Information Security and Privacy Advisory Board (ISPAB)

Final Summary of Meeting

George Washington University
Cafritz Conference Center
800 21st Street, Room 405
Washington DC

June 4 – 6, 2008

June 4, 2008

Started at 1:00 P.M.
Ended at 5:00 P.M.

Present:
Jaren Doherty (via phone)
Brian Gouker
Joseph Guirreri (via phone)
Rebecca Leng
Phil Reitinger (via phone)
Fred Schneider
F. Lynn McNulty
Ari Schwartz
Alex Popowycz
Pauline Bowen, DFO

Absent:
Lisa Schlosser
Peter Weinberger

Visitors, presenters, panelists: 7
Matt Scholl, NIST, Computer Security Division

Dan Chenok, Board Chairman, convened the Information Security and Privacy Advisory Board (ISPAB) for the first meeting of 2008 at 1:00 P.M. The Chair confirmed that the Board's new charter had been renewed and confirmed for the next two years. Any charter renewal delays were strictly an administrative issue. The meeting began with each Board member introducing themselves and sharing the highlights of their latest developments. The Board welcomed the following new Board members:

Ari M. Schwartz
Peter Weinberger

The Board reviewed the agenda for this meeting and the Chair provided information relating to each agenda items. Rebecca Leng reminded the Board of the scheduled attendance of Deputy Secretary, Department of Transportation on the next day, and the need to provide a list of issues and questions for the Secretary to include in his presentation. A list of questions was put together to be forwarded to the Secretary's office by Rebecca Leng.

Center of Strategic and International Studies (CSIS) Commission Briefing
James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program (CSIS)

James Lewis is a senior fellow at CSIS and directs its Technology and Public Policy Program. Before joining CSIS, he was a member of the U.S. Foreign Service and Senior Executive Service, where he worked on national security and technology-related issues (including global arms sales, encryption, space remote sensing, and high-tech trade with China).

The Center for Strategic and International Studies (CSIS) provides strategic insights and policy solutions to decision makers in government, international institutions, the private sector, and civil society. A bipartisan, nonprofit organization headquartered in Washington, DC, CSIS conducts research and analysis and develops policy initiatives that look into the future and anticipate change.

Program Overview of Technology and Public Policy - The CSIS Technology and Public Policy Program looks at how technological change affects security and economic growth in the new international environment. Current research includes cyber security, intelligence reform, military space, and Internet

governance. The program hosts regular discussions with leaders in government, industry, and the private sector.

This briefing evolved from a presentation at the last Board meeting in December 2007 by the Chair. James Lewis explained that the Commission consists of about 40 members with over half of the members from private sectors. The selection of members is based on their specialties and not affiliation. The Commission has met fifteen times during a 6-month period. Most briefings during every meeting were given voluntarily and were not solicited by the Commission. The focus is to present what the expected issues are to the next President. The Commission has selected a number of concrete topics for discussion: – strategies for overview on cyber security, FDCC, securing identity, robust credentials, authentication, public private ownership, rebuilding trust to organizations, creating better ways for public and private to work together, how to work with foreign partners, work with people we trust and cannot trust, and re-architecture of the internet. It is the Commission's intent to achieve a complete consensus. The project has three phases: presently at team center phase; recommendation phase: and final report. The estimated target date for releasing the commission's draft paper is Labor Day. The Board looks forward to reviewing the draft paper and to include it in the next meeting's discussion.

Board Discussion

- ***Board Administrative Discussion***
- ***Approval of December 2007 Minutes***
- ***Agenda Topics for September 2008 meeting***

