INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

Summary of Meeting
May 30, May 31, and June 1, 2012
NIST, 100 Bureau Drive, Portrait Room, Building 101, Gaithersburg, MD 20899

	Present:	
	Board Members	Non-Board Members
Wednesday, May 30, 2012 8:40 A.M. – 5:20 P.M. Thursday, May 31, 2012 8:40 A.M. – 4:30 P.M. Friday, June 1, 2012 8:30 A.M. – 1:00 P.M.	Dan Chenok (Chair) Chris Boyer Kevin Fu Greg Garcia Brian Gouker Toby Levin Ed Roback Phyllis Schneck Gale Stone Peter Weinberger Julie Boughn (participated via telephone)	Donna Dodson Matthew Scholl (DFO) Annie Sokol (DFO) Megan St. Clair (Recorder)

Wednesday, May 30, 2012

The meeting was called to order at 9:00 A.M. The Board members provided updates of their recent activities. The Chair thanked NIST for hosting the meeting.

FISMA and Joint Task Force (Presentation provided)[1]
Ron Ross, Fellow, NIST

Dr. Ross discussed the development of SP 800-53 Revision 4[2] and various appendices. The goal is to change how the publication is viewed with the emphasis to new cyber defense vision through continuous monitoring. New controls are added. In his presentation on cyber defense, he described processes, key elements, and dual protection strategies. He proceeded to update on SP 800-53 with key milestones, major drives, gap areas, expanded tailoring of the baseline, control enhancement naming, overlays, and assurance and trustworthiness. Ron Ross and his team have been working closely with many supply chain working groups so as to provide emphasis on supply

[1] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/may30_fisma_rross.pdf
[2] http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf

chain in the publication. Appendix E, Assurance and Trustworthiness has been completely revised and reworked, and Appendices D, F, and G are available for comments[3]. In response to question on how to measure continuous monitoring, Dr Ross stated that DHS and NIST are working on the appropriate metrics.

DIB Pilot and its Potential Application to Other Private Sector

Greg Garcia, (Moderator), Garcia Cyber Partners
Denise Anderson, Vice President FS-ISAC, Government and Cross-Sector Programs Financial Services Information Sharing and Analysis Center FS-ISAC
Scott Algeier, Executive Director of the IT-ISAC and President and CEO, Conrad, Inc.
Eric M. Hutchins

Greg Garcia as the moderator introduced the panelists and stated that he would like to see the DIB Pilot expanded to other private sectors.

Eric Hutchins illustrated the history of the collaboration effort in which he has been participating with DOD and Pentagon. The current challenge is it does not scale to nationwide unless an Intelligence driven model is built. He stated that he has the opportunity to collaborate internationally with Europe. As collaboration increases, there are tremendous successes in helping other agencies build resiliency. Eric Hutchins stated that intelligence is communicated after analysts are able to discuss through real time connection and activity. Information Technology Information Sharing Analysis Center (IT ISAC) is still waiting for an approved CRADA agreement. In the meantime, NCCIC is producing more detailed information than previously, but the release is still delayed.

There are some issues with DIB pilots: 1) DoD wants to limit who they could share the information with particularly not all of their customers are considered to be part of critical infrastructure. IT ISAC did not want to limit sharing information. There is a requirement in the pilot that companies are to share their information with the government. The government could examine the quality of information being shared and also how to share better information. Presently, they are not receiving the actionable information. NCCIC needs to improve internal collaboration, and to provide useful information to the community. There is a need for a Trusted Framework for information sharing.

Lunch time discussion with Dr. Patrick Gallagher, NIST Director

The Board enjoyed an informal discussion with Dr. Gallagher during lunch break. A range of topics were discussed but with a focused interest in international standards development.

[3] http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-53-Rev.%204

Automated Indicator Sharing

Phyllis Schneck, (Moderator), VP & Chief Technology Officer, Global Public Sector, McAfee
Robert Dix, Vice President, Government Affairs & Critical Infrastructure Protection, Juniper Networks
Peter Fonash, Chief Technology Officer for Cybersecurity and Communications, Department of Homeland Security
Ron Plesco, CEO, National Cyber Forensics and Training Alliance
Richard Struse, Deputy Director, Software Assurance Program, GCSM, National Cyber Security Division, DHS

Phyllis Schneck as the moderator of the panel, gave an introduction of information sharing in general and the progression of automation. Bob Dix discussed the element of an automated element in information sharing. Peter Fonash reaffirmed Bob Dix's points that a lot of issues are not technical. But there are a lot of technical issues such as the issue of automation to respond to automated attacks.

