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

George Washington University
Cafritz Conference Center
800 21st Street, Rm 101
Washington DC
September 14-15, 2006

September 14, 2006

Board members attending: Daniel Chenok (SRA International), Jaren Doherty (HHS), Joseph Guirreri (Computer Associates), Susan Landau (Sun Microsystems), Rebecca Leng (DOT), F. Lynn McNulty (McNulty and Associates), Alex Popocwyz (Fidelity Investments, via phone), Leslie Reis (The John Marshall Law School), Fred Schneider (Cornell University), Sharon Shoemaker represented NSA in place of Morris Hymes, and the Designated Federal Official, Pauline Bowen (NIST). Peggy Himes (NIST) transcribed the minutes. Board member Howard Schmidt (R&H Security Consulting LLC) was unable to attend.

Chairperson, Dan Chenok, called the meeting to order at 8:50a.m. He thanked NIST personnel for planning the meeting at a DC location which brought in more observers. Dan welcomed new members, Fred Schneider and Jaren Doherty. It was noted paperwork is pending for Phil Reitinger (Microsoft) and for Lisa Schlosser (HUD). Dan introduced Cita Furlani, NIST Information Technology Laboratory (ITL) Director, and she introduced Jim St.Pierre, NIST ITL Deputy Director. Cita pledged continuous NIST ITL support. Dan reported he met with House and Senate staff members, who were very interested in the Board's work. Dan reported he also met with Bill Jeffrey, NIST Director, and reported Dr. Jeffrey is very interested in the Board's activities and Dan extended an open invitation to future ISPAB meetings. Board members briefly introduced themselves and suggested current issues that they were working on (certification and accreditation (C&A), C&A policy watch from national security issue side, security risks of applying CALEA to VOIP, FISMA reporting, privacy and data breaches).

Twenty-four members from the public attended on September 14^{th} and two press reporters attended: Alexis Fabbri, Washington Internet Daily; and Don Aplin, BNA – Privacy & Security Law Report

Curt Barker, Division Chief
NIST Computer Security Division Update

Curt Barker reviewed the NIST Computer Security Division's mission, threats, and challenges. Dan asked about the current mission statement in that it does not provide a role in dissemination of information. Curt stated Liz Chew's group is working toward outreach. Cita Furlani added the NIST role is to create standards so that other organizations can teach it. Curt said his division provides additional support in providing speakers for outreach. Rebecca asked about open source code and Curt said it is encouraged and he does solicit advice from the national security community. Standards are mandatory for federal agencies but state government and industry also use them. The cost of doing FISMA implementation is an issue. Malicious intent to bring a system down is another concern as is the integrity issue.

Key concepts:

- Engage private sector to supplement technical expertise, foster feasibility, and maximize utility of NIST security standards and technology.
- Employ operational and management controls to mitigate limitations of current security technology

- Employ technical controls as practical to minimize the costs of labor-intensive operational and management controls

Curt Barker reviewed the major activities for FY07. NIST Computer Security Division key initiatives: Secure Hash, Security Metrics, Security Product Assessment Requirements and Methods, Engaging other NIST Labs. It was asked why the NIAP letter had not yet been signed. It was reported the letter was in NIST General Counsel office; Cita Furlani would check on the status. Curt reviewed the structure of the division. Dan offered the ISPAB's help in support for information dissemination about NIST activities to agency users, especially non-technical users.

- NIAP letter finalized. (complete) *Note, minutes after adjournment, Dan Chenok received word the NIAP letter would be sent out on Monday, 18Sept06*.

Mark Robbins, Executive Director
Overview of the Privacy and Civil Liberties Oversight Board
The White House

The Privacy and Civil Liberties Oversight Board came about after 9/11. The Chair and Vice Chair are confirmed by Congress, Carol Jenkins is Chair, and Alan Raul is Vice Chair. Three other members are Lanny Davis, Ted Olson, and Francis Taylor. The Privacy and Civil Liberties Oversight Board can change with elections. They are charged with providing advice, overseeing; however, they have no subpoena power, nor enforcement abilities to force, but during the implementation and development stages privacy and civil liberties issues are watched. They do not report to Congress but do testify on occasion. They met with a variety of interested groups including the American Civil Liberties Union, the American Conservative Union, and the Center for Democracy and Technology. The board's scope is confined to the war on terror; issues that will bring the most value to the American public (watch lists, law enforcement, and fusion issues). Mark Robins shared the Privacy and Civil Liberties Oversight Board's website www.privacyboard.gov and reported it provides the Board's legislative history and posts documents.

