Information Security and Privacy Advisory Board (ISPAB)

Summary of Meeting

George Washington University
Cafritz Conference Center
800 21st Street, Rm 101
Washington DC

December 7-8, 2006

December 7, 2006

Board members attending in person: Dan Chenok, Brian Gouker, Joe Guirreri, Susan Landau, Rebecca Leng, Lynn McNulty, Leslie Reis, Phil Reitinger, Howard Schmidt, Lisa Schlosser, Fred Schneider, and the Designated Federal Official, Pauline Bowen. Alex Popowycz teleconferenced for portions of the meeting. Jaren Doherty was unable to attend. Dan Chenok reported by phone for the beginning of the meeting. Peggy Himes transcribed the minutes. Dan thanked Pauline for setting up a meeting with Cita Furlani and Robert Cresanti next week. Susan Landau chaired the meeting in Dan's absence and welcomed new board members, Brian Gouker (NSA), Lisa Schlosser (HUD), and Phil Reitinger (Microsoft). They briefly introduced themselves as did the other board members.

The press was represented by the Washington Internet Daily. There were 16 members from the public in attendance.

The National Finance Center and Hurricane Katrina

Gill Hawk, Chief Information Officer

Susan Landau introduced Gill Hawk, Chief Information Officer of the National Finance Center. Mr. Hawk talked about how the National Finance Center worked before Katrina and post Katrina and the lessons learned. The National Finance Center (NFC) is an operating agency in the Department of Agriculture providing payroll for government agencies, human relations services, and health benefits. The business continuity approach is three-tiered (1) business impact analysis, (2) disaster recovery plan, and (3) business continuity plan (restoring a business plan; service back on line).

Mr. Hawk reported the key to success is doing practice drills where employees go to the actual sites. They did not anticipate the evacuation of most of their employees. The implications of Katrina were long-term and communication was preset-up using 800-number conference calls to do command and control meetings. Subscription services were trucked to Philadelphia and Grand Prairie; 50,000 tapes were needed to back up their systems. Local telecommunications were mostly inoperable. Every shelter had a different database which made locating and deploying staff difficult. All mission critical systems were back up by Wednesday following the Sunday disaster declaration. Financial Management Services (FMS) performs the payment part through Treasury not NFC. The NFC contingency plan was not planned for the long-term; their contingency plan was short-term for up to 3 days. Their contingency plan is now long-term. Lisa reported HUD is coming out with a plan where all vacancies will be in one database. They used risk mitigation for migration from subscription service to "cold site". Just to declare a disaster costs a significant amount of money. The subscription service can be pulled if another disaster comes along.

To get away from subscription services the NFC is building their own datacenter. The New Orleans facility had generator power and the National Guard used their facility which kept it

physically secure. Once the NFC was able to go back to their facility, housing became a tremendous issue, as were family issues, schooling, local infrastructure, and health care. Citrix was used for securing remotely. Disaster recovery is built into the NFC day-to-day operations and employee's performance descriptions. When Philadelphia became the primary site, New Jersey became the back up site and was tested.

Lessons learned:

- all disaster recovery cell phones should be done using numbers outside the local area, having a well-drilled plan allowed for the basics to be accomplished with little intervention,
- subscription service is not the right model for an essential service provider,
- should not split a work force out such as mail delivery and the NFC is in the process of obtaining their own zip code,
- cannot assume infrastructure items will be there for you,
- A new primary facility data center will open replacing the subscription service locations.
- People who understand and believe in disaster recovery and Continuity of Operations Plan (COOP) make it happen.
- Plans have to account for your threats, the business requirements for COOP and the people side of things.
- Practice is the best teacher.

Currently, housing in New Orleans is scarce and expensive, medical services are limited, and communication has changed. NFC lost about 15% of the former workforce. Gill Hawk said given such an event, the best came out of people. Most disaster recovery plans focus on 30 days and being bumped was never thought of. Telecom dual reverse routed service was provided. Through practice drills, everyone knows where they are going and when and there is a third-party listed for contact information.

Susan asked Gill Hawk what can ISPAB do for you and Mr. Hawks asked the ISPAB Advisory Board to brief the CIO council about this activity.

Action item:

- The Board later discussed the fact that NIST guidance on security in contingency planning is out of date. Lynn McNulty agreed to draft a letter from the Board on the importance of updating these contingency plans, following a second panel to address the issues (see below)

Susan announced the public participation is Friday at 3:30.

