectations are in ten years and the different classes of Body of Laws - Classes of Policies, Classes of Attacks and Classes of Defenses.

Peter Weinberger, of Google, started his presentation by stating that the presentation was based purely on his own opinions. While his opinions may change, cybersecurity remains a manageable problem. He illustrated the Technical Picture and how with Good Engineering and Robust Standards raise the general level of security and Dynamic Defense and Monitoring; Forensics; and Machine Learning deal with the 'Real World'. Cyber Security is a peculiar problem and many issues are unique. New technologies such as cloud, browsers, mobile, smart grid, multi-core CPU architecture and wireless will bring new opportunities. He presented various approaches to improve security. In conclusion, he listed the cyber answer as 1) it is manageable if we look; 2) the big players will work hard to make the difference; 3) substantial resources are required; 4) intrinsically a technical field; 5) improve the security baseline and deal with day-to-day; and 6) technology cannot make up for bad human factors.

Access of Classified Information to Improve Cyber Security

Alma Cole, Director of Security Operation Center, DHS
Robert McKinney, Senior Agency Information Security Officer, OEI, EPA
John Martin, Intelligence Advisor/Special Agent, Office of the Administrator, Office of Homeland Security
Steve Williams, EPA, Office of Homeland Security

The discussion began with defining 'Security Posture', the actual use of the system and the security of the system. It led to who should be given security clearance, various levels of access to classified information, techniques and approaches in handling vulnerabilities, and how to classify vulnerabilities. The panel discussed the difficulties for critical personnel to deal with incidents without being given the appropriate clearances. In many incidences, critical personnel do not have the clearance to see the source of attack, and therefore, they were unable to make informed decisions. Agencies such as EPA have mostly unclassified information but have dealing with agencies with classified materials. Therefore, agencies like EPA are not involved in decision making and processes. In fixing incidences in one agency may not completely eliminate the problems in the broader sense. USG needs to provide necessary tools and mechanism for improved and automated reporting. While US CERT has the right process to move more information to the CIOs and CISOs, the panel recommended that Information Assurance and Information Security people should have clearances.

The meeting recessed at 4:47 P.M., Wednesday, March 2, 2011.

Thursday, March 3, 2011

Lynn McNulty called the meeting to order at 8:30 A.M. as the Chair was to join the meeting later in the day.

VA Medical devices

Randy Ledsome, VA Director of Field Security Devices
Lynette Sherrill, VA Deputy Director, Health Information Security Division
Dr. Dale Nordenburg, Medical Device and EHR Innovation, Safety, and Security Consortium (MDISS)
William Elliott, Director, Government Contract Sales, GE Healthcare Representative
Steven Abrahamson, Program Manager, Product Security, GE Healthcare
[PowerPoint presentation provided]

At the beginning of the presentation, Randy Ledsome and Lynette Sherrill stated that it is necessary to work with many organizations in achieving security. VA diligently followed HIPAA to ensure secure medical devices in order to maintain data integrity and prevent invalid results that may negatively impact patient safety. Data Protection and Patient Safety are critical VA priorities. They discussed the threats to medical devices, providing different scenarios, examples and statistics of incidences. For example, a Microsoft based system was not able to receive patches or software updates as medical devices were on some isolated network. The protection set up for the general network is directly affecting the medical devices. They had been tracking their medical devices since March 2010 and they discovered many infections. To better safeguard medical devices, VA developed a comprehensive security initiative that encompassed – communication, training, validation, scanning, remediation, patching, medical device isolation and architecture. The program is Medical Device Protection Program (MDPP) and has been implemented VA-wide. MDPP is currently focused on the validation phase of the O&M process, and continuing on various MDPP activities. They are working with FDA to improve security and deploying patches. There are guidelines to evaluate patches before implementation, and therefore, some patches were delayed as long as thirty days.

Dr. Dale Nordenburg (The MDISS Consortium Provider Advisory Group) discussed medical device safety and how the consortium's roles in progressing a safe and innovative biomedical device industry. His presentation also described an overview of devices and the issues such as software failures, hacking of health related websites. He also discussed ISO Standards, FDA's increased control to reduce risk, and the challenges of security for medical device. In his latter half of his presentation, he explained the overview of MDISS - mission, structure, goals, working groups and membership.