Mark indicated that key issues for the Board at this time were watch lists, information sharing, data mining, and Real ID. Leslie Reis reported on the ISPAB privacy initiative and explained she will be taking a look at specific technologies and Real ID which can be shared. Dan reported that in addition data mining and data use, other issues of concern are security metrics, authentication, and implications of new risks. Mark said he would like to have a broader view of the technology side of data mining as Leslie's project progresses. Joe Guirreri asked what the intended products from the Privacy Board were and Mark Robbins replied an annual report to Congress, analysis (horizontal, vertical approach in form of a report), checking press stories; FOIA applies to the board. Susan Landau asked how many technological experts were on staff and Mark said none at present but that he can obtain new detailees as the need arose. Dan offered to brief the PCL Board on the privacy project, Mark agreed.

- Add www.privacyboard.gov to ISPAB website. (Pauline)

The ISPAB meeting adjourned for lunch until 1:00pm. Leslie Reis chaired the meeting for David Temoshok's presentation.

David Temoshok, General Services Administration
HSPD-12 Update

David Temoshok discussed the implementation of Homeland Security Presidential Directive 12 (HSPD 12). The control objectives include background checks, strong protection on cards, personal identical authentication. HSPD-12 was signed in August 2004, mandated by the President, and FIPS 201 was issued by NIST on Feb 27, 2005. Compliance with FIPS 201 Part

Two PIV-II is required by Oct 27, 2006. FIPS 201 creates the standard for technologies and defines the data model. The Presidential Directive charged NIST to come up with the standard for the civilian agencies. Susan inquired why the Common Access Card was not used, David reported the CAC and the PIV have different technologies and cards. David said rather than an "unfunded mandate", HSPD 12 is considered a "priority mandate".

HSPD-12 Key Policy Points

- To ensure government-wide interoperability
- GSA is designated as the executive agent for products/services to implement HSPD-12
- GSA will make approved products and services (SIN 132-62 under IT Schedule 70)
- GSA will ensure all approved suppliers provide products and services that meet all applicable federal standards and requirements

There were no united laboratories to test for standards in FIPS 201 so GSA created one. NIST has accredited labs that do certain aspects (cryptographic) and GSA further designated those labs to test software on interoperability requirements. Smart cards are tested by GSA and NIST. GSA tests the physical aspects under a contract and is working to get the testing stabilized.

Approved products for PKI, system integrators, and FIPS 201 products are accessed at http:idmanagement.gov. There are seven approved vendors. 100+ agencies want to share infrastructure. 9 agencies committed to their own infrastructure (DHS, DoD, NASA, DoS, SSA, EPA, NSF, HHS, Treasury). GSA is a shared service provider. GSA will issue PIV cards and meet the Oct 2006 date at four locations (New York; Washington, DC; Seattle, WA; and Atlanta, GA). These four providers have done testing.

- Pauline was asked to check on why did NIST not want to do the testing, is it true that if applets break if they are tampered with, chip controls and why isn't NIST testing smart cards. *(See response from Curt Barker to questions which were forwarded to him under NIST Update, page 9 of these minutes.)*

Glenn Schlarman
Office of Management and Budget (OMB) Update

Glenn Schlarman reported on March 1, 2005 OMB issued implementation of the privacy provisions of the 2002 E-Government Act, and the implementation of FISMA. Agencies were asked to report on statistics and IGs were to report on quality. On May 22, Clay Johnson directed agencies to look at privacy programs; are they protecting and how are they doing it. Glenn reported privacy reporting will be expanded over last year.

OMB recently issued several memoranda in response to data breaches. To encrypt documentation on a laptop is the best practice, and OMB also recommends two full factor authentication, a 30 minute timeout, audit logs and to check them. He suggested the need to change the reporting requirement time - to report incidents in one hour. An agency will not receive new money until their legacy systems are secure. OMB also issued a checklist of NIST requirements for remote access.

