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

DoubleTree Hotel and Executive Meeting Center
1750 Rockville Pike
Rockville MD

June 8 - 9, 2006

June 8, 2006

Board members attending: Dan Chenok, Joe Guirreri, Steve Lipner, Rebecca Leng, Sallie McDonald, Alex Popocwyz, Leslie Reis, and the Designated Federal Official, Pauline Bowen. Guest speakers on June 8th include Joan Hash, Ivan DeLoatch and Tom Kupiec. Dan Chenok called the meeting to order at 8:50 a.m. and said he needed humility and reliance to succeed the chairman leadership role held by Frank Reeder who recently retired. Board members unable to attend today's meeting: Lynn McNulty and Susan Landau (graduation ceremonies), Howard Schmidt (Brazil) and Morris Hymes. Susan was called into the NIAP discussion at 1:30 to cast her vote, and stayed on for the work plan discussion. Peggy Himes took the minutes.

Thirteen members from the public and one press reporter attended.

Dan Chenok presented Certificates of Appreciation to Steve Lipner and Sally McDonald in appreciation of their service to ISPAB. Steve and Sally received a round of applause from the other board members.

Joan Hash announced she would be retiring. Dan complimented her on the leadership she provided to the NIST division and said she will be greatly missed. Members also expressed their appreciation. New NIST people will come on board, Cita Furloni, the new ITL Director, will address the board on Tuesday. Curt Barker, the new NIST Computer Security Division Chief, will be on the agenda for September. Dan also thanked Pauline Bowen for her continued support and acknowledged Elaine Frye's support and retirement.

Steve Lipner reported he is working on the NIAP letter and would like to see finalization since today is his last board meeting; Steve co-holds the ISPAB tenure record with Willis Ware of over 12 years, counting both of his appointments. NIST is working on his replacement. Leslie is working on a concrete set of questions to be asked regarding the Federal Privacy Policy Review project. Joe Guirreri is working on HSPD12 testing, sees tremendous activity and is looking at assessment funding to be put aside for it. Joe and Steve will present today on Microsoft's new security features and related industry developments. Sallie McDonald said she steps down from the board with regret and will discuss the Federal Enterprise Architecture Security and Privacy Profile later. Rebecca Leng noted agencies are getting ready to for FY 08 budget submissions, and HSPD12 is more difficult to implement due to funding. Dan Chenok reported he met with the Privacy and Civil Liberties Board within the White House and they are eager to work with the ISPAB board. Pauline reported that the ISPAB website is up-to-date, board vacancies are in the selection process, and minutes should be distributed within 7 days. The next meeting will be in D.C. alternating with the Rockville area. The meetings will continue to be held in public places.

It was noted, members of the press should be announced on arrival. Gregory T. Simmons from Fox News.com attended.

NIAP Discussion

Dan asked, how the board can help the software industry, government persons, and help to shed some light on NIAP. Steve Lipner presented a draft letter, which will be sent to the directors of

NIST and OMB. Steve said the letter is basically a review of what the board has heard over the last two years. The first paragraph is background. The draft of the letter is attached.
Joe suggested a source code review should be done at lower level evaluations in addition to levels now done. Rebecca agreed with Joe's recommendation, but questioned if the assurance piece is the right thing to do? Software security is one of three controls (technical, operational, and management controls) that go into security criteria. Rebecca also noted that OMB supported not extending a mandatory NIAP review beyond the national security community. Dan said there should be a greater reliance on COTS. Alex inquired on the intent regarding software. Steve added to the draft NIAP letter, "The process should provide information that supports user agency certification and accreditation processes in meaningful ways." Alex recommended the letter be forward-looking and not too myopic. Dan suggested Steve lay out the process after the background information. Steve said NIST's role is limited to the lab process (NVLAP) and NIST involvement has been pulled back. Joan Hash said NIST's current role is only at the laboratory accreditation process level.

