Information Security and Privacy Advisory Board (ISPAB)

Summary of Meeting

George Washington University
Cafritz Conference Center
800 21st Street, Room 413-414
Washington DC

March 22 - 23, 2007

March 22, 2007

Board members attending in person were Dan Chenok, Brian Gouker, Joseph Guirreri, Susan Landau, Rebecca Leng, Lynn McNulty, Alexander Popowycz, Leslie Reis, Philip Reitinger, Howard Schmidt, Fred Schneider, and Pauline Bowen as the Designated Federal Official. Unable to attend were Jaren Doherty and Lisa Schlosser. Dan Chenok chaired the meeting and board members introduced themselves and reported on their current activities. Phil Reitinger, Microsoft, provided lunch for board members and snacks for the public on Thursday. NIST attendees included Jim St. Pierre, Curt Barker, Liz Chew, and Donna Dodson. Note takers were Peggy Himes and Annie Sokol, NIST. Lynn McNulty volunteered to brief the board on trying to get reclassification of infosec employees. Brian Gouker volunteered to present on NSA Best Practices. Dan reviewed the agenda. Phil Reitinger noted that the NSTAC had a Task force on emergency communications, for purposes of ISPAB coordination. Rebecca Leng noted that GSA had closed some external support for HSPD 12 activities; Rebecca also discussed the future of the President's Management Agenda as a driver for FISMA and whether the Board should address this. Pauline introduced Annie Sokol as the new ISPAB assistant.

NIST Briefing/NIST Metrics Project

Curt gave an informal update. He announced his retirement in early May and introduced Donna Dodson as his acting replacement. He mentioned a memorandum from Karen Evans, OMB, which was sent to the CIO Council to encourage particular security controls which the agencies should be using. Curt said the Checklists are available on the NIST Computer Security Resource Website (www.csrc.nist.gov) under Checklists. The National Vulnerability Database has expanded by adding The Security Content Automation Program (SCAP). Dan clarified particular implementations are not required.

HSPD-12 – Curt said there has been a protest on the integration and this caused a recess on activities although it did not change deadline dates. He reported there have been a small number of PIV cards done to date. Curt Barker said there has been more action on legacy systems. PIV space involves federal workers in HSPD12 but private industry is involved with port authorities. NIST is only providing advice on mechanisms but not involved in any formal effort. There are a number of ISO standards and they are working on and looking at identity management issues. Dan recommended looking at activities to link with other ID schema, including driver licenses, the EC card activity, E-PASS, TWIC, Real ID, and Registered Traveller, and the healthcare space looking at the possibility of a healthcare card.

As to what was NIST doing about laptops, Curt reported the Computer Security Division was in the process of installing encryption on all laptops and their security goes beyond the NIST standards but did not have recommendations for other government agencies. Curt noted that OMB and GSA may be involved in a Smartbuy activity involving laptops.

NIST ITL Security Metrics Activities

Curt Barker reported that theoretical foundations of cyber security metrics and individual measurements in some cases are difficult and predicting behaviors under composition are still more difficult. He reported

on the research activity of the initiative in cyber security on discrete mathematics, information science and applications. He said the Math Division, Ron Boisvert, ronald.boisvert@nist.gov, has the lead on this initiative. They are doing basic research on security metrics and will be interacting with the academic community and other department agencies. A separate effort shooting at short term goals is measuring network security using attack graphs. Curt reported they want to marry the National Vulnerability Database (NVD) Database and the Checklists so it will be one stop shopping. Steve Quinn is the point of contact, Stephen.quinn@nist.gov and was mentioned in the Karen Evans memo. Dan Chenok said the ISPAB Board is interested in hearing the progress. Curt reported that SP800-55 and SP800-80 are being merged into one document.