A system includes people. It was asked what is being done with the E-Gov reporting requirements and he reported they use what agencies send on how they have used technology to improve a process. The importance of the security line of business (LOB) is one would know everyone is getting the same training on the same processes and tools at the same level; each agency could speak on the same wavelength. FISMA set out the consistent management structure in FIPS 199.

Dan Chenok asked about whether the post 9/11 activities around computer security by DHS was leading to a new relationship between classified and non-classified system security – whether there was a difference in kind in security or if there was a difference in degree. Glenn said it is a difference in degree but the needs of both communities (national and non-national security) needs to be cost beneficial and adequate. In the basic business level the needs are so similar. Susan asked how will people know what security level to buy, are they buying too much, and said there is a need for guidance.

There is a policy issue that when we need a higher level of security, this will be used for lower level applications. This would be counter to the vast government mission is to communicate with the community. Thus policy has to guide the difference between the majority of security investment that is common across civilian and intel agencies, and those pieces that need to remain separate. Without this there is a danger that civil agencies will buy too much security.

Rebecca asked Glenn to expand on the FISMA implementation within the CIO community and asked how far senior management had come along before they sign on the dotted line. Glenn said they want an agency report. How much better or worse from the signing certification – Glenn did not know but he needs input from the IGs. Glenn has seen progress in planning but less progress in executing.

Dan Chenok thanked Glenn Schlarman for his leadership on information security issues, and wished him well in his retirement in the fall.

Greg Garcia, VP, InfoSec Program
Information Technology Association of America (ITAA)
Update Status of Security and Privacy Legislation

Greg Garcia reviewed a listing of existing laws, regulations and guidance: National Infrastructure Protection Plan, July 2006; OMB Memo to Agencies, June 2006; Energy Policy Act (EPACT) 2005 – federal penalties for not having cyber security standards for electric utilities; Federal Trade Commission Settlement with CardSystems – federal standards for private sector; HSPD-12; CA 1386; National Strategy to Secure Cyber Space; FISMA 2002; Sarbanes Oxley, 2002; Cyber Security R&D Act 2002; Gramm Leach Bliley 1999; HIPPA; Putnam Draft; Data Breach Notification Bills – will not happen this year from Congress. ITAA wants legislation in a national standard instead of the states doing individual ones.

Dan asked, what was new about the July 2006 National Infrastructure Protection Plan from others; Greg Garcia reported this one incorporated much more private sector input. Dan asked, if Greg saw any activity in Congress around FISMA. Greg said no but clarified he had spent less time on the Hill, however, a board member said he had heard there is something going on. Industries are putting more and more privacy policies online. There are gaps and tensions in the cyber security profile: governance of systems and policies, personnel, technology, standards and best practices, and incentives/liability. What can government do – ITAA recommends more funding for law enforcement and R&D, international coordination, better federal procurement, and partnership with the private sector. Dan invited ITAA to use ISPAB in any way needed and thanked him for his input.

General Work Plan Discussion

Dan Chenok led the afternoon work plan discussion. On behalf of the ISPAB Board he thanked Jason Kerben for arranging an earlier meeting at the Department of State.

Frank Reeder, former ISPAB Chair, entered the meeting.

New items on table:

- Return on Investment (ROI) from the meeting with Bill Jeffrey
- Congressional staff meeting input - Privacy

- IG Discussion that Rebecca brought up
- Katrina impact on security
- Review ethics on security of board (delay meeting with lawyer until all new members are on board)
- Data Protection

Current Strategic Thrusts

- Privacy Technology (Geospatial security and privacy)
- Real ID, biometrics and identity management
- Security metrics
- FISMA and related legislation
- Watch list issues:
  - ISS LOB - invite to March meeting
  - National Security community activities
  - SCADA security – there is a need but no funding.
  - Healthcare
  - Security funding
  - Role of chiefs

ROI: Are there needs to review FISMA ROI. It appears FISMA and other auditors ask the same questions every three months. Why are they looking at security plans every year when it appears the whole program is not recognized. Lynn recommended a possible survey to send to CISOs for input. Fred said the money spent on FISMA audits may be well worth it since security is increased and there is value in awareness. When questioned on what is the deliverable that Dr. Jeffrey is looking for; Dan replied, a letter with recommendations.