Steven Abrahamson's presentation included GE Healthcare and the healthcare environment, medical device security environment and challenges, and improving security within the medical device environment. In moving forward the goal of "At Work for a Healthier World", GE's strategy is to have a 'Healthymagination'. He stressed the importance of collaboration with FDA to address security standards within the various layers such as site, department, network and device. The security environment for medical device covers three main focuses – growing interest of government and customers, FDA recognition of security relationship to patient safety, and new risks stemming from security features. Steven Abrahamson recognized a number of security critical points and challenges such as security focus in designing new products, enhancing security with existing products, remote service operations, and finally, supporting customer's privacy and security obligations. GE is looking for a process for security improvements on devices that will expose it to more risks. He demonstrated the different layers of security involved - Device Security, Network Security, Data Security, Storage Security, Department Security and Site Security. The device manufacturers do not know of all of the security risks as product security covers a broad spectrum of networked devices and mitigations. It is important that security for each layer is addressed cohesively. In order to improve security in its products, GE Healthcare has taken these steps - build a Security Team at GEHC and integrate security in the design process. Moving forward, they reiterated the importance of collaboration on all layers of security.

Centers of Academic Excellence (CAE)

Brian Gouker, National Security Agency
[PowerPoint presentation provided]

Brian Gouker has been involved in the CAE program since 2003 as a NSA liaison. He would like to get more people involved in CAE. He explained CAE's goals, history, benefits, and current criteria. The three tiers within CAE are – CAE 2 Y, CAE, and CAE – R. CAE-R requires more rigorous pre-requisites as compared to the other tiers. The pre-requisites for CAE 2Y and CAE are two CNSS certifications which are under consideration to be eliminated. Generally, most students who graduated from CAE worked for private industry. This year, CAE was considering new criteria, and broadening faculty and collaboration with minority institutions, community colleges, and local communities. At CAE PI Conference, St. Louis, November 2010, there were a number of discussion items. Brian Gouker would like the board to review the CAE re-designation proposals and provide comments. He would really want to the board to answer this question – What would the board expects from a CAE graduate?

OMB Circular A130, Appendix 3

Patti Titus, Vice President and Chief Information Security Officer (CISO), UNISYS
Bruce Brody, CEO, New Cyber Partners, LLC

Bruce Body is the head of a Consulting company specializing in continuous monitoring. He is experienced with the application of A130 but he did admit the implementation had not been good. He discussed five things necessary for securing an enterprise including boundaries; devices; configuration of the devices; who is accessing the devices; and what they are doing with the devices.

Patti Titus talked about the move towards data consolidation and how it will cause a mess. She stated that this document approaches technology on 'yesterdays' mindset. It is necessary to categorize your data. Furthermore, it is also necessary to have a trusting culture in continuous monitoring. She raised that OMB has a Federal CIO and a Federal CTO but do not have a Federal CISO. It is her opinion that a Federal CISO is crucial in helping OMB to run things securely. Titus proceeded to raise some of the issues with the current A130 including no incentive from the secretaries, and the need for an agreed upon strategy that is coming from someone less than the National Security Advisor. It is necessary for the Senior Executives to fully understand FISMA, and education should begin from the top down so as to allow them to see the issues and how to incorporate in the cloud. The implementation does not include clear paths for authority, procedures and categorization. By having lower levels reporting to the higher levels, the possibilities of human intervention to compromise reporting are high as it is human nature to cover-up or shield reporting of any compromises. OPM does not have a position for an IT security person and there is no central person for reporting gaps.

Patti Titus emphasized that security is a continuous and all day activity and should not be structured as five year plan. Presently, monitoring seems to be just "checking boxes" without knowing relationship among the boxes. She believed it is useful to have this framework, and simultaneously, to give to federal officials authority, funding and incentives to understand and respond to vulnerabilities.