- Dan Chenok announced to the Board that Jason Miller, a representative from a federal radio station, will be attending the meeting during the next two days and may be taping the meeting for a future broadcast.
- Pauline Bowen reminded Board members that ethics forms must be completed by all members as it is a legal requirement for such an advisory board.
- Dan Chenok asked for a motion that the draft Summary of the Meeting from December 6-7, 2007 be approved. Lynn McNulty proposed the motion that Meeting Summary be approved and accepted, and the motion was seconded by Fred Schneider.
- To decide on whether the Board is to prepare a statement or white paper regarding FISMA review.
- A motion was passed to write a letter to OMB regarding the Board's concerns and funding on the framework presented by Brenda Oldfield, DHS, at the last Board meeting in December. Dan Chenok will consult with Lynn McNulty to draft a letter to be presented to the Board.
- While the scheduled meetings for 2008 remain unchanged, NIST has proposed to the Board to hold three 2½ -day meetings in 2009 instead of four 2-day meetings. Dan Chenok will work with NIST to confirm the dates of the 2009 meetings.
- Potential Agenda Topics for September 2008 meeting:
  - CSIS's draft paper – to decide on whether the Board wants to review and comment on the draft, and to define NIST's involvement in CSIS. Board plans to recommend to the Commission to consider NIST presentation and to allow both NIST and CSIS to respond independently,
  - Privacy impact (Einstein) Hugo or the program
  - DOJ's FOIA guidance which needs to be updated every two years. DoC is now responsible for this FOIA guidance, and it has not been updated for the past four years.
  - The Board is to review the article *FBI partially blames procurement rules for fake IT products* and provide their comments/reaction.
  - DOJ Privacy briefing on policy update in May 2004. (Ken Mortenson (DHS) or John Lee, OMB
  - Einstein II briefing.
  - Technical person talk about Einstein – Randy Vickers
  - Rod Beckstrom, DHS Cyber Security Coordinator to brief
  - Melissa Hathaway to give brief on selected subject
  - WFED discussion
  - The issue of bringing in intern(s) to work Board's related projects.
  - FBI procurement rules discussion

- Biometrics accreditation planned
- Privacy Technology Report
- Discuss Transition letter for old and new administration to include: CPO position issue, recommendations for training CPOs, and other important issues
- Telecommuting session
- Private sector CISO best practices panel
- Executive training for incoming political officials (Dec meeting)

Board members developed five questions for the Deputy Secretary of DOT's presentation on Thursday.

FISMA Metrics Efficacy
Board Members

The board's consensus is that the FISMA reporting process is a good process but it is overly burdensome. It is necessary to improve the metrics. Prior to moving on to next phase, OMB needs to provide measures at the beginning of the program and not at the end of the program, so as to have the right measurements. The Board agreed to draft a letter to OMB with a summary of the evidence presented to the Board, and a set of recommendations for action.

Meeting adjourned 5:00 P.M.

June 5, 2008

Started at 8:30 P.M.
Ended at 4:50 P.M.

Present:
Jaren Doherty
Brian Gouker
Joseph Guirreri
Rebecca Leng
F. Lynn McNulty
Alex Popowycz
Philip Reitinger
Fred Schneider
Howard Schmidt
Ari Schwartz
Peter Weinberger
Pauline Bowen DFO

Absent:
Lisa Schlosser

Visitors, presenters, panelists: 20
Matt Scholl, NIST, Computer Security Division

Dan Chenok started the meeting at 8:50 A.M. with a recap of yesterday's discussion. Matt Scholl, NIST's Computer Security Division was also present at the meeting.

Privacy Technology Report Review
Dan Chenok, Board Chairman

This is to update on the status of this white paper. Since the last meeting, GAO has finalized their studies. Leslie Reis has completed a lengthy draft. The Board needs to decide on whether to review the draft. While the Board originally sponsored the work three years ago, Leslie Reis is no longer a member of the Board, and therefore, the draft is not a product of the Board. The Board requested Pauline Bowen, DFO, to provide a clear understanding of the timeline from past meeting minutes. If the Board decides to endorse the draft with the intention to post it on its Website, the Chair is required to submit it to OMB and NIST with a cover letter or a written summary by the Board. It was agreed that the Board will look at the product and review the options to proceed.

Federal Initiatives Due in June (Trusted Internet Connection, Federal Desktop Core Configuration, Homeland Security Policy Directive 12, & Internet Protocol version 6)
Bill Vajda, Chief Information Officer, Department of Education
Ed Meagher, Deputy Chief Information Officer, Department of Interior

Bill Vajda oversees the effective and efficient design and operation of all major information resource processes for the Department of Education. Previously, Vajda held senior positions at the Department of Defense and the Department of Treasury, in addition to the private sector. He is a graduate of the Ford School of Public Policy at the University of Michigan.