Dan asked for a motion to allow the final NIAP letter to be voted on at the next meeting. It is necessary to have 7 board members for a forum vote. Steve asked that the NIAP letter be voted on at this meeting and he would redraft the letter incorporating member's comments.

Federal Enterprise Architecture Security Privacy Profile
Sallie McDonald with the support of Booz Allen Hamilton, MITRE and previous board members developed the document, *The Federal Enterprise Architecture Security and Privacy Profile, Version 2.0,* and distributed it to board members. Pauline noted it would be posted on the website. Sally said a simple description of "enterprise architecture" is total quality management; everything is complementary. There are several steps: Identification step – what is the risk analysis and threat level to that organization; analysis is the next step, followed by the selection process. The methodology is outlined on page 4 using the 17 control families in SP 800-53. This document gives the fundamentals. In July 2004, a document was put together on Phase I, the security profile. Then Phase II was introduced. The final document version before the board incorporates NIST guidance. This introduces in plain English what is enterprise architecture, what is security, and what is privacy. OMB comments are incorporated into this document. Sally talked to Dick Burk about marketing this document and making people aware of the need for security.

Dan asked what would a CSO do with this document - they would be looking across enterprise, looking to economize, looking for different groups to work together. Rebecca Leng said FISMA may be revised and that privacy and security need to be addressed. Dan said OMB is pushing for a business process level, data reference model, as well as service and technical levels. Alex understands the need not to be overly detailed, but at some point you need an evaluation and although this document is educational, inquired about its purpose. Sally closed by suggesting the board look at OMB and NIST and at what happens in the next 30-60 days and, if necessary, she asked that the board push this document forward.

Prior to each guest speaker, Dan Chenok explained that the ISPAB Board is chartered under FISMA to advise to NIST. It was renamed ISPAB and was formerly chaired by Frank Reeder. The board reflects a mix of government, academia, and industry. The Board members briefly introduce themselves.

Security and Privacy Issues in Geospatial Data
Ivan DeLoatch, DOI, and Tom Kupiec, Director of NGA Mission Assurance Office, presented to the Board. Ivan DeLoatch presented the Geo LoB Approach including the vision, objectives, timelines and milestones with key deliverables. Common Solution and Target Architecture is targeted to be out in June. Several security and privacy considerations were mentioned. Tom Kupiec said there is a partnership forming with industry and community to look at the C&A challenges. Tom explained the role of NGA that DoD wants to streamline C&A, and the architecture is changing to different levels of security, portal application. One question is, who's

looking at the application rather than intrusion and how do you tag data systems? Leslie said she's looking at gaps in federal emerging programs in privacy, taking a year long approach to identify gaps or issues that require guidance or legislation. What the board is doing dovetails what Tom and Ivan are working on and she asked if there is something this board can help them with. Tom Kupiec said they are looking into regional rights management and federated access, including striking a balance between open access and data security. Key elements are having architecture with good code, sound from the beginning, tagging the data within the systems, and then the data set. Another issues of potential interest for the Board is C&A for GIS, across DOD, intel, and civilian agencies. Dan said the board may want to think about geospatial and provide feedback, especially in the area of building security into GIS IT architectures. Steve asked Tom about the CC and NIAP testing and Tom replied the testing is extremely costly.

Approval of March Minutes

The Summary of the Meeting for March 2006 were approved pending changes suggested by Susan and to check on the spelling for Mr. Richard Schaeffer (not Shaver) fourth paragraph, NSA's replacement for Dan Wolff.

NIAP Letter Revisited

Steve Lipner incorporated the comments on the NIAP letter earlier to bring together the strands including software assurance and a set of recommendations to OMB, NIST. Definitions of NIAP, the Common Criteria, and software assurance efforts were added. Dan asked for discussion. Dan noted there was nothing about the GAO report in the letter, in the findings section it will be added "this finding is consistent with the recent GAO report on NIAP." Dan said the letter will be sent to the Secretary of Commerce, with copies to the Director of NIST, Director of OMB, and Under Secretary at DHS. Dan said he and Pauline would formalize the letter and copy the Board. Leslie moved the letter be finalized for final review and the board approved. The letter will be sent around one more time before it is mailed.