Ron Plesco covered the discussion on private industry sharing intelligence. Richard Struse is working with the government and private sector to find an ecosystem. He pointed out that information sharing is not a useful term as it means many different things to different people while the focus has been finding defense mechanisms to be shared. A lot of information is classified, which hinders progress.

There is a necessity to educate the public and for Americans to have a clear understanding of the relationship between security and privacy. It is important to help people understand that it is not about reading their emails or looking at their social network accounts but about getting valuable information shared.

Exploring the Future of Privacy for Federal IT (Presentations available)

Toby Levin, (Moderator)
Gerald Beuchelt[4], Principal Information Security Engineer, The MITRE Corporation
Jeannette M Wing[5], President's Professor of Computer Science and Department Head, Carnegie Mellon University (CMU)
K. Krasnow Waterman[6], Visiting Fellow with DIG, the Decentralized Information Group of the Computer Science and Artificial Intelligence Laboratory at MIT

Jeannette Wing focused her works on Trustworthy computing, programming languages and software engineering work and has been on editorial board of twelve journals. She discussed about the breadth of approaches from across Carnegie Mellon University (CMU) and provided samples of three things they are focused on including: auditing, government databases and maintaining consumer-centric. Included in her presentation were her students' works - first set is on Semantics of Use and Purpose; second set is on Languages and Software Architecture: Exceptions in Law and Patterns of Compliance; third set is on Outputting Sanitized Databases Using Differential Privacy; and fourth set is on Statistical Disclosure Limitation and the Challenge of Societal-Scale Data.

[4] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/may30_future-privacy-health-it_gbuchelt.pdf
[5] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/may30_privacy-research_jwing.pdf
[6] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/may30_playing-by-rules_kwaterman.pdf

Krasnow Waterman works with the Decentralized Information Group: The Decentralized Information Group explores the consequences of information on the Web: where it comes from, what happens to it, and what are the rules for using it. The goal is to build tools to help people control the policies governing information, and to build automated reasoning systems to help determine whether information used complies with policy. On the topic of privacy, she gave examples such as Hospital Records and the project that they are working. The sponsor of the project is the Department of Homeland Security, and the goal is to determine whether each use of data is/was permitted by the relevant rules for the particular data, party, and circumstance and decision on access control, audit, and other technology for real-time enforcement, retrospective reporting, redress, and risk modeling. The determination is 'Scenario Driven'.

Gerald Beuchelt's presentation began with MITRE, MITRE mission statement and MITRE's Focus on Health IT. The focus on patient-centric privacy leads to basic access control available today through limited privacy controls, web based privacy and access management.

The Road to Confidence in IT System Performance (Presentations available)

Gordon Gillerman[7], Director, NIST Standards Services, NIST
Barbara Guttman, Group Manager, Software Quality Group, NIST
Paul E. Black[8], Computer Scientist, Software Quality Group, NIST
Matt Scholl, Deputy Chief, Computer Security Division, NIST

Gordon Gillerman's presentation included the definition of conformity assessment, and the four major players are seller/manufacturer; purchaser/user; independent entity; and Government. There are standards for everything, and there are types of conformity assessment: Suppliers Declaration of Conformity; Inspection; Testing; Certification; Registration; Accreditation. There are also different types of assessments in very formal and simple forms. Certification can be expensive so it is only used when there is moderate to high product risk. Examples of each assessment are also discussed.

Paul Black, Software and Systems Division at NIST, leads the Software Assurance Metrics and Tool Evaluation (SAMATE) project. The project focuses on Static source code security analyzers, Static Analysis Tool Exposition (SATE), SAMATE Reference Dataset (SRD), and Vote tools evaluation methodology. The presentation also included Statistic Analyzers, which is used to check for bugs, Static Analysis Tool Exposition (SATE). SAMATE Reference Dataset (SRD), which is the program created to test the SATE.

The meeting recessed at 5:10 P.M., May 30, 2012.