Ed Meagher is the Department of Interior's Deputy Chief Information Officer, and also helps to oversee the acquisition and installation of infrastructure (hardware and software) and applications supporting Interior's varied mission areas, including major investments for recreation, mineral leasing and development, wild land fire management and financial and business management. Before joining Interior, Meagher was the chief technology officer for the Department of Veterans Affairs and previously held the post of deputy CIO at Veterans Affairs, where he also served as acting assistant secretary for Information and Technology, acting chief information officer, and special assistant to the Secretary on Information Technology. His extensive career in the area of Information Technology spans more than 25 years in both the public and private sectors.

Dan Chenok introduced the panel speakers and stated that both speakers oversee the security apparatus at each agency. The third speaker, Casey Coleman, Chief Information Officer, GSA, was unavailable to attend. This discussion was derived from various briefings on desktop, Einstein, and loose discussions on cyber security. The Chair requested the speakers to identify challenges and contributing elements on various activities coming together that the Board will be able to submit to OMB and NIST for considerations.

He agreed with OMB that there is no lack of funding spent on security but funding was spent inefficiently with many issues remaining unchanged. There is a lack of a cohesive and collective approach and commitment within the government toward security, with the focus seemingly on defending agencies against each other. He stated that the agency avoided complicated patch up and that execution was less than optimal. He considered Einstein primitive in its capabilities, and that any action from the government is at least six years behind.

Bill Vajda's career has spanned through both government and non-government. He believes that the United States gave away the key of our technological capabilities when we decided to manufacture both hardware and software overseas so as to realize lower costs. The United States government must consider the true cost in order to be fully committed to security. The government's approach is deemed as insufficient and inefficient, and it is simply applying a 'bandage' to the system. He noted that government coordination is inconsistent between budget initiative, practical operations, and implementation of mandates. Therefore, he suggested the need to involve the Executive Branch and Congress to coordinate budget, resources, and initiatives for all agencies. As most security initiatives are driven primarily by budget and not focus on security, CIOs have been unable to fully exercise their functions in the area of security. The speakers suggested the following urgent issues:

1) to define the perimeter and functions of CIO,
2) to integrate security with people,
3) to impose a certain level of accountability and consequences in order to achieve results,
4) OMB to coordinate security initiatives with Congress, and
5) Security operations must primarily be security driven, not budget driven, but use the budget to drive resutls

<u>VA Data Breach Follow-up Briefing</u>
Adair Martinez, VA

Ms. K. Adair Martinez serves as the Deputy Assistant Secretary (DAS) for Information Protection. She is the primary advisor to the Assistant Secretary for Information & Technology on matters related to information protection, including: Privacy, Security, Risk Management, Records Management, Freedom of Information Act (FOIA) requirements, and Business Continuity. As the DAS for Information Protection, Ms. Martinez ensures Department-wide compliance with information security and privacy policies and procedures.

Ms. Martinez previously served as the Chief Information Officer for the Veterans Benefits Administration (VBA) in the Department of Veterans Affairs (VA), from December, 1999 to June, 2006. Ms. Martinez was then detailed to the VA as the Acting Chief Technology Officer. In this capacity, Ms. Martinez was responsible for a number of projects including responding to the May data breach incident and other Enterprise Identity Safety Initiatives until March 2007.

Adair Martinez briefed the Board on the follow-up structure set-up after the data breach. Her PowerPoint presentation included the following points:

- Incident Response in the Department of Veterans Affairs = description of trends, metrics, tools of the trade, lessons learned
- Detailed explanation on how the VA responded and the present process in place
- Education programs and training
- Handbook 6500.2
    - Management of Security and Privacy Incidents

- the primary goals of managing data breaches
- The Four Phases of an incident

Chief Privacy Officer Training
Ken Mortenson, Acting Chief Privacy and Civil Liberties Officer, DOJ
Mark Brown, DHHS
Marc Groman, CPO, FTC

Kenneth P. Mortensen is the Acting Chief Privacy and Civil Liberties Officer for the U.S. Department of Justice. He is the former Deputy Chief Privacy Officer of the Department of Homeland Security and a practicing privacy attorney, Mr. Mortensen brings expertise not only in protecting and safeguarding privacy and civil liberties, but also integrating those protections and safeguards into an operational framework for law enforcement and national security. Within the Office of the Deputy Attorney General, he determines appropriate privacy protection collaborating in the development of policy supporting the mission of the Department.

Mark Brown is the HHS Senior Information Security Officer, in the office of the Chief Information Officer. He has been at HHS as a security officer for more than 10 years. He works with implementing the HHS Enterprise Architecture.