Liz Chew discussed the NIST Security Seminar Series. She reported the first in the series was held on January 10th and attendance was limited to federal CIOs, IGs, CISOs. Approximately 500 attended. Ron Ross spoke on lessons learned and Marianne Swanson spoke on SP800-53. Panelists provided their view of FISMA implementation and Rebecca Leng was the IG on the panel. A similar workshop was held on Feb 1st with the same speakers except Russell Rau, an IG for FDIC, replaced Rebecca Leng. There were about 300 attendees and it was open to support contractors as well as CIOS, IGs, and CISOs. The workshop goal was to share knowledge on best practices and to bring IGs, CIOs, and CISOs in the same audience to hear the same thing at the same time. Rebecca Leng said people doing the auditing and the people being audited found value in communication by attending this meeting.

Pauline Bowen discussed the article in GCN on NISTIR 7359, titled *Information Security Guide for Government Executives*. Pauline said NISTIR 7359 addressed five questions.

1. Why do I need to invest in information security?
2. Where do I need to focus my attention in accomplishing critical information security goals?
3. What are the key activities to build an effective information security program?
4. What are the information security laws, regulations, standards, and guidance that I need to understand to build an effective security program?
5. Where can I learn more to assist me in evaluating the effectiveness of my information security program?

Susan recommended to Pauline that the CSRC website reflect the streamlined nature of the NISTIR. Dan said the ISPAB Board would be more than willing to review and suggested the Presidential Council be informed about the Guide, and recommended affirmative outreach to disseminate this activity.

In answer to an earlier inquiry from Phil Reitinger, Jim St. Pierre reported Cita Furlani is very connected with NITRD (National Information Technology Research and Development). Donna Dodson, Acting NIST Computer Security Division Chief, asked the board to provide input in the selection process for the new division leader. Dan thanked and wished Curt Barker well in his retirement and thanked Liz Chew and Donna Dodson for coming down.

<u>NIST Activities on IPv6 (Internet Protocol version 6)– Stephen Nightingale</u>

Dan Chenok said about a year ago there was a briefing to the ISPAB Board on IPV6 and thought it was a good time to have someone come back. Stephen Nightingale of the NIST Advance Network Technologies Division reported the comment period for Draft USGIPv6 – v1.0 closed on March 2, 2007 and comments received included policy as well as technical concerns. Stephen's discussion went into a walk-through of the Profile, the differences from other Profiles (IETF, DoD, IPvready,) major comments received, other procedural consequences, testing arrangements, and harmonization.

Stephen reiterated NIST is not making policy but are determining technical requirements. Carol Bales is the OMB point of contact. The profile should insure interoperability, enable secure operation, and protect early investments. Stephen said IPv4 is the network today and June 2008 is the staging point where OMB is able say the government can do business in IPv6. There is concern that code will not operate in IPv6, but Stephen said the common sense approach is being taken. IPv6 is a different protocol from

IPv4. There are three types of devices for sub profiles – host profile, router profile, and network protection device profile. There are 12 functional categories of capabilities.

Dan questioned what the document is trying to do. As he (Dan) understands it, the scope of this document basically helps one know the specifications and requirements. The IETF (Internet Engineering Task Force) standards are very general and the industry can do what it wants with it, no timeline. Stephen said a testing program is being discussed and there will be a public meeting to address what a testing program should and will look like. OMB will make the determination.

Dan asked if there are two different requirements, the DoD side and the IPv6 specifications? Stephen said there are some concerns but DoD always defines itself for specific requirements – there will be differences. Mr. Nightingale reported they received over 400 comments and areas of concern were on policy application. OMB and GSA are in the throes of hatching a FAR clause that will depend on the NIST profile and testing recommendations. Calls for Industry interaction may lead to a government organized "Industry Day". There is a need for policy to include Revision Management beyond June 2008.

Howard Schmidt said the DoD difference is mainly the mail spec and cost issues. Howard also said Europe and Japan are using IPv6 in the next generation software being developed and there is concern that the US is behind the curve. Stephen Nightingale said we need interoperability, conformance, and an approved products list (APL) and the next steps are public meetings, NIST recommendations to OMB, and an establishment of a testing program and APL.

Dan thanked Stephen for his patience in answering the numerous questions.

The lunch break is until 1:10pm. Dan thanked Phil Reitinger and Microsoft for hosting the lunch and resumed the afternoon session.