Conversation with the National Institute of Technologies (NIST)

Cita Furlani, Director Information Technology Laboratory
Curt Barker, Chief, Computer Security Division

Ms. Furlani reported she has a full management team now. Upcoming projects are ID management, complex systems and the American Competitiveness Initiative (ACI). The government is still under a continuing resolution. Questions were asked about the election project and Cita reported NIST's role is to assist the election committee with technical guidelines but the election committee advises states. The NIST role is to bring technical expertise to the Technical Guidelines Development Committee (TGDC) specifically security and transparency issues and core requirements. TGDC is a committee comprising of election officials and other technical experts. The Technical Guidelines Development Committee's security and transparency subcommittee (STS) nuances made their report look like a NIST report; however, it was not a NIST document. The TGDC rejected the proposal on Monday but was approved after some

wording changed. Curt Barker reported the initial proposal used paper as an alternative for verification and resolution; the proposal that passed did not stipulate what format verification it would be in. The STS subcommittee made the recommendations, not NIST.

Lynn asked if NIST would get involved with lower level evaluations since national security was not evaluating below Level 4. Curt Barker said NIST is working with the community to figure out a way forward; it will not be a NIST laboratory. Lynn said the national security side has requirements to be certified but there are not places to verify lower level security assurances. Susan asked where NIST was going with hashing and the Cryptographic program. Curt said NIST established a workshop and are working with the community.

Jim Dray is the program manager working on new Identity Management project. The technical details under are under review and involves the ISO community. They are incorporating lessons learned into documents. Upcoming programs that may come to NIST's door include first responder communications and identity management consortium.

Susan asked what can ISPAB do for Cita and NIST. Cita had no specific requests now but is appreciative of the board's insights. The Board later discussed sending questions to ITL in advance of the future updates.

The board reconvened at 1:00pm with Dan Chenok assuming Chair responsibilities.

Inspector General (IG) Presidential Council Integrity Evaluation (PCIE) Panel

Rebecca Leng, DOT
Chuck Coe, Education
Judy Gordon, Commerce
Andy Patchan, GSA
Gale Stone, SSA

Important issues to ISPAB include privacy and to clarify how IGs score on FISMA. The IG community addresses three components (1) investigations, (2) auditing, (3) evaluation/inspection. The ISPAB heard complaints that certification and accreditation (C&A) is merely a paperwork exercise and that scoring would be different if an agency was reviewed by a different IG. Rebecca reported there are three issues the Inspector General panel was asked to provide input on:

- Have they witnessed improvement in security protection over information systems and data under FISMA
- What is their assessment of FIPS standards/guidance
- What progress has your agency made in protecting citizens' privacy

Special Agent, Charles (Chuck) Coe said it is important to urge the general public to adopt safe computing habits and practices. His agency's investigations identified no personal firewalls, out-of-date or no anti-virus software, and risky surfing habits (peer-2-peer and porn sites) as commodities on exploited systems. The stolen VA computer highlighted the need for privacy protections. FISMA is hard work but it is important and progress has been made because it is stressed at higher management levels. Resources will continue to be an issue in implementing. Lynn McNulty explained the DoD 8570 requires the quality of key security personnel have approved certifications. Chuck Coe said many IGs have the necessary clearances but clearances are lacking at the CIO level, and recommended more such clearances. By not having clearances, information does not come immediately and immediate information is needed to fend off attacks. He reported 62% of the PCIE member survey thought the IG's participation in FISMA brought about positive change in their agency and information assurance had improved significantly.

Judy Gordan, Assistant Inspector General for Systems Evaluation, spoke on her experience doing FISMA work at the Commerce Department. In early review, after the first review after GISRA, they found few systems had security plans to provide a foundation for security. She reported senior management gives greater attention to information security. When asked if Certification &Awareness was just a paper exercise, she responded if C&A is done right it helps ensure secure systems. Judy said the IG's follow PCIE quality standards, NIST and OMB guidance. They are sensitive to duplication; cost and burden can be addressed by common controls. Ms. Gordan recommended the Scholarship for Services hiring program; you get the people with the skills you need. Chuck Coe said IT auditing is a weak link in the cyber corps program and should be improved. Judy suggested NIST come up with examples of security plans.

Andy Patchan, Assistant Inspector General for GSA, said a working group had been working on a PCIE framework which will be available on the website. In answer to how IGs do reviews, he said it varies but is internal to the IGs. Rebecca said FIPS 199 and FIPS 200 should be the backbone for all IGs. He referenced NIST SP 800-100 and NIST SP 800-53. He suggested using a sample of systems rather than all systems. Rebecca stressed the importance of an IG staying independent. Mr. Patchan has seen improvements reporting under FISMA and doing certification and accreditation but they started out at such a low level.