Marc Groman serves as the Federal Trade Commission's first Chief Privacy Officer. As CPO, Marc coordinates the FTC's efforts to implement, monitor, and review policies and procedures regarding the safeguarding of all sensitive data maintained by the Commission. In this capacity, he reports directly to the Chairman's Office, serves as the Senior Agency Official for Privacy, and chairs the agency-wide Privacy Steering Committee. He also coordinates the FTC's Breach Notification Response Team.

Dan Chenok gave a brief introduction of the panel of speakers. While the Board is always interested in privacy issues, this presentation stemmed in part from a suggestion from one of the Board's member, Susan Landau, on the required technical training for CPO.

Marc Groman began the discussion by stating that the role of CPO is closely dependent on where the CPO is placed within each agency. The role requires a high level of involvement and is a central role in competency, policy and privacy compliance, counseling to people, and privacy by design. The CPO must have access to the top management. A CPO should have a separate role from the role of CIO while maintaining coordination with the CIO. This will eliminate any potential tension and conflict of responsibilities.

Generally, the panel agreed that the CPO must have knowledge of technology in the areas of compliance, FTC's security, encryption, FISMA, areas of vulnerabilities in the CPO's responsibilities. Apart from the essential technology training and some kind of IT boot camp, the CPO needs to establish his/her credibility, maintain a network with upper management, understand the mission of his/her agency, and should make every attempt to collaborate and recommend the security network so as not to be viewed as a prohibitor. While the CPO does not have to be an expert in every aspect, he/she should have sufficient knowledge and understanding to find the needed answers when the incidence arises.

The panel offered the following suggestions for consideration:

1) to press OMB for more resources and a clear operation plan
2) Privacy training should not be restricted to CPO but be extended to CIO and its personnel.
3) To organize a cross governmental discussion on the roles of CPO and CIO.

Cryptographic Hash
William Burr, NIST Computer Security Division
Group Manager for Security Technology Group
Electronics Engineer

Mr. Burr gave a presentation on the NIST Hash Competition, which included information from John Kelsey who is the senior cryptographers in NIST's Computer Security Division. The technical presentation explained the Hash function, its original function, the properties of Hash function, and work factors. It also provided results for the last four years of the various attacks and illustration of what can be done with collision attacks, the relating problems of hash, the impact of collisions, and NIST Hash function policy.

Mr. Burr's presentation included the Historical background and competition timeline of SHA-3 Hash Competition with a planned submission of a FIPS package to Department of Commerce, 4th quarter of 2012. The panel of judges consists of employees and Guest Researchers at NIST.

The Board asked if NIST has cleared any complications if any non-US is declared winners. Bill shared the complete set of his presentation.

FISMA Implementer Panel
VADM Thomas J. Barrett, USCG (ret.)
Deputy Secretary, Department of Transportation

The Chair, Dan Chenok, thanked Rebecca Leng for arranging for deputy secretary to speak to the Board. The Board has great interest in FISMA, and has heard from CIOs and various critical personnel, but has yet to hear from senior executives. The Secretary stated that security is improving and adapting. As in most security initiatives, a fair amount of time is needed to capture the risks as economic trade data as transaction networks are becoming global. The Department of Transportation (DOT), like many other agencies, has increased utilization of contractors. There are many security concerns and we must fix the mechanical failures, as failure stems mostly from mechanical issues rather than from hackers. With the increase of telecommuting, many people have yet to adopt the security culture because there are insufficient resources to maintain security. DOT needs to foster partnership with other agencies to identify and work through all the issues. Therefore, it is necessary to have a system that is resilient and adaptable to the ever changing and sophisticated software globally.

Board Discussion
Board Members (Lynn McNulty acting chair)

Lynn McNulty agreed to be acting chair for this discussion as the Chair was called away. In summation of today's discussion, the Board noted vast inconsistency and lack of harmonization across all agencies which hinders the government to perform properly. While FISMA and NIST standards are the baseline, the baseline has not been met. It is necessary to set up a baseline recommendation. Implementation of The Privacy act varies from agency to agency and from organizations to organizations. Fundamentaly limiting vulnerabilities will make them more manageable.

Meeting adjourned at 4:50 P.M.

June 6, 2008

Started at 8:30 P.M.
Ended at 3:11 P.M.