Real ID's Relationship to Overall Security Vulnerabilities and Privacy Risks

Susan Landau led the discussion on Real ID, what these impacts might be and what the Board should do about it. Susan recommended the board write OMB a letter. The question was raised, is she looking for OMB guidance or widespread acceptance? DHS has a committee to look at real ids. The real purpose is to comply with federal standards; is the person holding a driver's license, really that person. Rebecca Leng said the real id is a starting point to create new drivers license for everyone, every state has its own, everyone will get a new id that is hard to forge, using biometrics to authenticate and the board may want to make some recommendations. Alex asked how they are prioritized, which ones we should the board get involved with, and should there be statements by the board going back to the starting charter.

To summarize, a general issue that is coming up in two different ways is the increasing use of systems for multiple other purposes; there is an increase risk that if there were an attack, the attacker could use linkages to introduce DDOS into 51 different systems (each State and the national pointer) and t here is an information security risk that real ID cards would not support existing mission applications. We are tying to build awareness, but recognize budget constraints for the Board. Dan proposed to add this to the list of issues under discussion for the work plan.

"Thoughts Going Forward" by Dan Chenok – Future Work plan

Dan reviewed the email he sent to the board members on 6/6/06 outlining expectations for the upcoming term and detailing overall expectations, operations, and future issues. On operations, Dan is working with the NIST staff to enhance timeliness of minutes, agendas, etc, and NIST is updating the web site. Dan noted that the next meeting will be in downtown DC. Alex suggested the Board have specific metrics or ways to measure the Board's efforts and effectiveness at the end of each year.. Rebecca asked who are we here to serve and stressed the need to identify our stakeholders. Dan suggested importance and influence are the two metrics to use when deciding the upcoming issues for the board to focus on in the upcoming year. He suggested one person be designated as the leader for each issue. The following issues were discussed:

- NIAP study - wrapping up.
- Privacy technology is on the active issue list and will be visited at each meeting.
- Outreach to small business will remain at a lower priority.
- Information Systems Security Line of Business – (ISS LOB) – do we want to actively engage on this project. This is not an issue where the Board can add a lot, OMB can handle. – put on watch list, inactive.
- ID Panel – not work program but a board presentation.
- National security community activities in areas relevant to civilian agency security (e.g., architectures) – watch list.
- SCADA security – federal agencies are not responsible for these systems, OMB does not think this is an important issue for the Board. The board could offer management advice. Brief, not a program, watch.
- Real ID, biometrics and ID management – huge topic – above the cutoff line
- IPv6 – not an issue for the board, what could we add.
- Security Professional Development - credentialing and CyberCorps. – what is the problem statement that we could add influence. – not to be an active project.
- How government IT security relates to private sector IT security, through greater engagement with DHS NCSD – this is a topic many board members already deal with.
- Geospatial security and privacy issues – above the line item.
- Role of chiefs (CPO, CSO) – middle issue – table decision until after tomorrow's panel presentation.
- Information dissemination
- FISMA Reauthorization
- Healthcare – is on the watch list, middle list.
- Security funding – below the line, keep a watch on.