Federal Risk and Authorization Management Program (FedRAMP)

Dave McClure, Associate Administrator, Office of Citizen Services and Innovative Technologies, GSA

Dave McClure said that cloud computing environment has created greater speed and simplicity but also created two other issues - data categorization and risk assessment. He said that the cloud environment accentuates the necessity for security. He stated that FedRAMP attempts to define risk assessment orientation. It is still leveraging FISMA through focusing on risk categorization, documentation and authorization. In order to accelerate adoption, they are trying to get all of the players at the same table, including ISIMC, NIST, DOD, DHS, CISO Community engaged, NSA, and CSIS. Each week, there are four teams reviewing the public comments, and they are focusing on the comments that are moderate to high impact issues. While they are focusing on the move to continuous monitoring, they are challenged to draw up a list of controls for the community. There are concerns that there are too many controls for different risk levels so they are working to consolidate the controls. Presently, FedRAMP is not operational but they would like to have it ready by this summer.

DHS Updates - Access to classified information to improve cybersecurity
Bruce McConnell, Counselor to the National Protection and Programs Directorate (NPDD), Deputy Under Secretary
Sandra Stanar-Johnson, NSA/CSS Representative to DHS

Both presenters started the discussion on the memo between DHS and OMB relating access to classified information to improve cybersecurity. Bruce McConnell offered a general update of DHS and the collaboration with DOD. He emphasized that DHS considered cybersecurity a critical component of DHS, and he will be most happy to return and brief the board on cyber strategy, roles and responsibilities, budget and strategic assumptions of these topics. Bruce McConnell also touched on Cybersecurity Awareness campaign and the current work on international strategy.

Sandra Stanar-Johnson talked about the intermediate cyber language that was not understood in different parts of the world. NSA sent seven technicians to DHS to learn a common language and after a year they are gradually gaining some momentum. But the structural questions are slowing improving, and furthermore, knowing what we know has not changed the way we share information. She talked about initiating a Memorandum of Agreement for DHS, DOD and NSA. They are moving forward swiftly as they continue to learn from each other. There is a need to provide use cases on privacy to general public. Sandra Stanar-Johnson stated that the board could assist with issues relating to privacy and civil liberty and working with private sector.

HSPD 12 and Status

William MacGregor, Computer Scientist, Computer Security Division, NIST
Deborah Gallagher, Office of Government Wide Policy, GSA
[PowerPoint presentation provided]

William MacGregor provided the status of HSPD12 Implementation -- such as, there were approximately 4.6 million cards issued to employees, and 1.6 million PIV cards to contractors. His presentation also included some useful URLs for the board to find information. He proceeded to brief the board on the revision of FIPS 201-1. About a year ago, FIPS 201 team determined that FIPS 201-1 needed to be revised. As technology developed, it was necessary to incorporate technology changes into this standard. The Team recently received approval from OMB to proceed with revising this standard and a workshop was being organized in mid April to present and discuss the changes on FIPS 201-1. He reported on extensive research on iris detection and other possible solutions including raised physical bump to counter the problems for people who have unreadable fingerprints. While they are exploring the use of biometrics in cell phones, there is also the fear of the risks of malware.

Since Deborah Gallagher joined GSA about 7 months ago, she has been working on FICAM (Federal Identity, Credential and Access Management). Within FICAM, they developed segment architecture, use cases, created best practices for use cases and transition activities. There are twelve different use cases. Deb Gallagher prepared presentation provided the background scope, motivation, and goals of ICAM. The FICAM Roadmap document includes use cases, transition roadmap initiatives, implementation guidance, workplan progress, milestones, and concluded with the high points of OMB document M-11-11.

The Meeting was recessed at 5:30 P.M., Wednesday, March 3, 2011.

Friday March 3, 2011

The Chairman of the board reconvened the meeting at 8:10 A.M. Dan Chenok as the Chairman of ISPAB, thanked Lynn McNulty and Alex Popowycz for their services on ISPAB. ISPAB will certainly look forward to inviting them to future meetings.