Gale Stone, Deputy Assistant Inspector General for Audit for the Social Security Administration, reported SSA's information systems infrastructure consists of 20 major systems that process information from over 1,500 field offices. Most major systems are tied directly into the production of the financial statements. SSA hired Price Waterhouse Coopers (PwC) as an independent auditor to perform additional steps to evaluate its compliance with FISMA. OIG decided the additional contract vehicle with PwC would be an Agreed-Upon-Procedures (AUP) engagement. SSA and the OIG have met the FISMA reporting requirements every year. SSA improved it POA&M process, developed a systems inventory, and added staff to the CIO's office. FISMA has impacted SSA in getting security in the forefront. When asked about the insider threat, she said because of improved security awareness now the threat is reduced. Rebecca said FISMA has had a positive impact by bringing information security to a mainstream issue, officials have to sign, Congress issues grades, and IG audits all add to improvement.

During the discussion period that followed, the IGs indicated that a Performance Metrics Report would soon be released and that the Board would receive a copy. The Board recommended that the IGs brief again in December of 2007 to report on the next year's FISMA findings; Dan Chenok offered to brief the PCIE on the Board's activities.

Action items:

- Rebecca Leng will obtain performance metrics report from PCIE
- NIST will leave place on 12/2007 agenda for IG briefing on 2007 FISMA performance
- Dan Chenok will offer to Rebecca to brief the PCIE on ISPAB activities.

HSPD-12 Plan

Carol Bales, OMB

Date	Federal Agency Actions:
Oct 27, 2005	Comply with FIPS 201, Part 1
Oct 27, 2006	Begin compliance with FIPS 201, Part 2
Oct 27, 2007	Complete background investigations and issue PIV credentials for employees employed 15 years or less and contractors
Oct 27, 2008	Complete background investigations for all federal department or agency employees employed over 15 years and issue PIV credentials

Carol Bales reported the Executive Steering Committee has reached out to provide recommendations to physical security systems. What are the consequences if the dates above are not met - at this time there is internal discussions and she cannot comment. Current activities and plans are the validation of PIV credential (GSA to review topography of cards); OMB established an interagency working group to check minimum background (NACI) of foreign nationals; NIST prepared a draft document on PIV card technology which will be posted in the next few weeks; the steering committee continues to meet and provide recommendations. NICI background checks include database check, fingerprint check, and the State Department does a name check. The program manager is same for e-authentication and GSA is working on a business model. OMB may add progress toward HSPD 12 compliance to the management scorecard. When asked about Real ID, Ms. Bales said she is not really involved and cannot respond. The board suggested OMB look at forward-looking technologies rather than getting locked in. Carol also noted that the Foreign Nationals policy under HSPD 12 will be out for public review and welcomed the Board's input. She also said she could arrange for a meeting with the Executive Steering Committee if there were interest.

Action items:

- When available, NIST to distribute Foreign Nationals policy for Board review
- Dan Chenok will offer to brief the HSPD 12 Steering Committee

General Work Plan Discussion

It was announced tomorrow's meeting would be held in Room 308. A photo was taken of the ISPAB board for the NIST Computer Security Division Annual Report.

Dan asked for additional edits for the draft September06 minutes. Lynn McNulty reported a correction to page one, third paragraph - Dan Burton is not with the press. Lynn made a motion to accept the minutes as corrected, Susan seconded. The Advisory Board voted to approve the September 2006 minutes.

Tentative dates for upcoming board meetings:

March 22-23, 2007
June 7-8, 2007
September 6-7, 2007
December 6-7, 2007

Tentatively, future meetings will be held in the DC area. Dan asked the minutes reflect the board's appreciation to Pauline and Peggy for arranging the DC location.

Phil Reitinger recommended Dave Roosenzweig as a speaker on disaster recovery after 9/11. Rebecca stated the board's mission and questioned the strategic planning in topic areas. Lynn said the mission is more forward looking than just looking at the FISMA report.

Howard suggested the board investigate why some agencies continue to fail on their report cards. IG reports are public and are posted on websites. An OMB report will be issued in March – it would be good to have a speaker from OMB, an IG, and a representative from the House Government Reform Committee.