- Dan with input from Peggy's minutes will put together an outline to brief NIST Director; invite the Director to address the Board at the December meeting to include more specificity around the FISMA ROI issue.

Katrina issues: how data was handled, geospatial issues, impact on privacy. It was questioned whether intellectual property rights were something the ISPAB Board would even want to handle. What were the impacts on federal IT operations? Did they work; what did not. This Board could recommend a study be done or at least lessons learned. Susan said she was at a meeting where someone announced NCS is doing this.

- Lynn check into obtaining a speaker from National Finance Center to come to ISPAB to brief on Katrina.

Privacy: Work session will be held tomorrow. Work commitment Leslie, Howard, Lynn, Dan. The session is devoted to having a white paper available in June 2007.

- Invite Carol Bales to December meeting to explain in detail what the HSPD12 plan is. Carol Bales was recommended by Glen Schlarman. (Pauline)

ID Management: There is still not a plan for logical access by agencies based on the HSPD 12 cards.

Discussions Needing Additional Follow-on:

- Mark Robbins' briefing
- IG panel in December
- Invite the new Assistant Secretary for Cyber security to DHS to ISPAB
- SCADA (Lynn will follow-up)
- Move Geospatial security and privacy into the privacy project as a technology needing analysis of impact on fair information and related principles.

Jason Kerben recommended a panel including PCIE to come to ISPAB to provide feedback. Venue will be in DC for December.

- Brief the Hill on the Privacy Technology Project (Dan)
- Rebecca Leng to arrange PCIE panel for December meeting
- December meeting have topic on metrics

September 15, 2006

Dan Chenok called the meeting to order at 8:45a.m. and reviewed the previous day's meeting. Dan asked for amendments to the June draft minutes. Leslie asked a more extensive explanation on the privacy issue be added but will add it to September's minutes. Lynn McNulty moved to accept the minutes, it was seconded. There was a unanimous decision to accept the June 2006 minutes.

Board members attending: Daniel Chenok (SRA International), Jaren Doherty (HHS), Joseph Guirreri (Computer Associates), Susan Landau (Sun Microsystems), Rebecca Leng (DOT), F. Lynn McNulty (McNulty and Associates), Alex Popocwyz (Fidelity Investments, via phone), Leslie Reis (The John Marshall Law School), and Fred Schneider (Cornell University). Bill Barrett represented NSA in place of Morris Hymes and Pauline Bowen (NIST) attended as the Designated Federal Official. Peggy Himes (NIST) transcribed the minutes. Board member Howard Schmidt (R&H Security Consulting LLC) was unable to attend.

Nineteen members from the public attended on September 15th and two press reporters, Alexis Fabbri, Washington Internet Daily and David Hatch, Technology Daily

Alan Paller, Director of Research, SANS Institute
Data Security Breaches

Alan Paller said his talk would be about *how* not about *what* needs to be done. He distributed an article "Beyond Media Hype: Empirical Analysis of Disclosed Privacy Breaches 2005-2006 and a DataSet/Database Foundation for Future Work" by Ragib Hasan and William Yurcik from the National Center for Supercomputing Applications (NCSA). Data breaches are a huge issue for federal agencies and shared examples of attacks that show there is a massive failure of security. Two attack vectors include spear phishing and exploiting new vulnerabilities. Cyber fraud is a massive crime wave with lucrative payoffs. Nationstate threats are increasing, especially from China Terrorists raise money through cyber fraud and hacking. Laptops are lost all the time; IRS lost more than 100 laptops in the last 12 months. But lost laptops lead to a very small portion of identity theft cases, and only a slightly larger number of credit card fraud Dan asked if there were a way to tell if the laptops were sold for the machine on the street or for the content on the machine. There is interest in finding out the level of threat.