NCCIC and Cyber Storm- Lessons Learned
Sean Paul McGurk, Director, National Cybersecurity and Communications, Integration Center (NCCIC)
Brett Lambo, Director, Cyber Exercise Program, National Cyber Security Division, DHS

NCCIC was established in October 2009. They have taken the physical facilities and combined them at the DHS Gleeb Road location. They are working closely with private sector and have also enlisted the aid of Carnegie Mellon and MITRE to draw up a framework that is translatable to industry. The initial step is to provide a set of analytical tools so as the intelligence agencies collaboration operation will be able to develop a common operation. Sean McGurk stressed the importance of information sharing – the law and policy landscape with sharing between government and industry and the relation to data streams. The goal is to have every sector represented and map with other centers in real time. The challenge is identifying each sector's central point. The team is working with administration to identify various challenges. Furthermore, the primary issues are 1) NSA and Cyber Storm team do not have access to certain data from DHS, 2) there are no common sets of tools for analyzing, and 3) culture integration.

Cyber Storm 3 was a very large-scale exercise that involved 3000 participants, seventy companies in the private sector, twelve international organizations and simulated testing set up in fifteen government facilities. When building the exercise, it is important to define end results and to focus on the objectives. It is essential to understand the relationship between the stakeholders and how the connection can be leveraged such as how the right side can break through the left side. It is also necessary to manage different perspectives – national and terrorists, and to manage dissemination of information. Although it is ideal to share data but it is challenging to keep up with the enormous amount of data coming through. The main objective of Cyber Storm is to find and build a National Cyber Incident plan. They wanted to exercise the incident plan and to design exercise controls and gaps through dynamite plays. The experts had identified vulnerabilities and they were looking for solutions to some technical problems. All participants took the exercise seriously. They had distributed findings to relevant groups and make modification to NCIC before sending the report to the White House. After which they will work on the broader after report to have it available to the public. The team cannot control all remedial actions but it will be internalized by DHS. Congressional staff was briefed post and pre exercise. The next step is to begin conceptualize Cyber Storm 4.

US Department of State- Update on Continuous Monitoring Activities

John Streufert, Deputy Chief Information Officer and Chief Information Security Officer, State Department
[PowerPoint presentation provided]

John Streufert started the discussion with FISMA 2.0 and nature of attacks of which 80% of attacks leverage known vulnerabilities and configuration management and setting weaknesses. In case of continuous monitoring, it is necessary to also to track each machine for vulnerabilities. He described what and how they are testing. They designed the structure according to SP 800-53, and for continuous C&A 2.0, and they focused on the library cost and changes. He mentioned that the scanner scanned every 3-15 days but they are working to increase the frequency to every 36-72 hours. He considered 'Brody's Best 5' as the five best practices of Continuous Monitoring – know the boundaries of the enterprise; identify the devices on the network; know the configurations settings; monitor who are accessing the systems; and what those individuals are doing in those systems. Finally, John Streufert maintained that the Continuous C&A Process should perform security more effective in real time and not just provide a snapshot in time.

IG Panel

Andrew Patchan, Assistant IG for Auditing, Federal Reserve Board of Governors
Louis King, Program Director, DoT
Brett Baker, Assistant IG for Audit, NSF
[PowerPoint presentation provided]

Andrew Patchan
Andrew Patchan described the OIG responsibilities under FISMA and that FISMA provides a structured process for assurance of information security. When conducting OIG FISMA reviews, they combined information security structured processes with control effectiveness metrics. In relation to NIST Maturity model, OIGs recognized the need to measure the maturity of agency information security program policy and procedures.

Louis King
Louis King recommended the following changes to FISMA – 1) either legislation or OMB needs to clarify authority of CIO and CISO to ensure responsibilities align with authority; 2) establish statutory deadlines for FISMA results; 3) mandate assessment of agencies' information security maturity level based on NIST model; 4) require reviews of personnel performing information security work; 5) define inherently governmental roles, and finally, 6) require security clearances in the cyber security process. He also recommended that the board review the DOI report. He explained the reporting process provided to legislation and the hill staff and which he had proposed legislative changes. In conclusion, Louis King explained audit versus evaluation.

Brett Baker
Brett Baker presentation included description of the NSF agency overview, Research and Education Grants, FISMA review which is contracted to a CPA firm, and 2010 FISMA OIG report scores. There are fourteen NSF information systems and three contractor systems. He offered some suggestions toward the FISMA framework such as supplement OMB questionnaire with a narrative report; ensure FISMA and Financial Statement Auditors communicate results to each other.