[7] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/may30_conformity_ggillerman.pdf
[8] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/may30_road-confidence-samate_pblack.pdf

Thursday, May 31, 2012

The meeting resumed at 8:35 A.M., and the Board reviewed the discussion from yesterday, May 30, 2012. Donna Dodson, Chief, Computer Security Division, NIST, and Dan Chenok, Chair, ISPAB, planned to participate in a farewell event in honor of Howard Schmidt, ex-Board member, who was retiring from his position as the White House Cybersecurity Coordinator.

Cyber Security Assurance Program (CAP) - Red Team, Blue Team (Presentation provided)[9]

Don Benack, Program Manager, Cybersecurity Assurance, Federal National Security, National Cybersecurity Division, DHS
Rob Karas, Risk Evaluation Program Manager, National Cybersecurity Division, DHS

Through his presentation, Rob Karas discussed the importance of Red Teaming, which include the challenge of organizational thinking, unbiased view of network defense and security. The more realistic picture of security readiness includes exercises, role playing and announced assessments. The traditional Red Teaming incorporates testing the organization's intelligence, threat, physical security such as physical access to network and dumpster diving; institutional posture such as SOPs policies; and network security such as vulnerabilities. Rob Karas cautioned that organization could suffer from target fixation. The presentation further discussed the approach of Red Team vs. Blue Team. In conclusion, he presented the future of Red Team should focus on leveraging results from specific, actionable outreach projects and establishing an information exchange for Federal cybersecurity practitioners.

A-130 Project Outline/Template

Dan Chenok, Moderator
Karen S. Evans, National Director, US Cyber Challenge
Frank Reeder, Chairman, Council of Directors, National Board of Information Security Examiners

The Information Policy Circular was created by Frank Reeder and is revised every few years. The Appendix A3 is dedicated to cybersecurity. Karen Evans and Frank Reeder agreed to revisit the guidance on CyberSecurity as it is over a decade old. The end product due to be completed in the summer will be in the form of a white paper or report on the key area of concerns as well as the improvement opportunities. Continuous monitoring consumed a lot of discussion, and particularly that the Circular is just out of date is also a big concern.

There were a number of questions from Board Member relating to the system of record notices and relevancy to the task that they are trying to achieve, and whether HSPD7 was part of any discussions. Frank Reeder would like to check on the relationship between national security systems and non national security systems and to provide feedback to the board. Ms. Evan stated that through their research and activities in order to move from the model of compliance to actually showing results of managing risk or reducing risk, it is necessary to have a maturity model. The intention of this report is to present the development of a maturity model, which agencies could be evaluated individually so that they can be tested along a linear level. This could be easier for IGs to

[9] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/may31_cap-red-team-brief_rkaras.pdf

audit from a maturity model. They would like to move the maturity level into different security levels (low, moderate, high).

An Overview of NIST

Willie May, Associate Director of NIST Programs and Principle Deputy, NIST

Dr. Willie May, Associate Director of NIST Programs and Principle Deputy provided an overview of NIST including NIST's six laboratories include the Physical Measurement Laboratory, Material Measurement Laboratory, Engineering Laboratory, Information Technology Laboratory, the Center for Nanoscale Science and Technology and the NIST Center for Neutron Research. The NIST Laboratories collaborate with U.S. industry and universities to conduct measurement, standards and technology research that advance the nation's R&D infrastructure. The overarching goal of the NIST laboratory programs is to accelerate U.S. innovation, which is a major driver of economic growth and job creation. Following the presentation, the Board was invited to visit two separate demonstrations – 1) Trace Explosive Detection Research, and 2) Vision Science: Accelerating the Development and Commercialization of Solid-State Lighting.

A Comprehensive Approach to Key Management (Presentation provided)[10]

Tim Polk, Group Manager, Computer Security Division (CSD), NIST
Elaine Barker, Computer Scientist, CSD, NIST
Lily Chen, Mathematician, CSD, NIST
John Kelsey, Computer Scientist, CSD, NIST