Alan said that they key issue is, How do we get to a common benchmark that all can agree on? NSA/DISA/SANS/CIS/DHS/Microsoft came up with a consensus guide for securing Windows. Consensus procurement specs led by Will Pelgrin, CISO of NY State, are being applied to industrial control systems and could apply here as well. Rebecca said FAR (procurement process) can be important since many times grant specifications are copied by management and not looked at by the IT people. This could provide a safe harbor for entities who follow the specs. A starting point for such specs is to encrypt the data on laptops and to log all computer-readable extracts and erase within 90 days if not required for immediate use. Alan suggested the government do a massive buy of data encryption for computers. Fred Schneider said people are buying new laptops that will have encryption and he would be hesitant to have people add additional encryption. Alan suggested agencies highlight successes and share them.

Alan noted that there is a conference in December around benchmarks, and suggested ISPAB members look into attending.

- Invite Will Pelgrin to December meeting to discuss consensus specs and how it may apply to the FAR. (Pauline) *(Contact information for William Pelgrin, NYS Office of Cyber Security, william.pelgrin@cscic.state.ny.us, 518-473-4383. Peggy Himes had contact information as a keynote speaker at the FISSEA Conference in March 2006.)*

Privacy Technology Project Discussion
Leslie Reis, Professor, The John Marshall Law School, Facilitator
John Sabo, Director, Computer Associates
Paula Bruening, Staff Counsel for the Center for Democracy and Technology
Maureen Cooney, Head of the Washington Privacy Practice, Hunton & Williams Law Firm

The mission of the ISPAB Federal Privacy Policy Review Subcommittee is "to examine the extent to which changes in the nature and use of information technology by federal agencies have created the need for revision of the legal and policy framework of privacy in the 21st century. The ISPAB subcommittee will effort collaboration with a corollary subcommittee of the DHS Data Privacy and Integrity Advisory Committee." (FPPR Subcommittee Draft Scope 6/6/2006)

Leslie Reis explained the privacy project is looking at technology evolution and policies and whether the policies need to be updated. This is the third meeting on this subject. The goal is to continue to evolve the framework and come out with a white paper to be circulated in draft next summer and formally released next fall. Leslie questioned, are the technologies that we are looking at the most relevant - are these ones that need revised. Leslie reviewed the initial talking points. She said the white paper should include legislative recommendations and best practices. Leslie said they are looking at a 3-D view at the regulations. The ultimate work product will be for all non-national security issues (DPIAC). Dan reported the Congressional staffers he spoke with are concerned with data breaches and the need for a possible amendment.

In March 2007, ISPAB is looking forward to a draft for distribution. Since the last meeting, Leslie refined the research methodologies --is the principle contemplated, is there a gap or vulnerability and what do we do about it. 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 and shared so that all reviewers have the same meaning.

John Sabo said Alan Paller made two important points; 1) the importance of building a consensus, and 2) nothing we do will fully solve security problems, there will always be security problems. John stated he is not speaking officially for DPIAC and that the DPIAC board is working on a similar privacy project. John shared the website for the Privacy Framework on the International Security Trust and Privacy Alliance (ISTPA) www.istpa.org. John explained the information privacy "environment" which includes law, regulations, requirements, business processes, protocols/standards, operational systems, external factors, and technologies. Rigor is needed to improve information privacy operations, management, and compliance. Technology will change, new technologies will be invented and used, and there is a need to define core technology.

Maureen Cooney said she sees priorities in the network area, interoperability, third party use of information (which can lead to a gap in notice and choice), location-based tracking, and data mining. The issue is privacy and how it is affected by security. Areas to look at include data sharing and data matching. People may not be receiving adequate notice through the Federal Register notices. She advocates teaching technologies. People may not be aware of the way computers are intertwined, (Treasury links to DHS etc). How long information is retained is another issue to be reviewed.

Paula Bruening said technology neutrality is worth repeating and whatever is done builds in flexibility; take a lighter touch on specific technologies. Notice will be more important than less. Notification in the Federal Register is good but more additional notice would be better. Locational technologies that lead to ubiquitous computing create questions of “who should provide the notice” , and whether general notice is useful. Susan added that with anonymizing technology you should not have to identify yourself. She said there is public concern that people are not part of the data collection process, it is happening to you without consent. Classes of mechanisms may be the term to identify this category.

Leslie said she received good ideas on the framework and approach from this panel. Maureen said using metadata is not simple to do a model but would be helpful for DHS and other federal agencies. John said most important areas are third party and network use of data. Leslie said there are big areas to look into, port data, technologies/practices and network, data mining and notice/retention. Paula added to look to the future and focus on security that protects data, not just information privacy.