<u>Ground Zero Restoration – Security COOP Panel</u>
Dave Rosenweig, Verizon
Robert Desiato, AT&T
Philip Reitinger, Microsoft

Phil introduced Dave Rosenweig, Verizon, and Robert Desiato, AT&T. They were involved in the disaster recovery after 9/11 and/or Hurricane Katrina.

Dave Rosenweig said his background is Bell systems network operations. Dave reflected with photos the devastation of the collapse of the World Trade Towers and the fire that took down 7 World Trade which damaged the Verizon building. He explained that the fire collapsing 7 World Trade did more damage to Verizon communications. There were 4 dial tone switches in that building, most towns have one. The east side of the 30 story building at 7 World Trade was torn off. About 200,000 dial tone lines were in the building and serviced residential and businesses. Battery backup and generators only lasted so long. The physical force brought in dirt and debris, destroyed cables, and flooded the basement. Asbestos was in the air. The plan was to clean up, apply power, and operate equipment. It was necessary to develop a plan at the moment with the people that were available. Ordinary people rose to the occasion. West Street rose above the disaster. Engines were not put back into the basement but on a higher floor level, however, fuel is still stored in the basement.

Robert Desiato said his report focuses on AT&T network continuity best practices after 9/11. Robert reported they never figured air traffic would be shut down over the US and now have a plan in effect to address this issue. They have trailers to respond, repair and recover. On 9/11/2001 the AT&T network handled 431 million call attempts. They set up a 'war room' in New Jersey and obtained a lot to set the trailers on. They were on 24-7 mode with shifts. Within 52 hours they were starting to switch calls that were coming into the World Trade centers. AT&T practice recovery of main offices regularly and they are training more people. During the recovery period federal agents asked that all visible logos be masked and covered. Emergency Communications Vehicles (ECV) are used in disasters to provide telephone service.

Dan said part of the ISPAB charter is to advise the government and asked for suggestions to pass along regarding recovery. Dave Rosenweig said well intentioned, well informed and prepared people are key. Robert Desiato suggested one of the major problems is not having a standard identification for first responders and suggested a nationally recognized badge. It is critical to have experienced and talented people as well as the ability to access restricted areas. Fuel is key issue to keep generators running and theft of fuel is a problem. POTS (plain old telephone service) is the recommended medium to have.

Information Systems Security Line of Business (ISS LoB)
Mike Smith, Department of Homeland Security

Mike Smith explained the background of the lines of business. LoB was initiated in 2004 with designed goals to support performance of the federal government, to establish mechanism and leverage with the existing workforce resources. The problems faced by LoB are security training, FISMA reporting, situational awareness & incident response. LoB's Overall Task Force recommendations include governance structure, phased implementation, common solutions in areas relating to FISMA reporting, emerging security solutions to the lifecycle, and closing security gaps by establishing Shared Service Centers (SSC). Each area has a high level implementation rollout schedule. Governance structure is comprised of Federal systems security governance board (FSSGB), Program management office (PMO), Shared Service Centers (SSCs), Federal agencies and departments (customers.) In answer to a Board question, Mike agreed that the IGs should be part of this governance structure.

Mike Smith affirmed that DHS defines standards and schedules for businesses who wish to provide services to the government. He said among the many accomplishments, LoB prepared guidance to agencies, established new and future work groups (Security Solutions for the Life Cycle) and the DoD product training link is available on the web. Mike Smith recommended inviting Brenda Oldfield (DHS) to speak on "Essential Body of Knowledge" on certifications.

Dan offered that Mike could call on the Board to give advice and recommendations going forward.

General Work Plan Discussion

Dan Chenok asked for a motion that the draft Summary of the Meeting from December 7-8, 2006 be approved. Susan Landau proposed the Meeting Summary be approved and accepted, which was seconded by board members. A correction to a bullet title from Network Effect of Real ID to "Security issues arising in inter-agency collaborations" will be incorporated. Dan reviewed the Action Items from the December 2006 meeting. Lynn McNulty requested Action Items be shared via email before the minutes are finalized for quicker reaction.

Action Items (see end for complete list)

Friday's coffee break will be provided by Leslie Reis and the John Marshall School of Law.