Mr. Polk's presentation titled, *Goals, Assumptions & Cold Realities of Cryptography*, covered discussion on symmetric encryption algorithms, whereby an algorithm is secure if an attacker (given the algorithm and some ciphertext encrypted under an unknown key) cannot practically derive any information about the message (other than its length) or the key and for public key algorithms, an algorithm is secure if an attacker (given the algorithm, public key, and a signature or ciphertext) cannot practically forge a signature, decrypt a message, or obtain the key. He also discussed the multiple facets of key management problem and NIST's Key Management Standards and Guidelines. NIST's work in key management is on-going for more than a decade and while they experienced many accomplishments, the work is not finished. Cryptographic key generation algorithms are deterministic if you repeat the algorithm with the same set of inputs, the same "secret" value will be generated, one of the inputs is intended to provide the entropy needed to generate random values and when the entropy is insufficient, key generation algorithms produce weak keys. Tim Polk;s presentation also included Random Bit Generation (RBG) Specifications, Key Establishment Using Public Key Cryptography, and Key Derivation Functions, NIST Key Management "Mechanism" Specifications, Managing Key Materials, and Managing Transition. Donna Dodson stated that almost all Federal Agencies are running Key Management systems.

Action Item: The Board would like to maintain vigilant on the developments

[10] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/may31_key-mgt-overview_wtpolk.pdf

The NIST Beacon: Prototyping a Public Randomness Service (Presentation provided)[11]

Larry Bassham, Computer Scientist, CSD, NIST
Micheala Iorga, Computer Scientist, CSD, NIST
Rene Peralta, Computer Scientist, CSD, NIST

The NIST Beacon is a source of entropy for people to use as a trusted source. The architecture of the Beacon: random numbers but not secret numbers to be used by people for key materials. The Beacon has entropy sources in which to feed into the system, data analysis on these sources is first to be fed into a program which in turn perform crypto hardening and time stamp the values. It is next processed into a database and stores the values to a http server.

Larry Bassham explained that Beacon will broadcast full-entropy bit-strings, broadcast blocks of 512 bits per minute, sign and time-stamp each block, and link the sequence of blocks with a secure hash. He further illustrated a database snapshot with the database scheme columns. The database is currently only NIST accessible but will be put out on the web very shortly. Dr. Rene Peralta explained the purposes of the database including many forms of human interaction have moved from the meeting table to the Internet. Tim Polk discussed some of the future plans for Beacon, including Enhance user interface with REST design, Migrate database and web services to NIST public network, increase number and diversity of randomness sources, and collaborate with PML to integrate quantum noise sources. Ed Roback suggested that this could be a contest for college students or high school students to test a real system, and Tim Polk concurred.

National Supply Chain Risk Management Practices for Federal Information Systems, NIST IR 7622 (Presentation provided)[12]

Jon M. Boyens, IT Specialist, CSD, NIST

Jon Boyens explained that it has been big misconception that NIST Interagency Reports (IRs) are considered as mandatory. He then proceeded to explain the purposes and scope of NIST IR. Jon Boyens expanded the discussion to include guidance and recommended practices to manage supply chain risk to a level commensurate with the criticality of information systems or networks for the acquiring federal agency only. His presentation also discussed the changes to the second draft of NIST IR 7622.

Action Item: Model Language discussion for next meeting.

Updates on FIPS 201, Personal Identity Verification (Presentation provided) [13]

Hildegard Ferraiolo, Computer Scientist, CSD, NIST
David Cooper, Computer Scientist, CSD, NIST

Hildy Ferraiolo described updates included in the latest version of FIPS 201, Personal Identity Verification. The timeline aided in illustrating progress and next steps in updating the document - Resolve Comments on 2nd Draft FIPS 201-2; Deliver Candidate FIPS 201-2 to the Secretary of

[11] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/may31_why-the-beacon_rperalta.pdf
[12] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/may31_nistir-7622_jboyens.pdf
[13] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/may31_fips201-2-rfinal_hferraiolo-dcooper.pdf

Commerce for consideration; Announce Final FIPS 201-2 with Federal Register Notice; Publish Final FIPS 201-2 at csrc.nist.gov; Publish public comments and resolutions. It is necessary to explain the relationship between HSPD 12 and FIPS 201. Chain of Trust is the new approach introduced with this version in which cardholder enrollment records (including status of BI –NACI init/complete?) linked/chained via 1:1 biometric match.

David Cooper discussed the new approaches of renewal and reissuance of PIV cards as described in this latest version. A renewal process can be initialed whenever necessary. The process for issuance, reissuance, and renewal is simplified through an automated biometric match. In addition, an introduction of an iris based match for those who cannot provide a fingerprint. He talked about new requirements including; Digital Signature Key and Key Management Key; and the UUID (The Universally Unique Identifier). PIN Reset needs to be done remotely with the use of General Computing Environment (desktops, laptops, etc).