Howard Schmidt

Howard Schmidt, Cybersecurity Coordinator and Special Assistant to the President

Howard Schmidt last visited the board two meetings ago. He introduced Naomi Lefkovitz who recently joined his office from FTC. Ms. Lefkovitz last spoke to the board on the subject of NSTIC at March 2011 meeting. She is currently working on the NSTIC implementation. Howard Schmidt stated that they relied heavily on Cyberspace Policy Review to develop National Strategy Plan and developing strategic plan to counter national incidences based on the National Incident Response Plan. They are analyzing feedback and status reports to determine how best to implement. They will continue to work with the communities and formulating partnership with private and public.

Cyber Storm 4 exercises coming up next year will be built on the feedback received. There are much work to be done in raising awareness of cyber threats and educating the public, and organizing Cybersecurity month. They have recognized that Cybersecurity month should be a yearlong event as they have yet to reach out to many communities. NIST NICE initiative plays a huge role and developing of many activities. In meantime, OPM conducted a government-wide survey to gather information for a competency model description for a job position in cyber security, cybersecurity career in the government, and what are the required skill sets. Howard Schmidt talked about the launch of Stop Think Connect Campaign and the activities that followed – campaign forums and newsletter. He was very encouraged by the fact the cyber citizen forums held across the nation were well attended and feedback was gathered. There will more forums to discuss best practices. He was concerned about coordination and how best to get visibility to ensure that there are no overlapping of effort. While he is looking to update security strategies, he is not moving to make new strategies.

National Strategy for Trusted Identities in Cyberspace (NSTIC) is a key building block in the national effort to secure cyberspace. Howard Schmidt talked about the four key points of the initiative, the compromise of user identity, vulnerabilities, and the search for ways to lighten the complexities. It is not a national identity card and it will not be mandate or required by the government. NSTIC should be led by the private sector.

In response to the Chair's questions on areas of focus and new challenges, Howard Schmidt emphasized the importance of keeping a clear guideline of authority, structure and making sure of continued coordination with the private sector. Lynn McNulty, member of the board, raised his concerns with federal budget trends affecting cyber security. Howard Schmidt affirmed that Cybersecurity is unlikely be put on hold because of budget issues.

Board Discussion

March 3, 2011
The board approved the meeting minutes for November 2010, albeit making a few minor changes. A motion was proposed by Lynn McNulty and seconded by Peter Weinberger.

Donna Dodson informed the board that Dr. Ron Ross of the Computer Security Division, NIST, has been accepted as a NIST fellow. She then talked about the new positions that will be open on the board as this is the last meeting for Lynn McNulty and Alex Popowycz. They will work on filling those positions very shortly. Donna Dodson said that she has invited 3 or 4 people to visit NIST to talk about joining the board in the future. Alex Popowycz expressed his appreciation to the board for the six years that he was member of ISPAB.

The board discussed dates for the next two meetings. The board decided on July 13, 14, and 15 as the next meeting dates and reserved October 19, 20, 21, 2011 for the meeting after July. The board discussed the presentations done by Fred Schneider and Peter Weinberger. Donna Dodson thought that the two presentations were very different. The board did not think it would be necessary to prepare a letter to OMB regarding research on security.

March 4, 2011
Board Member Lynn McNulty's term on the board ended at this meeting. Cita Furlani and Donna Dodson of NIST presented him with a Certificate of Appreciation from NIST. As Alex Popowycz had already left the meeting, a Certificate of Appreciation will be sent directly to him.

The board discussed the Agenda topics for the next meeting:

- Cloud Computing: How do we secure the cloud? What is the Government doing for securing different types of Cloud? Would like to see a panel of agency users, email cloud, private cloud. When is it appropriate to stay public/private? Why agencies use a private cloud? Cloud monitoring privacy.

- Discussion on CSD's Organization Panel (Donna Dodson)

- Concept of longer-term research priorities. Donna recommends inviting representative from MITRE, CSIA or DHS, and the possible panelists as Bill Newhouse, Doug Maughan, and Lee Badger, who has been working on some network measurement techniques.