Possible June Agenda items were discussed (see end for complete list):

- Panel on the OMB memo regarding software configuration
- Panel on the Hill report card with Hill staff
- Panel on the OMB FISMA report
- Briefing on the NRC Privacy study (due out just prior to the June meeting)
- More detailed, deeper level presentation on NIST metrics activities -- The Board should carefully provide recommendation to NIST if the metrics are not established clearly or sufficiently so that guidance will appropriately drive R&D for the businesses.
- More thorough briefing on NIST basic research program on metrics

Alex Popowycz raised the needs at some level of understanding that transport of information between agencies and the private sector that will meet regulations, provide privacy and prevention of identity theft, and the mechanism to protect information.
Two-fold transfer information, e.g., healthcare, payroll, income tax. Who or What is the obligation for reporting a breach? Dan suggested a discussion panel on this subject
Susan we need to define our perimeter in order to be able to produce a concrete action by June meeting. Where and what are Federal govt's responsibilities in this area?

Alex agreed to lead a discussion of these issues the next morning.

March 23, 2007

The Board members attending in person Dan Chenok, Brian Gouker, Joseph Guirreri, Susan Landau, Rebecca Leng, Lynn McNulty, Alexander Popowycz, Leslie Reis, Philip Reitinger, Howard Schmidt, Fred Schneider, and Pauline Bowen as the Designated Federal Official. Lisa Schlosser joined the board for the morning session. Howard Schmidt and Leslie Reis, The John Marshall Law School, sponsored refreshment for the day.

Discussion on Data Protection
Alex Popowycz

This item was not included in the agenda for discussion but was added as a point of interest. Alex begun the discussion on "*Non-Public* Protecting citizen identifiable information through data protection mechanism" with an overview and problem statement. Alex raised the possibility of engaging a representative from Liberty Allliance to discuss the trust model involved in federated identity management. This is an internal discussion to decide whether the board should act in the form of submitting a brief recommendation on consumer data protection. Susan asked if there is a timeline and the achievable objectives from this discussion.

A number of action items were discussed and collectively recommended. Philip Reitinger offered to provide a report on network identity. The Board members were interested in understanding the framework and practical solutions used by other countries' governments. Alex Popowycz will distribute a list of links of such examples. Alex agreed to chair a panel for the June meeting involving Liberty and other appropriate rep, including Microsoft Card Space (Phil agreed to help with a speaker) and FIXS (Dan agreed to help).

Scholarships for Service
Lynn McNulty suggested that the board could use the scholarship of service program to get students to do research on behalf of the board as the board is unable to research on subjects and to provide the needed depth on issues that concerned the board. This could be set up as an internship through NIST. The board members could work with a NIST staff to monitor the progress. Lisa Schlosser, Pauline Bowen, and Lynn McNulty will work together to research on such an internship. Lynn will work with Lance Hoffman, Director fo the CyberCorps, on this initiative.

Emergency Response and Security
Although the board gathered a few ideas from the striking presentations from Verizon and AT&T, the board was unsure how best to use the lessons learned. One item highlighted was the important of communications in emergency planning. Philip Reitinger offered to work with Lynn McNulty to write to NIST enquiring about adequate guidance provided in the revision of NIST standards, e.g. 200 or 800-53 without entirely reworking the standards.

Robert Desiato, AT&T, suggested the necessity of Federal ID tags for first responders, after consideration, the board decided that the subject is not within the scope of this board.

Board Discussion of FISMA metrics and future directions

After the break, board members introduced themselves in acknowledgement of the presence of Adam Bordes, House of Representatives, who was present as an observer. Lynn McNulty began the discussion on the issue of FISMA and it successes, software assurance, Common Criteria, and product certification. It was stated that Common Criteria address software features well, but not underlying vulnerabilities – in other words, Common Criteria can improve quality in the face of known problems, but do not help confront unknown problems.. Howard commented that there is no concerted and harmonized effort to address vulnerability. Vulnerability is often narrowly focused on software and not widened to include vulnerability through accessibility. Discussion followed with identifying the known and defining the unknown, the measurement of vulnerabilities and threats; the Board identified 3 classes:

1) protection again attacks that are knowable, which can be addressed through tools
2) protection against attacks that are not yet known, which could be identified through better requirements definition and better coding in the underlying software
3) protection against customized attacks – this problem will always exist, especially around applications

Lisa and Rebecca maintained that the agencies are progressing well with FISMA, and that the board should focus on providing guidance on performance measures and addition areas of concerns to OMB. The larger risks may come not from software but rather from managerial and operational controls. This includes personnel security risk, where agencies would have greater efficiencies if the clearance process was more accurate in limiting system and information access to those with proper credentials and privileges – absent a sound process, agencies have had to spend additional money on work-arounds at the expense of other actions to reduce vulnerabilities.

It was noted that FISMA laid out a metric involving C&As, assessing threats and fixing weaknesses through POAMs Agencies made the initial heavy investment in the C&A process, and the new activities are more paper-based than improvement-driven. OMB guidance could now focus on the assessment of vulnerability, risk, threat, corrective action, and measure.

There was agreement that it would be desirable for the Board to suggest a framework of suggested measures and levels of risks that industry could use. Such a framework could include internal and external risks and threats at the technical, managerial, and operational levels. The metrics in this framework should include process measures such as, do vendors have continuous improvement processes and make use of 3rd party evaluations for COTS? At the same time, the government should avoid poor metrics that try to stop new sw vulnerabilities as this will not yield a sound return on the investment.

The Board returned to a discussion of how the procurement system could drive this framework – building off the suggestion in prior Board meetings that procurement specs may be the best available approach to measurably improving security for the government -- so that vendors are incentivized to offer reduction in vulnerability especially for the most serious threats. NIST could play a new role in providing guidance for such procurement activity. The FAR could require configurations in procurement responses, as well as SLAs that focus on delivering sound performance. This could be recommended to the Infrastructure Optimization LOB as requirements for desktop, network, and hosting environments.

Dan volunteered to draft a letter outlining what such a procurement initiative would look like, incorporating the above and prior considerations. This could also address grant activities in terms of building security, as well as privacy across contracts and grants.

Privacy Technology Project

Leslie Reis

Leslie Reis reported on her contact with Joanne McNabb and John Sabo of the DHS Privacy Advisory Committee. She planned on setting the rules for writing an initial white paper in April. At the meeting in June, she will be able to report on the status of the white paper. In response to Dan Chenok, Leslie could

not confirm if they would be able to put together a complete draft by June. Dan said that he would work with Leslie to determine how much progress could be made by June.

Security Issues arising in interagency collaborations – Panel discussion
Diane Davidowicz, NOAA, Valdis Kletnieks, Virginia Tech, Sean Donelan, Akamai Technologies, Martin Lindner, CERT, Susan Landau, Sun MicroSystems (moderator)

Dan Chenok introduced the panel and explained the background for assembling this discussion. The perimeter of discussion based on the security issues arise from interagency collaborations and security risk so as to gather information to provide guidance to OMB.

Diane Davidowicz is the Project Manager of the NOAA Computer Incident Response Team (N-CIRT). The N-CIRT is part of the NOAA Office of the CIO (OCIO). In her role as project manager, she is responsible for all coordination concerning information technology (IT) security incident response and remediation within NOAA. She is responsible for communicating IT security related information with outside organizations such as law enforcement, Department of Commerce (DOC), United States Computer Emergency Readiness Team (US-CERT), the Computer Emergency Response Team (CERT) Coordination Center at Carnegie Mellon University and with other IT security organizations both in the private, non-profit, and commercial industry. In addition, she and the other team members perform computer forensic analysis, planning and execution of remediation activities, and reporting. The N-CIRT also conducts IT security audits, provides IT security consultation, and advises on IT security policy.

Diane maintained that NOAA is most concerned with accessibility of data on a timely basis and availability of accurate information. NOAA collaborates daily with many different organizations, agencies, private and public sectors, and is constantly gathering and compiling data to be used by various groups, and this activity is increasing tremendously each day, each year. Obviously, there are intentional and unintentional malicious attacks on the system, but on most occasions, the problematic activities are related to managing traffic to access the information in NOAA.