Final Active Strategic Thrusts:

- Privacy technology
- Real ID, biometrics and ID management
- Security metrics
- Geospatial security and privacy issues
- FISMA Reauthorization (and other legislative support)

Watch List:

- Information Systems Security Line of Business – (ISS LOB)
- National security community activities in areas relevant to civilian agency security (e.g., architectures)
- SCADA security
- Healthcare
- Security funding
- Role of chiefs (CPO, CSO)

Implications of MS Security Option and Other New Developments for Federal Users

Steve Lipner addressed the implications of MS security options. The set of requirements are evolving threats, data protection, pc performance, pc support. He reviewed Windows OneCare Key Features and Core Security Features. It is consumer oriented not enterprise. It is hoped that users connecting in from non-business machines are protected and clean. It will help with worm protection and includes a two-way firewall. Joe Guirreri listed top antivirus companies. Several potential implications include a convergence of products, decrease in costs due to competition, possibly fewer vendors, additional and faster innovation, and more integration across information security. Dan reported this is good news, to improve security, keep costs down, and the board discussed how it could be measured. Asset management, backup systems on an enterprise

system are ways to measure and metrics are available. C&A is a system measurement and with room for improvement.

The meeting was recessed at 5:10 p.m. until 8:30 a.m. tomorrow morning.

June 9, 2006

Board members attending: Dan Chenok, Joe Guirreri, Rebecca Leng, Steve Lipner, Alex Popocwyz, Leslie Reis, and Pauline Bowen. Guest speakers Cita Furlani, Eva Kleederman, Maya Bernstein, Barbra Symonds, Gerald Gates, John Sabo, Ari Schwartz, Peter Swire. Dan Chenok called the meeting to order at 8:50 a.m.

Yesterday's issues were reviewed:

- Recap the decision on the NIAP letter, revised letter will be forwarded to board. (Steve Lipner)
- Privacy profile good briefing from Sally - look at what happens in next weeks using the sunshine pack later.
- New issues: continue, developing a work program around
- Real ID discussion – continue to assess how to go forward
- Steve and Joe presented on Microsoft security for personal home computers – how do we measure the success of that program, continue to follow
- Work plan issues were boiled down to 5 strategic areas, 6 watch areas.
- Visiting the FISMA mandate will be looked at.

NIST ITL Update

Cita Furlani, NIST Information Technology Laboratory Director, reported Curt Barker will be the new Computer Security Division Chief, she hopes to have an ITL Deputy, and is hiring for the position of Director for the Statistics Division. ITL has almost 500 people of which 300 are federal employees; others include guest researchers, students, and contractors. She explained the NIST strategic process to explore what it had, what mandates, what are the core competencies, and metrics. ITL Core Competencies are IT Measurement and Testing, Mathematical and Statistical for Measurement Science, Modeling and Simulation for Measurement Science, IT Standards Strategic Implementation Groups. Broad opportunities will be decided by June 15. By mid-July a management decision will be made to select FY07 programs. Selected programs will start October 1.

Steve asked how much flexibility is there to manage the program – SDRS is fairly flexible. When there are other agency funds, ITL can use it. Rebecca asked what does measurement of science mean – Cita explained it is what the National Bureau of Standards has done for 100 years, to explain what is a meter, what is the make up peanut butter, what is the uniform size of nano particles - NIST does that. Standards are measurable. Face recognition, voice recordation, standards are needed to test against so they can interoperate. When Cita was asked what the most pressing issue is, she replied that it is making ITL work together as a team, it has 6 divisions. Joe asked who the real customers are – Cita said industry is the primary customer. Leslie asked what ISPAB can do to help – Cita replied give me a sense of what's going on, provide input on core competencies. Security and privacy are big issues, Dan said the board could look at the ITL report and give feedback in upcoming meetings. Cita reported funding is being moved and some things are going to slow down and stop. ISPAB will provide some advice. Dan asked for Cita's input on the 5 work areas suggested for the upcoming ISPAB work plan. Cita replied they were in line with what she had in mind. Geospatial is not a big issue at this point but healthcare is an issue to be watched. Other issues are working with ANSI to use the standards that are now in practice and there will be a big effort to assist HHS. Joe said key areas in infrastructure are the issue of metrics – how do you know how trustworthy it is, how much is NIAP providing. Joe said board is in a great position to assist NIST with measuring metrics. Cita

wants to start a series of workshops. Dan suggested a panel on metrics, what works. Dan is to meet with the Under Secretary of NIST, and the Director, and will look to Cita to schedule hopefully prior to next board meeting in September. Rebecca asked what role should NIST play in FISMA II and Cita said it would be worth discussing at another point. Dan thanked Cita and invited her back.