Action Item:

- Add this panel to the March (or June if March is not feasible) agenda,

The strategic plan items would be reviewed tomorrow.
The meeting adjourned at 4:15pm

December 8, 2006

Board members attending: Dan Chenok, Jaren Doherty, Joe Guirreri, Susan Landau, Rebecca Leng, F. Lynn McNulty, Leslie Reis, Howard Schmidt, Fred Schneider, and the Designated Federal Official, Pauline Bowen. Alex Popocwyz joined by phone. Unable to attend Brian Gouker, Lisa Schlosser, Phil Reitinger. Peggy Himes took minutes.

Actions: Leslie Reis offered that The John Marshall Law School would sponsor morning coffee breaks for the next meeting. Howard Schmidt volunteered to provide water.

The press was represented by the Washington Internet Daily and National Journal's Tech Daily. There were 8 members from the public in attendance.

Upcoming issues that may be valuable for the board to investigate, include:

- Follow-up on the USDA panel: Summary of, Verizon, AT& T actions in response to 9/11 with Dave Rosenzweig
- Meeting with GAO on FISMA report
- Susan said there needs to be guidance from OMB on the network issues raised by the Real ID legislation. Susan and Dan will work on a panel for March.
- Hillary Jaffe is the new OMB privacy official, invite her to March/June meeting
- CDT working group on privacy and security issue – Howard will email to board a summary from CDT
- Lynn suggested having Bruce Brody speak to Waxman staff on discussion of tweaking the FISMA Act particularly in the area of data breach
- Line of Business – training, incident response, security – Jaren said centralizing the LOB is a concern – LOB Panel for March. LOB common activity across agencies such as security.
- Ask Brian Gouker to give a factual update on NSA programs, including a previously briefed program (Susan will look at old minutes to see which program and will work with Pauline.)
- Health information – Jaren said maintaining privacy but still having access to records. Leslie suggested HIPPA. Jaren and Leslie to work on.
- Security funding – Howard said in R&D space there is duplication, lack of coordination, are we doing R&D in the right areas. The Board could take a longer view and make recommendations. Ask NIST what grants are going out. Fred Schneider said there will be an NAS Report coming out, work with Fred on getting a person to brief on this report. Where research money is going – Fred mentioned another CTSB report.
- There was a discussion that the Senate may want ISPAB input on new additional language (1) giving CISO enforcement authority, (2) OMB responsible for drafting policy (3) requiring an inventory of all hardware.
- FISMA – invite IG community back in December 2007
- Suggest to NIST the contingency plan document needs to be updated
- Lynn was asked to draft a letter from the Board to OMB on contingency plans which can be updated after further presentations

New Items

- Lynn suggested checking into the 2010 census – what are the security aspects – what plans is the Censes Bureau taking – front end technology has changed, additional access, wireless, statistical sampling. Dan will make phone calls to find the right person to brief board.

Potential March Meeting Agenda Issues:

- FISMA report panel in light of March report release– OMB-Hill staffer-GAO (review whether FISMA needs amendment) Panel to hear from the users (system owners, program officials) about their view of FISMA. Rebecca to work with Lynn, who

recommended having Cheryl Pease from the classified side to present. Centers of Excellence and management and operational controls representatives.
- LOB Panel (invite Mike Smith from DHS who is program manager)
- Security funding – Academy, CTSB Reports if available (Fred Schneider)
- Board discussion of security metrics (with additional reports from Fred Schneider – invite NIST speakers?
- Disaster recovery panel – ATT, Verizon, Rosenzweig, discussing OMB contingency plan
- NIST ITL discussion – it was suggested advance questions be prepared and distributed to Cita prior to the meeting
- Privacy Technology project – review first draft of report
- Susan Landau to lead panel on security issues arising in interagency collaborations
- NSA update
- Briefing on 2010 Census and security/privacy issues (Dan to identify speaker)
- Invite Greg Garcia, Senior Cyber Security official at DHS
- Invite Bill Jeffrey, NIST Director
- Invite Hillary Jaffe, OMB Privacy analyst

Privacy Technology Project Discussion

Leslie Reis, Professor, The John Marshall Law School, Facilitator

Leslie reviewed the Privacy Technology Project graphic. The goal is to vote in June on a draft white paper and get it into the legislative arena in 2007. The white paper should include legislative recommendations and best practices. Leslie asked if the technologies needed any revisions. The top line of the distributed graph is the process. The project team is currently modifying working definitions and the next phase is working on the vertical swipe. Dan suggested adding wireless to the list of mechanisms to be considered. Susan suggested adding outsourcing and rules for outsource data. Technologies used to locate should include RFID. Fred asked why the Internal Revenue Service was not included if the Census issue and healthcare issues are; it was suggested that census, healthcare be removed from the list.