Valdis Kletnieks is a Computer Systems Senior Engineer in the Networked Storage and Backup Group, where his work is mostly focused on day-to-day operations and developing Best Practices for a fairly large network of essentially untrusted end-user machines. In this capacity, Mr. Kletnieks handles a wide range of different data and visibilities accessible with no identity management to minimize exposure and operate very much on “trust” basis as the best approach to get things done. Communication is generally through adhoc basis.

Sean Donelan, Director-Network Strategy at Akamai Technologies, Inc. He has extensive experience with inter-network peering, network reliability and disaster recovery. Akamai delivers 10%-20% of all Internet traffic with a pervasive platform in 71 countries and nearly 1,000 networks designed to survive most severe Internet storms. Before joining Akamai, Mr. Donelan was the SBC (now known as AT&T) Internet security manager, where he was responsible for network infrastructure security of SBC’s commercial Internet services for over 8 million residential, business and government customers. He served in a variety of positions, from database programmer to senior network architect. He was responsible for building a nationwide backbone network that provides Internet, inter-library loan and database services to more than 3,000 libraries. Mr. Donelan received his B.S. in computer science and psychology from Vanderbilt University in May 1986.

Martin Lindner is a senior member of the technical staff in the Networked Systems Survivability Program at the Software Engineering Institute (SEI) and is focused on providing technical support and expertise to U.S. government agencies. In his previous role as the team leader for the incident handling, Lindner was responsible for overseeing and processing all the security incidents reported to the CERT/CC. Lindner worked with government agencies, other CSIRTs, vendors, ISPs and security experts to understand and limit the impact of malicious Internet activity. Lindner lead the cyber investigation of the August 14, 2003 Northeast power outage and had a lead role in designing national and international cyber exercises including Livewire and Cyberstorm. Prior to joining the SEI, Lindner worked at the University of Pittsburgh for 18 years, where he held numerous positions, including manager of desktop services and

network manager. As the manager of desktop services, Lindner was responsible for all aspects of the PC desktop operations for the university. As the network manager, Lindner designed and implemented the tools used to control, manage, and study the university's network.
Lindner teaches Internet Security at the Carnegie Mellon University Heinz School.

Sean indicated that networked systems requiring computing collaboration were increasingly being run by "clearinghouses" on open networks, and that the apps layer engineers don't think about security in the clearinghouse – examples were the NLETS for law enforcement, Public Health and Infonet for health care, and the Interlibrary Loan system. Also there are few rules addressing the roles of these clearinghouses to protect security in the apps and data that they coordinate, and few resources that address interconnection. Additionally, the Panel noted that multiple players lead to a problem where no one owns the ultimate security of the system

Martin indicated that the government has plenty of rules, and it is not necessary to add any more new rules. Instead, we should review the existing rules such as NIST 800 and the DITSCAP, and emphasize those that are most applicable. With enforcement of the proper regulations and policies in place everyone will be able to function independently.

Diane stated there is a definite drop in incidents since the implementation of FISMA. Government metrics focus on detection, but Martin asserted the metrics mentally toward compliance, i.e. human behavior. But who is enforcing compliance? There are millions of computers being compromised but users are unaware of the intrusions. While government agencies are increasing reporting of intrusions which could be due to increasing awareness. Yet, the incentive awarded for reporting that could explain the increased reporting. The panel members stressed that FISMA has brought attention within the Federal Government to cybersecurity, which had previously been much neglected. Simultaneously, agencies following these mandates have become more focused in "compliance" and little on "security." Many agencies lack resources to address and comply with FISMA requirements.

The panel made several recommendations for inter-entity collaborations of this type:

- better enforcement of existing rules
- keep track of what data are leaving a system to prevent information sharing from going out of control
- address the clearinghouse problem

Susan Landau suggested that there should be an agenda item to discuss the clearinghouse issue.