Afternoon Session Cancellation
Dan noted the GSA presentation on *Safeguarding Personal Information – Government Steps and Lessons Learned* by Martha Dorris would be rescheduled at a later date.

SP 800-100
Pauline reported the release SP 800-100, a guide for managers with 14 chapters including all major components, is ready for distribution. She asked members to provide comments. SP 800-100 is a summary of NIST security documents.

Privacy Reporting under FISMA Guidance
Eva Kleederman, Office of Management and Budget, reported OMB required the designation of a Senior Agency Official for Privacy last year and all agencies have done so. OMB is in the process of reviewing the FISMA template. FISMA will remain the same but gaps that are discovered will be corrected (extensive damages and definitions sections). Eva reported OMB Acting Director of Management, Clay Johnson, issued a memorandum for heads of departments and agencies to remind all employees of their privacy responsibilities. The results should be included in the upcoming FISMA reports. Results from the last year's FISMA reports showed the privacy issue had an excellent showing. It was noted that fewer than half the agencies did IG work under Sec 522. Major agencies document according to policy and procedures, provide training, and conduct reviews to OMB policy.

Leslie reported on the privacy study the board is undertaking and asked Eva what specific questions, what policies, what particular technologies, what end product will be of greatest use to OMB. Dan suggested Eva give this thought and get back to the board with suggestions. The ISPAB privacy study is not a criticism but is intended to provide assistance.

Privacy Office Panel Discussion
Participants Maya Bernstein, HHS; Barbra Symonds, IRS; Gerald Gates, Census
The role of a privacy officer was discussed and how technology in its various forms has affected agencies. Gerald explained data stewardship and the need to go out and do case studies to see how other agencies handle privacy. A chief privacy officer's responsibilities include advocate, legal compliance, research, internal awareness of responsibilities. After internal privacy awareness then outreach partnerships should be created. The need for contingency plans is the last step. It is critically important to have regular meetings with CIOs, serve on privacy boards (policy setting and review), have interaction with the policy officer, and to know how the privacy positions relate. It is necessary to look at innovative ways to develop hand held computers for gathering data – encryption and biometrics need to be used. Wireless technology is a critical issue too.

Barbra Symonds, IRS, recommended to move all security and privacy to CIO level. PIA is a required by a DAA. PIA is part of the C&A process. Building the next generation PIA, by breaking down into data classification, controls, entire lifecycle process. Time is spent in raw data collection and the need to share. There is a need to put in plain English then they can go in and check. IRS is looking at more than just checkboxes. IRS has massive visibility at what is privacy. IRS trust is key. Electronic returns are cost savings to paper returns. Privacy is becoming tangible and privacy tools are costly. Most privacy occurrences are human mistakes. Barbra recommended to do the same type of contingency plans for privacy (audit trail, mitigate, minimize) – what matters is how they respond to it. Alex said encryption is not always used for very sensitive information and he wanted to know the best vehicle to send sensitive information. IRS requires encryption within IRS and the IRS has ongoing work on transmission.

Maya Bernstein, senior policy analyst at HHS, stated she was speaking on her own experience not on behalf of the agency. HHS has an oversight review for each department. The Public Affairs office handles some privacy issues including FOIA requests. The CISO handles management policies. CISO has a counsel that meets monthly that monitors policy issues. There is a HHS council that can disseminate information. Maya recommended the need to focus on prevention before breaches happen. Maya also discussed training for agencies that rely on new technologies like RFID; re-identification of data; and how to revise consent procedures in a technology-intensive environment.