Fred asked about the Fairness principle. Leslie indicated that Fairness is a process, may be a front end consideration, but the DPIAC paper defines fairness clearer. The content of the example is one dimensional rather than a drill down. Leslie said they are looking at a 3-D view of the regulations. The ultimate work product will be for all nonnational security issues in coordination with DPIAC). ISPAB is looking for a draft for distribution in March. Leslie has set this up as a research project with her law students. The underlying analysis will be gathered by the students but the end product will be by the ISPAB Board. Definitions are being refined so that all reviewers have the same meaning. Dan will work offline with Leslie on the mechanisms to be considered. Leslie would welcome comments on the deliverables.

Action item:

- Leslie will work with Dan and John Sabo of the DPIAC to develop first draft of white paper for review at the March meeting

Security Metrics Panel

Fred Schneider, Professor, Cornell University
Steve Bellovin, Professor, Columbia University
Jaren Doherty, CISO, HHS
Bruce Brody, VP, IA, CACI
Richard Guida, Director, IS, Johnson & Johnson

Fred Schneider introduced the panel discussion on Metrics for Trustworthiness. Questions on metrics include: do they exist, can they exist, are federally-mandated ones effective, and are others effective, in what settings. The panel ranged from federal to the private sector.

Jaren Doherty spoke about the 400 page report for HHS but it boils down to people looking at the spreadsheet on routers and certifications & accreditations; no one looks at the overall security plan. FISMA does not show how the security program is integrated; it does nothing to see if top management is aware and understands security. FISMA does not go into the overall look at the HHS program and FISMA does not support the integration of IT security into all Agency business processes. While current FISMA metrics measure some key IT security components, they do not accurately reflect an Agency's comprehensive IT security posture. FISMA should promote an integrated reporting process. When asked if antivirus spyware is a security or IT function, Jaren replied both. He said FISMA should measure overall progress toward IT security program maturity. The vulnerability statistics are more important than how many C&A were done.

Bruce Brody, formerly with the VA and DOE, said before FISMA we had nothing, it is a great base, and needs to be improved. There are key questions that need to be answered (1) it is possible to receive a high FISMA grade and not have a "secure" enterprise, (2) does FISMA measure the right things, (3) if not, what should we be measuring. FISMA must evolve from largely paper-based compliance processes to technology-based security processes. Lynn asked what the cost was to do the FISMA report and Mr. Brody estimated between $2-$3 million; Richard Guida indicated that comparable activity for Johnson & Johnson cost $500k, for a $51 bn enterprise.

Richard Guida explained security metrics are a very wide variety (number of port scans, number of stolen laptops, number of password lockouts, number or people failing to take security training). One should compare results with other organizations, use them for comparison, look for trends, and use them as an indicator to make security-related decisions. He suggested metrics not be used as a performance imperative or to measure overall security status of organization at a point in time. Mr. Guida said security metrics are akin to return on investment debate; there are lies and ROI calculations. The natural hunger for quantitative data drive us to bad decisions. Metrics should inform management decisions, but ultimately those choices should be based on management judgment.

Steve Bellovin quoted Lord Kelvin "if you can not measure it, you can not improve it." All software is buggy. There is no measurement on how long it will take to find the next bug. Turn off unneeded services. Testing can show bugs but can't show their absence. There is no perfect software. Layered defenses are stronger – first eliminate known problems, and then areas where you don't need activity. We need a way to make software less brittle. Software is better today and self-healing software where a hole can be closed behind the attacker may help. A key metric may be, "what is the work factor for an enemy to attack us?" A higher work factor can reduce the probability of a successful attack.

Discussion: It was reported the human factor is the place where most security problems occur; we must train people in proper computer security. Is there such a concept of adequate security? Does FISMA define the right approach? FISMA fails on the categorization and does not look at the architecture.

Also, Bruce Brody asked to whether adequate security was a better standard than absolute security, but then pointed out that adequate security is hard to define. A solution may be to develop two kinds of measures:

- Outcome measures for known problems
- Process measures (such as security reviews) for unknown problems.