<u>Government Identity Projects and Real ID – Getting to know you; Getting to know ALL about you</u>
Dan Combs, Global Identity Solutions

Dan Chenok introduced the speaker, Dan Combs, President, Global Identity Solution, member of the board of the E-Commerce Coordinating Council and Chair of the Federated Identity Workgroup and formerly the Director of Digital Government for the State of Iowa. Dan Chenok explained that board was specifically interested in whether the Board could make a positive contribution to the regulations that the government has issued. Dan Combs proceeded to provide the background on Real ID (Real ID Act of 2005.) The basis for developing Real ID includes: to improve privacy and security, help protect citizens and provides tools for self protection, improve identity functions, and integrate identity functions into wide range of commerce, interactions and transactions for government and non-government participants. DHS is the responsible administrative agency to develop the rules. Information/discussion can be found on the ACLU (American Civil Liberties Union) website – [**ACLU Issues Real ID "Scorecard," Checklist Provides Framework For Evaluation of Upcoming Regulations**]

Dan Combs believes that Real ID will be replaced by some kind of bill to help fix the identity gap, and that this problem is a multi-generational one. Real ID missed several factors including governance, the business model for data sharing, privacy, and system security. Clearinghouses would likely be used to

accomplish the transactions required by Real ID, where the Government makes systems relying on presumably accurate data.

Discussion during the presentation dictated that the board should advise on privacy, transparency and systems security, and address the board's concerns to OMB. The Board recommended a short letter as a public comment, recommending that DHS address these issues in the final rule to be consistent with OMB policy. The notion was proposed Lynn McNulty and seconded by Susan Landau

Action item: Lynn McNulty is to work with Dan on a comment from the Board.

Public Participation
Jessica Gulick, SAIC, requested discussion on work product and work flow issues relating to many people are telecommuting nowadays especially employees handling PII and SCU.

- There is NIST guidance on federal rules on security breach?
  - encrypting of computers, employees are not allowed to have information relating to PII and SCU while telecommuting.
  - Policies deviate among agencies.

Administrative and Upcoming issues:

Action Items:
- Forward Board members a copy of the OMB memorandum on software – Rebecca Leng forwarded it on 3/22/07
- Dan is planning to discuss the ISPAB budget with Cita M. Furlani, NIST ITL Director – both what the budget is at present, and how the Board can identify its request for the next Budget cycle (FY 09)
- Dan to meet with Hill House staff as a follow-up to their interest in the Board.
- Pauline/NIST to share the Executive Guide, NISTIR 7359, with the President's Management Council.
- Lynn is to prepare a letter pertaining to COOP & COG
- Lynn to work with Lance Hoffman on options for engaging Scholarships for Service
- Dan to draft a letter on procurement and metrics
- Lynn and Dan to work on public comment around Real ID.
- Leslie to continue working with DHS Committee on Privacy Technology white paper
- Dan to follow up with Mike Smith to determine if the Board could be of further assistance to the ISS LOB
- Pauline was asked to get a copy of the annual report on FISMA performance.

Potential speakers at June or future meetings (to be prioritized based on Board strategic focus areas, and scheduled based on availability):

- Dr. Jeffrey
- Hilary Jaffe, OMB (Privacy)
- Greg Garcia will be briefing the board – Board members suggested to provide suggested topics of interest with invitation
- Sallie McDonald – possible September 2007 meeting
- Robert Cresanti, Under Secretary of Commerce for Technology, National Communications System – to schedule for September 2007 meeting.
- Brian Gouker, NSA, offered to talk about NSA and its services. He will also check on the availabilities of the relevant people who will be able to give presentation at the future meeting.
- Brenda Oldfield, Brenda.oldfield@dhs.gov, 703-235-4184, to speak on DHS "Essential Body of Knowledge."
- Panel on the OMB memo regarding software configuration

- Panel on Liberty Alliance and similar organizations around federated identity and government involvement in consumer data protection
- Panel addressing policy and technical integration of various ID management activities.
- Panel on the Hill report card with Hill staff
- Panel on the OMB FISMA report
- Privacy Technology white paper update
- Briefing on the NRC Privacy study (due out just prior to the June meeting)
- More detailed, deeper level presentation on NIST metrics activities

- Susan Landau suggested that there should be an agenda item to discuss the clearinghouse issue.

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting.

Daniel Chenok
ISPAB Board Chairman