Rebecca asked the panel what percentage agencies use PII. IRS does more than 95%. Personal Identity Information – what is the definition of system, how are you counting them? Census does PII on all systems. Joe asked how Census balanced information sharing on potential terrorists with privacy. Census does not share any information because it is the law – Census is to collect information but not to share information. Title 13 has no exceptions.

Alex pointed out that the government should engage in data breach tabletop exercises. Also, there was discussion as to whether spending on privacy should be tracked in the same way that security spending is tracked.

Rebecca wanted to know and have in minutes:
FISMA is permanent law; reauthorization needs to be by Chairman Davis who sponsored the law is looking into reauthorizing – revising

Panel – Technology and Federal Privacy Legal/Policy Principles
John Sabo, Computer Associates; Ari Schwartz, Center for Democracy and Technology; Peter Swire, Ohio State University
Leslie explained ISPAB is undertaking an effort to examine the framework of the privacy policy and to see what gaps need input on. Leslie said ultimately she's looking at possible best practices and she needs a clear notion of what questions the board should be looking at.

John Sabo is speaking for himself not on behalf of any committee. John said a standing subcommittee on DHS and Data Sharing and Usage Committee was formed. There is an excellent report by Claude Morris, a professor in the UK. Collection of data is kept longer than intended. Privacy considerations (1) assure records are accurate, relevant, timely, complete (2) permit individuals access and amendment of records (3) provide reasonable safeguards regarding disclosure and protections against security and integrity threats. Security is only one piece of privacy.

Ari Schwartz said federal privacy rules have fallen behind. There is a failure to address the aging Privacy Act, the OMB Chief Privacy Counselor position is not renewed, and full Privacy Act guidance has not been overhauled since 1975. There are mixed messages in OMB memos to agencies. Ari reported the systems of records describe a '70s style flat database and not relational or distributed databases. Routine use exemption is overused and under defined. Section M for commercial data is unclear. Perhaps we need a CMM for privacy, and commercial standards for data integrity.

Peter Swire circulated his article on data retention, which is to be published in Federal Computer Week on June 12, 2006. Three categories of potential problems include (1) what protections are needed against inadvertent data breaches, (2) what government activities might be compromised by data retention, and (3) what are the counter-intelligence and national security implications. Peter said systems can collect more data. The security side of compliance deals with the policies but questions like should information go to John Doe is a privacy issue. Technologies also are affecting how we view anonymized data, and audit trails are a huge issue. The ISPAB can raise privacy's profile relative to security.

Leslie will forward the ISPAB Federal Privacy Policy Review Subcommittee mission statement, work plan and steps to be taken that she put together to all board members. Her time line and matrix were reviewed. In January 2007 she would hope to have a first draft of the paper out.

Public Question

"Have you considered requesting presentation or interaction with international privacy boards for opportunities to learn their lesson's learned, challenges, future areas of concentration and US impact? (In expectation of further FISMA refinement)

Respectfully,
Jessica Gulick
gulickj@saic.com"

Dan reported the response is the board is in scrutiny of the suggestion.

Action Items

- Forward finalized NIAP letter to Board (Steve) – finalize (Dan, Pauline) send to appropriate channels
- Keep watch on NIST, OMB, possibly promote *Federal Enterprise Architecture Security and Privacy Profile, Version 2.0* – post on ISPAB website
- Sept agenda – invite Martha Dorris, GSA, to speak (cancelled June 9 ISPAB presentation)
- Sept agenda meeting with Privacy and Civil Liberties Board within the White House with Mark Robbins
- Plan Sep agenda early.
- Follow up on partnership, DNI initiative – (Tom Kupiec) with industry and community looking at the C&A challenges.
- Plan a panel with Ivan and Tom for a future meeting
- Arrange for a meeting of Dan Chenok, Cita Furlani, and NIST Director
- Share the "list of friends of ISPAB" with the current board members – Pauline
- Get Joan back for hip hip hooray
- Continue to refine Leslie's chart, have one panel presentation on this next meeting

Dan adjourned the meeting at 4:05pm