The meeting recessed at 5:20 P.M., Thursday, May 31, 2012.

Friday, June 1, 2012

The meeting resumed at 8:15 A.M.

E-Gov Update

Lisa Schlosser, Deputy CIO, Federal Government, OMB - joined on the phone.

Ms. Schlosser talked about Howard Schmidt's retirement and Michael Daniels from OMB will be assuming Mr. Schmidt's responsibilities. Lisa Schlosser will continue to focus on FedRAMP, TIC, Identity Management and continuation of Einstein. Michael Daniel's main focus will be Identity Management and NSTIC. The next evolution is directed at Digital Strategy[14], for which a document[15] was released. In the document *Building a 21st Century Platform to Better Serve the American People*, describes a common approach to security. The Digital Strategy falls under three ownerships, DoD, NIST and OMB in which each is trying to get everyone involved including Government, Academia, and Industry. Efforts were also made to reach out to members of the web community such as social networking sites. The next area of action is targeted towards the Federal CIOs and NIST on developing guidelines for digital privacy controls. Some tactical things that will need to be tackled are: how to insure secure identity management and to approach security controls differently. It is also necessary to address mobile app risks from app developers.

Public Participation

Debbie T. Moore, Founder & President CyberZephyr

Ms. Moore is an Independent Consultant to help industry work better with government and she tries to connect pieces where needs to be connected. She presented three topics: RVA, ENISA, and Privacy's, 'right to be forgotten'.

Legislature Updates

Matt Grote, Senate Homeland Security and Governmental Affairs Committee

Matt Grote has been working on the Cyber Security legislation, and a new proposal was released this past February, with much focus on critical infrastructure protection. He talked about the new bill, the FISMA Reform, Critical Infrastructure protection. Some companies did not pay much attention to security and some are getting it right. Agencies will need to perform risk assessments instead of threat assessments.

[14] http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html
[15] http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf

Highlights of New Federal Guide to Privacy and Security of Health Information

(Presentations provided)
Kevin Fu, (Moderator)
Kathryn Marchesini[16], Office of National Coordinator for Health IT, Office of the Chief Privacy Officer, HHS
Deven McGraw, Director of the Health Privacy Project at CDT
Ross Koppel[17], Ph.D. University of Pennsylvania Sociology Department Faculty
Kevin Stine, Group Manager, CSD, NIST

Kathryn Marchesini discussed setting policy to building privacy and security in Health IT. The reasons to create privacy and security include Good business practice for those adopting EHRs, assistance with qualifying for CMS Medicare and Medicaid EHR Incentive Program – meaningful use, assistance with legal compliance and that it is just the Right Thing to Do – Establish Patient Trust. The challenges in creating the culture include providers and staff have little understanding of new technology and privacy and security issues, and vendors may assume providers/staff understand privacy and security and are not adequately trained. The guide, 'Guide to Privacy and Security of Health Information', was released February 2012. Some training materials including a series of Security Training Video Games are scheduled for release in summer. There are a lot of policy challenges that are difficult to resolve and there are many guidance available. Smaller providers do not have expertise and would rather be told what to do.

The most common request for Health IT is 'What is my Password?'. There are so many passwords needed that there is proper password protection as passwords are being posted in plain view. The barcodes needed to access patients' information are kept in nurses' pockets instead of attaching to actual patients.

One recommendation for ONC is to expand the guidance for risk assessment or to make available a few NIST resources noted in the guide. There are a number of resources available at NIST such as outreach program for small businesses led by Richard Kissel, NIST. There is a need for basic awareness for the staff. National Center for Cybersecuity of Excellence (NCCOE) will examine use cases in the Health IT as well as electronic health records. About a year ago, NIST started a project, HIPPA Security Rule to help show a better understanding of the HIPPA Security Rule. NIST has had over 10,000 downloads of that since around thanksgiving time.