Present:
Jaren Doherty
Joseph Guirreri
Rebecca Leng
F. Lynn McNulty
Alex Popowycz
Philip Reitinger
Fred Schneider
Howard Schmidt
Ari Schwartz
Peter Weinberger
Pauline Bowen DFO

Absent:
Brian Gouker
Lisa Schlosser

Visitors, presenters, panelists: 8
Matt Scholl, NIST, Computer Security Division

Meeting began at 8:50 A.M. with a recap of yesterday's discussion by the Chair, Dan Chenok.

FISMA Report Briefing
John Lee, Acting Chief
Information Policy & Technology Branch, E-Gov/OIRA
Office of Management and Budget

The Chair, Dan Chenok, introduced the speaker and the purpose of the presentation. John Lee's presentation included an organization chart of OMB, which was only updated as of last week. He explained the FISMA and privacy straddle between the chief architect and branch chief. The perimeter of the reporting incorporates new FISMA privacy reporting requirements. The report, which originally was scheduled for May 2008, is now scheduled for the end of next week. The reviews primarily are evaluated by policy analysts. There are Five PMA Government-wide Initiatives: 1) Strategic Management of Human Capital; 2) Competitive Sourcing; 3) Improved Financial Performance; 4) Expanded Electronic Government (ensuring the federal government's $71 billion annual investment in IT significantly improves the government's ability to serve citizens; and 5) Budget and Performance Integration. John Lee also touched on the legislative background of e-Government, the goal and responsibilities of FISMA 2002, what are the FISMA reporting requirements, the purpose and advantages of Federal Desktop Core Configuration (FDCC), and the Trusted Internet Connections (TIC).

A discussion ensued on who were the technical advisors to the policy, and whether NIST and the Air Force contributed largely to the initiatives. The Board also discussed the processes that led to implementing FDCC, or any other policies. The Board members were interested in the decision process before implementation of any mandates and policies. They were reminded of yesterday's discussion with CIOs from the Departments of Education and Interior, who raised the issue of funding apportionment often being decided prior to implementation of programs/policies and demonstrating a lack of connection between policies and funding.

John Lee's presentation also included the New FY07 FISMA Reporting Requirements – the privacy related policies and plans are in place. In response to the Board's query regarding ensuring that OMB receives accurate data, John Lee stated that agency heads are held accountable for all submitted reporting, and GAO is responsible for ensuring the integrity of the data. The Board was requested to check the White House's Web site to confirm that data accuracy data had passed, and any documents relating to any persons are considered as PII.

In summary, the speaker agreed that it is good to listen and hear other opinions and he was glad to hold discussions before the Board. He will take under advisement technical guidance for implementation of future policies/mandates, as well as a suggestion to integrate management priorities and budget execution more closely.

FISMA Program Phase II
Ron Ross
NIST, Computer Security Division

Dr. Ron Ross is a senior computer scientist and information security researcher at the National Institute of Standards and Technology (NIST). His areas of specialization include security requirements definition, security testing and evaluation, and information assurance. Dr. Ross currently leads the Federal Information Security Management Act (FISMA) Implementation Project for NIST, which includes the development of key security standards and guidelines for the federal government, contractors supporting the federal government, and the United States critical information infrastructure. His recent publications include Federal Information Processing Standards (FIPS) Publication 199 (the security categorization standard), FIPS Publication 200 (the minimum security requirements standard), NIST Special Publication 800-53 (the security controls guideline), NIST Special Publication 800-53A (the security assessment guideline), and NIST Special Publication 800-37 (the system certification and accreditation guideline). Dr. Ross is also the principal architect of the NIST Risk Management Framework that integrates the suite of FISMA security standards and guidelines into a comprehensive enterprise-wide information security program.

Dr. Ross described to the board the process of how FISMA moved into phase II and what phase II intends to accomplish, the overall process of managing risks and defining risk faced by federal information systems supporting defense, civil and intelligence agencies with the federal government, how does the private sector information systems support US industry and business, and information systems supporting critical infrastructures within the US. He stated that we need to examine the threat situation and remember that risk-based protection strategy is about drive security requirements, and it should be a highly flexible implementation. Certification and accreditation are all about managing risk and not about just securing your system as the focus to whether or not you can survive any attack. The generalized model for a Unified Framework for information security applies to all FISMA documents. OMB has been briefed by NIST and has been involved in every step, including collaboration with NIST in many other initiatives.