Lunch break until 1:30

SCADA Briefing (Process control briefing)
Consensus Procurement of Industrial Control Systems

Julio Rodriguez, Control Systems Security Program
Idaho National Laboratory, DHS

SCADA: Mr. Rodriquez reported elements of the DHS program are providing guidance and developing partnerships. Their goal is to reduce the risk to critical infrastructure control systems. DHS launched www.us-cert.gov/control_systems for incident, vulnerability and threat reporting. The site also includes reference architecture of recommended practices. They provide outreach and awareness. They are piloting a CS2SAT tool with EPA that provides a systematic and repeatable approach for assessing the cyber security posture of industrial control system network. DHS develops partnerships through a vendor forum conference call. Another venue for their outreach program is the Process Control Systems Forum (PCSF) www.pcsforum.org dealing with security control systems. Institute of Information Infrastructure Protection (I3P) is the academia outreach. Cyber security is a shared responsibility but more can be done.

Action item:

- Invitation to give NIST guidance to push forward SCADA (Keith Stouffer – action – wait until DHS document is finalized and it is reviewed before doing further action)

Consensus Procurement Spec:

Project website: www.msisac.org/scada/
Contributors include: DHS National Cyber Security Division, NY State (Will Pelgrin – CSCIC) SANS (Alan Paller – Director of Research), Idaho National Laboratory (Michael Assante – Strategic Lead)

The scope of the project is new control systems, maintenance of systems, legacy systems, and information and personnel security; it is designed to incentivize providers to address security in their procurements. The initial focus of SCADA procurement objectives started in April 2006 and they have draft Version 1.5 posted. Vendors, asset owners, and regulators collaborate in the SCADA procurement objectives. The control systems procurement cycle is a lengthy process (request for bids, proposals submitted, bid review, contract award, SOW). It takes the vendor, asset owners, and government to make the process work. After the procurement language goes out, it is tested, then goes through site acceptance test measurements, and lastly configuration management (requires an understanding of why it was delivered that way). Dan said he would take Mr. Rodriguez' advice to NIST.

Action item:

- Dan Chenok to recommend that NIST recognize the benefits of this process for building security into Federal contract activities.

Public Participation

Brenda Abrams, GSA, suggested the board advise Rep. Waxman and others on FISMA legislation. She suggested to seek out agencies that have (GSA) tapped into CIO community for feedback. Ms. Abrams hears anti "mandatory" statements but she feels it is easier to enforce if something is mandatory. She would encourage OMB to continue to make mandatory guidance. She reminded the board of the low tech catastrophic affect on 9/11 and said there seems to be a lot of low tech ways to breach security not just technical stuff. Recommended "Can Audit" give a presentation on low tech such as e-fraud.

Next meeting actions

1. Carol Bales invited us to provide HSPD12 group (Motion: to refine about not locking into standards send copy of SHA letter)
2. Invitation to give NIST guidance to push forward SCADA (Keith Stouffer – action – wait until DHS document is finalized and it is reviewed before doing further action)
3. FISMA advise Congress (it was suggested to wait until we know what we want to say and when Congress is ready)
4. Rebecca wanted to hear from the users (system owners, program officials) about their view of FISMA. Lynn recommended having Cheryl Pease from the classified side to present. Centers of Excellence and management and operational controls representatives.

Dan announced at the next meeting there will be three new members.

ACTION ITEMS:

- The Board later discussed the fact that NIST guidance on security in contingency planning is out of date. Lynn McNulty agreed to draft a letter from the Board on the importance of updating these contingency plans, following a second panel to address the issues.
- Prepare and forward questions to ITL management in advance regarding future updates.
- Rebecca Leng will obtain performance metrics report from PCIE
- NIST will leave place on 12/2007 agenda for IG briefing on 2007 FISMA performance
- Dan Chenok will offer to Rebecca to brief the PCIE on ISPAB activities.
- When available, NIST to distribute Foreign Nationals policy for Board review
- Dan Chenok will offer to brief the HSPD 12 Steering Committee
- Plan panel - it would be good to have a speaker from OMB, an IG, and a representative from the House Government Reform Committee. This panel to the March (or June if March is not feasible) agenda,
- Leslie Reis offered that The John Marshall Law School would sponsor morning coffee breaks for the next meeting.
- Howard Schmidt volunteered to provide water at future ISPAB meetings.
- Leslie will work with Dan and John Sabo of the DPIAC to develop first draft of white paper for review at the March meeting
- Dan Chenok to recommend that NIST recognize the benefits of this process for building security into Federal contract activities.
- Cafritz Conference Center Scheduling 202-994-7470 reserve room for March 22-23, 2007 meeting (Rm 308). Ask board members prior to meeting how many need wireless access and conference call-in capability. Bring copies of ISPAB public statement sheet. Transcribe notes. - Peggy

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting.

Daniel Chenok
ISPAB Board Chairman