NSTIC Updates

Jeremy Grant, Senior Executive Advisor for Identity Management, NIST

Mr. Grant updated the Board on a formal Federal funding opportunity, which was in March. NSTIC received twelve proposals and a public announcement of the award will be released in a couple weeks. The fund is for a 24-month period. It will include setting up as a <dot>com or <dot>org. The target date if they get the award made should be the end of July. There is a Steering Group organized in a two tiered structure. International coordination is to play a huge role for the committee. A Stakeholder event organized at the White House was well attended by senior leaders from eBay, Aetna, among others. There was a really compelling discussion on why NSCTIC adds

[16] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/june1_privacy-security-guide-culture-for-ispap_kmarchesini.pdf
[17] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/june1_hit-workarounds-in-security_koppel.pdf

value to ecosystem. It is anticipated that the steering group will be like the constitutional convention, and they have yet to set the start date. Jeremy Grant would like to see from the first meeting, a work plan on what needs to be worked on in the next months/year. They know who is interested in the steering group, Chairs have been elected and there is a nomination process. He would like the Board to nominate an interested party.

SEC Security Breach Notification

Jacob Olcott, Principal, Cybersecurity, Good Harbor Consulting

Mr. Olcott stated that they are seeking ways to promote usage Cyber Security for consumers. These are issues that should be considered by not only by Corporate Its but also by corporate executives. The focus is how to change the behavior in companies to stop the bad situations. There are two thoughts: by regulating companies, or leave it to the open market to work out the approach. There are certain elements in the corporate environment that are regulated, but things are being exploited. There was a briefing on the cyber threat and Senator Rockefeller heard about a huge breach on a large company, but it seems people are not concerned.

Securities Exchange Commission (SEC) is tasked with the role as the information enforcer. Companies today have different ideas of priority of a breach. Staff Guidance defines what companies are required to do. The guidance also advises on how to manage your cyber risks without disclosing anything to your investors. International Community, particularly the international investment community, is very interested in this guidance.

NIST Updates (Presentation provided)[18]

Donna Dodson, Chief, Computer Security Division, NIST

Donna Dodson updated the Board on recent NIST Draft publications and internal activities. The Board members were presented with the latest Computer Security Division Annual Report. She also reported on the Botnet Workshop held at NIST earlier in the week and the Kickoff workshop coming up for the new NCCOE.

Board Review/Discussion

1) FISMA and Joint Task Force, discussion as presented by Dr. Ron Ross – no further action is required.

2) DIB Pilot and its Potential Application to Other Private Sector, panel discussion – the Board agreed to invite the Director of the NCCIC to participate at the next ISPAB meeting for a follow-up discussion.

3) Lunch time discussion with Dr. Patrick Gallagher, NIST Director, Under Secretary of Science and Technology – Dr. Gallagher asked the Board to consider standards and regulations, and international regulations as part of the Board's discussion. The Chair suggested to include the discussion in future board meeting.

[18] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/june1_nist-updates_dodson.pdf

4) The Board will draft a memo of appreciation to Howard Schmidt of his dedication and contribution to the board.

5) IG Issue: vendors have been approved by OMB to produce the PIV cards.

6) Tony Sagar will be retiring from NSA.

7) The Board looked forward to welcoming Chris Boyer, a new ISPAB member to come to the board next meeting. Chris Boyer works in Policy and Technology Space for AT&T (the appointment letter was officially signed on June 11, 2012).

8) Donna Dodson observed that the Board is working effectively. Many of the Board's recommendations through letters and white papers are benefitting the whole government.

9) After more than six years, Dan Chenok is retiring from the Board as the Chair and member. The next meeting will be his last meeting. Phyllis Schnek and Matt Thomlinson have agreed to take on leadership of ISPAB. Donna Dodson is seeking clearance from NIST legal on these appointments.

10) Peter Weinberger proposed the motion to approve the meeting minutes for February 2012, and Toby Levin seconded the motion to approve the minutes.

11) Phyllis and Greg drafted bullet points for a recommendation letter on Automated Indicator Sharing. Toby Levin and Greg Garcia motioned to formulate the bullets into a letter. Motion approved by the Board.

12) To include the following topics/panel for next/future meeting: a Privacy Research Panel with focus on Consumers reaction and thoughts, and executives who are not cyber people; FedRAMP Updates; Privacy enhancing tools; Data loss prevention issue (Toby is to moderate); GAO & Medical Devices (Kevin Fu, moderator); NSTIC Update, Model Language, and Ethics Discussion.

13) Next meeting is agreed to be October 10, 11, 12

Meeting adjourned at 2:35 P.M.