- Leslie should send revised documents to ISPAB Board including definitions.
- Leslie to refine outline and present at December meeting, with appropriate outside review.

Break for lunch.

Teresa Nasif, General Services Administration
Joanne McNabb, Chief, State of California Office of Privacy Protection
Safeguarding Personal Information – Government Steps and Lessons Learned
Dan prefaced stating House and Senate committees want real world contacts for data breaches. Teresa Nasif provided the Federal view and Joanne McNabb provided the State/local/private view.

Teresa Nasif reported that on May 3rd the VA computer was stolen which affected 26.5 million veterans. On May 19 she received a call from USA Services and the stolen laptop was recovered June 29, 2006. USA Services is a Presidential E-gov initiative that helps government be more citizen-centric. They provide direct service to citizens through firstgov.gov, email distribution, 800 FED-INFO, and distribution of publications. The VA worked closely with FBI and local law enforcement, they set up multiple contact centers, issued press releases, and constantly updated information on va.gov, FirstGov.gov, DoD website, and on their contact centers. The VA sent letters to all veterans and placed VA program managers on-site at the contact centers. They had 250,000 phone calls and a million hits to va.gov.

Teresa reported lessons learned from the VA breach were to expect an influx of inquiries quickly, work out a telephone response plan, involve all relevant government websites, create a swift approval process for updates to information as situations unfold, ensure consistent information, have positive responses for all questions. Federal agencies should be aware that GSA has credit monitoring services on schedule now at http:www.gsalibrary.gsa.gov/ElibMain/SinDetails. Leslie asked if the Privacy Act should be revisited to bring in the recovery area and vulnerability.

Joanne McNabb explained the California Office of Privacy Protection (COPP) was founded in 2001 to protect the privacy of individual’s personal information. Half of their calls are on identity theft. They provide consumer assistance, workshops, town hall meetings, coordination with law enforcement, and best practice recommendations. COPP’s website is www.privacy.ca.gov. COPP cannot keep up with logging breach notifications, and from July 03-04 there were about

100 notifications. Data breaches occur when data is moving around with people, data is retained too long, unneeded data is still collected, paper records (stolen/lost mail), and due to human factors. People are not aware of the value of data and people delay in reporting incidents.

The COOP policies on information security program are on their website, www.dof.ca.gov/FISA/BudgetLetters/BudgetLetters.asp. A mandatory annual privacy/security training and certification for all employees is a new policy. Their policy was expanded to include a privacy component. They are trying to tighten up information security through awareness programs. Joanne said the VA should have recommended that individuals put a fraud alert on their credit file. Lynn asked, do you see a need to have a federal law or has the California law has become the defacto? Dan asked if she could recommend companies that deal well with breaches of information; Joanne recommended Wells Fargo and the University of CA San Diego.

NIST Update

Below are questions and answers posed to Curt Barker, NIST Computer Security Division Chief. *Will the PIV cards break if they are tampered with*? I'm not sure how to interpret the question. It is possible for the issuer to add applications. There are protections against loading of data or programs by other than the issuance facility. It's relatively easy to damage the electronic components so that they don't work.

Why did NIST not want to do the testing for physical security? Since the CMVP laboratories do determine the physical security characteristics of the cards, I'm assuming that the question relates to the contact less card reader interfaces employed in physical access control. We have published interface guidelines for the card readers. Testing of the readers themselves is interface testing rather than security testing; that's not really part of our CSD mission; and we don't have the facilities or the budget to carry out such testing. We believe that such testing falls into the realm of qualification testing (a procurement activity responsibility).

What are the chip controls? (Note: I am not sure about that question.) If I understand the question correctly, the applicable controls are FIPS 140-2 Level 2 controls, with Level 3 physical security controls.

Public Participation

Brenda Abrams, GSA, stated nothing she said represents the GSA IG and she thanked the board for the opportunity to attend their meeting and found it very informative. She said Alan Paller made her open up her eyes and that management does not realize how vulnerable their data is. She asked two questions (1) Is it possible to arrange some sort of outreach to the business people in agencies, it makes good business sense. (2) Help the CSR to have a plan in place. Lynn recommended Brenda Abrams get in touch with the people that write NIST 800-16 which is role-based training. She would like to see information go out to a broader audience.