- NIST NICE initiatives, Cybersecurity Awareness Activities - Ernest McDuffie, NIST NICE

- NSTIC Governance - Jeremy Grant, NIST

- Bruce McConnell to talk about Strategy Plan

- A representative from Howard Schmidt's office, DHS and NIST re. indepth study on cyber security

- FDA involvement in medical devices
- Mississippi State's success story on medical device – Brian Gouker to arrange the speaker/panel
- NYAID
- Attack device, various issues between devices and healthcare identity – Kevin Fu
- Fred Schneider's paper on cybersecurity policies

In addition, board members made the following suggestions/requests:

- Fred Schneider suggested that to have a discussion/presentation from FDA regarding FDA process.
- Brian Gouker suggested having someone from Mississippi State to discuss NIAAP.
- Fred Schneider suggested Kevin Fu to talk to the board about implantable medical device attacks.
- Joe Guierri suggested a discussion on NHIN.
- Fred Schneider would like to present his paper on Cyber Security Doctrine.

The meeting adjourned at 12:18 P.M., Friday, March 4, 2011.

ANNEX A

LAST	FIRST	AFFILIATION	ROLE
Abrahamson	Steven	GE Healthcare	Presenter
Adums	Michael	VA	Visitor
Baker	Brett	NSF	Presenter
Benitez	Maggie	NIST	Visitor
Brody	Bruce	New Cyber Partners	Presenter
Camm	Larry	Schweitzer Engineering Laboratories, Inc.	Visitor
Cole	Alma	DHS	Presenter
Conley	Sarah	Intermental Observers (Researchers)	Visitor
Davis	John C	Teknet	Visitor
Davis	Jerry	VA	Visitor
Dickson	Virgil	FDA News	Visitor/Media
Elliott	William	GE Healthcare	Presenter
Friel	Megan	VHA	Presenter
Gallagher	Deb	GSA	Presenter
Garcia	Mike	NIST	Visitor
Gardner	John	VA	Visitor
Gephart	Charlie	VA	Presenter
Grant	Jeremy	NIST	Presenter
Hale	Larry	GSA	Visitor
Higgins	Maureen	OPM	Presenter
Hoffensperger	Chris	Business Software Alliance	Visitor
Kerban	Segen	DOS	Visitor
King	Louis	DOT	Presenter
Lambo	Brett	DHS	Presenter
Lightman	Suzanne	NIST	Visitor
MacGregor	Bill	NIST	Presenter
Marino	Stacy	Booz Allen	Visitor
Martin	John	DHS	Presenter
Maxson	Peggy	DHS	Presenter
Mayfield	Harry	Lewis-Burke Associates, LLC	Visitor
McClure	David	GSA	Presenter
McConnell	Bruce	DHS	Presenter
McCormick	Jill	VA	Visitor
McDuffie	Ernest	NIST	Presenter
McGurk	Sean P.	NCCIC	Presenter
McKinney	Robert	EPA	Presenter
Miller	Jason	Federal News Radio	Visitor/Media
Myers	Phil	Unisys	Visitor
Nordenberg	Dale	Security Consortium	Presenter
Ozment	Andy	NSS/WH	Presenter

LAST	FIRST	AFFILIATION	ROLE
Patchan	Andrew	Fed Reserve Board of Governors	Presenter
Roundtree	Terence	GSA	Visitor
Schmidle	Rikki	Forrester Research	Visitor
Schmidt	Howard	WH	Presenter
Schwartz	Ari	NIST	Presenter
Sherrill	Lynette	VA	Presenter
Smith	Michael	SAIC	Visitor
Stanar-Johnson	Sandra	NSA/CSS	Presenter
Stine	Kevin	NIST	Visitor
Streufert	John	DOS	Presenter
Suh	Paul	BAH	Visitor
Tarbox	Andrew	Wave Systems	Visitor
Taylor Moore	Debbie	CyberZephyr	Visitor
Titus	Patti	Unisys	Presenter
Toledo	Luis	DOS	Visitor
Van Horne	Meghann	FBI	Visitor
Williams	Steve	EPA	Visitor