Wrap-Up and Agenda Review for December 2006 Meeting

Dan will work with Pauline to resolve action items quickly.

Data breach material – Dan was asked by House and Senate staff to report back to them on data breach issues, to distill information and report back with summary. The Board concurred and asked what format is requested. Dan will communicate via a letter and a meeting using power point slides.

Fred stated if your social security number is stolen, there needs to be a way to revoke social security numbers. Identify theft takes identifiers and uses them as authenticators. It is necessary to treat data breach at root of problem.

- Fred will prepare 3-4 slides on his recommendation. Dan will draft a letter that summarizes the Board's findings as discussed in the September meeting, as well as a short set of slides to brief the Hill and provide technical details. Lynn moved to approve as discussed, all were in favor, motion approved.

It was reported Dr. Jeffrey asked to be informed of metrics and NIST outreach. Dan asked if the Board if he should schedule a meeting with the Director prior to December meeting and/or invite Dr. Jeffrey to the December meeting. It was reported Dr. Jeffrey wanted to know if the Board knew what the FISMA cost was and the Board said they are not ready to give analysis. It was suggested NIST work with OMB and asked NIST to provide clear concise questions that they want answered to the ISPAB board.

- Verify latest OMB memo asking for plans – Pauline.

Dan Chenok thanked new members, Jaren and Fred, and other board members for their input. The meeting adjourned at 4:10p.m.

Summary of Action Items:

- NIAP letter finalized. (complete) *Note, minutes after adjournment, Dan Chenok received word the NIAP letter would be sent out on Monday, 18Sept06*.
- Add www.privacyboard.gov to ISPAB website. (Pauline)
- Arrange briefing for the PCL Board on the Privacy Technology project (Dan)
- Pauline was asked to check on why did NIST not want to do the testing, is it true that if applets break if they are tampered with, chip controls and why isn't NIST testing smart cards. (See response from Curt Barker to questions which were forwarded to him under NIST Update, page 8 of these minutes.)
- Dan with input from Peggy's minutes will put together an outline to brief NIST Director; invite the Director to address the Board at the December meeting to include more specificity around the FISMA ROI issue.
- Lynn check into obtaining a speaker from National Finance Center to come to ISPAB to brief on Katrina.
- Brief the Hill on the Privacy Technology Project (Dan)
- Invite Carol Bales to December meeting to explain in detail what the HSPD12 plan is. Carol Bales was recommended by Glenn Schlarman. (Pauline)
- Rebecca Leng to arrange PCIE panel for December meeting
- December meeting have topic on metrics
- Invite Will Pelgrin to December meeting to discuss consensus specs and how it may apply to the FAR. (Pauline) *(Contact information for William Pelgrin, NYS Office of Cyber Security, william.pelgrin@cscic.state.ny.us, 518-473-4383. Peggy Himes had contact information as a keynote speaker at the FISSEA Conference in March 2006.)*
- Leslie should send revised documents to ISPAB Board including definitions.
- Leslie to refine outline and present at December meeting, with appropriate outside review.
- Fred will prepare 3-4 slides on his recommendation. Dan will draft a letter that summarizes the Board's findings as discussed in the Sep meeting, as well as a short set of slides to brief the Hill and provide technical details. Lynn moved to approve as discussed, all were in favor, motion approved.
- Verify latest OMB memo asking for plans – Pauline.

Additional action items for Peggy and/or Pauline:

- Have permanent sign made up for Information Security and Privacy Advisory Board **(**ISPAB) Meeting (8 x 11)
- Conference phone set up - use NIST telecom for number and pass code
- Water pitcher & glasses for next meeting

- Email Curt Barker's slides to melaug@gwu.edu
- Tim Parisi wants added to friends and wants slides for privacy technology, Pauline email to tparisi@gwu.edu
- Cafritz Conference Center Scheduling 202-994-7470 (Billie Ann Foote) reserve rooms for December 7-8, 2006 meeting (Rm 101 Dec 7) (Rm 308 Dec 8). - Peggy

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting.

Daniel Chenok
ISPAB Board Chairman