Dr. Ross' presentation was sub-divided into the following Transformation –
1) Reflecting the C&A Process within the Risk Management Framework, which involves four phases – Initiation, Certification, Accreditation, and Continuous Monitoring
2) Extending the Risk Management Framework to the Enterprise
3) Incorporating Trust Models into Enterprise Risk Management - Trustworthiness is related to preserving the confidentiality, integrity and availability of the information being processed, stored, or transmitted by the system. Trustworthiness defines the security state of the information system at a particular point in time and is measurable.
4) Integrating Risk Management into Enterprise Architectures and System Development Life Cycle Processes

Dr. Ross explained that when you try to build a program, it is critical to recognize two factors affecting trustworthiness – security functionality and security assurance:
Trusted relationships - determining risk to the organization's operations and assets, individuals, other organization, and the Nation; and the acceptability of such risk. The objective is to achieve visibility and an understanding of the prospective partner's Information security programs, while establishing a trust relationship based on the trustworthiness of their information systems.

Dr. Ross continued to explain FISMA Phase I and II. The timeline for phase II is 2007 through 2010. The mission is to develop and implement a standards-based organizational credentialing program for public and private sector entities to demonstrate core competencies for offering security services to federal agencies. When looking at a broader perspective, everything is tied to a customer base, with reference to the produce and service supplier, support tools, training initiative and ISO Harmonization. The process invested extensive mapping from FISMA standards and guidelines to ISO 27001, and much effort to

provide the necessary tools and resources for agencies to use. There are a number of NIST special publications relating to FISMA which are under review and are made available for public comments. The Board could review and provide appropriate comments.

The State of Telecommuting: Privacy and Security Survey Results Discussion
Sagi Leizerov, Ph.D, Information Technology Enablement Center, Ernst & Young LLP

Sagi Leizerov is a leader in Ernst & Young's privacy practice, providing the firm's clients with privacy assurance and advisory services. Sagi has worked with organizations from both the private and the public sectors on privacy-related issues and has served clients in the online, computer, financial, human resources, and healthcare industries.

Dan Chenok explained that the purpose for this discussion/presentation is based upon the Board's interest in emergency response privacy, which also is the charter and Board's function. He then asked Ari Schwartz to introduce the speaker, Dr. Sagi Leizerov. Ernst & Young approached Ari Schwartz to conduct the survey on telecommuting. Dr. Leizerov was to present the results of the survey which includes the following subjects:
1) What are the organizations doing?
2) What are the policies that organizations have in place?
3) Outline of telecommuting
4) Why telecommuting?
5) Key observation and practices to adopt
6) The challenges created by telecommuting

There are fifteen sections in this survey and the survey respondents were from 73 federal organizations in the US, Canada and Europe; and included ten industries with an average of 50,000 employees. Dr. Leizerov presented the results and provided the practices to adopt in response to the findings:

- Most respondents allow employees to handle personal information at home, but only 50% of the respondents developed guidelines for telecommuting and provided guidance to their employees on the topic.
- Many devices used at home: telecommuters usually use their own personal computers and PDAs at home for work purposes.
- Authentication and emerging technologies: few organizations have adopted thin-client terminals or biometric authentication for telecommuters. It is important to start assessing the adoption of biometric technology for local authentication
- Wireless security: the use of wireless internet connections is a common practice, but it is uncommon to require telecommuters to use wireless security measures.
- Hard-drive encryption is common, but of little help when employees use their home computers for work.
- Imposing any limitations on telecommuters regarding the use of e-mail and external and services are not common.
- It is uncommon to impose limitations on downloading software and using peer-to-peer file-sharing applications
- Monitoring telecommuting: those organizations with a higher number of telecommuters are more likely to monitor the telecommuters' use of tools and technology.
- Survey key conclusion: 1) telecommuting risks are not effectively managed today, and 2) there is a definite and urgent need for action.
- What are the legal implications of sending sensitive information off-site? Survey is rolled out later this month for Capitol Hill employees.

Authentication of the Future – Looking Ahead To Advise NIST and OMB
Board Members

DISCUSSION POSTPOSED

Public Participation
There were no requests for public participation.

Wrap-Up and Agenda Review for September 2008 Meeting

The Board approved two letters.

- Essential Body of Knowledge (EBK) - Dan Chenok revisited a motion taken during a meeting in December regarding the Board's desire to write to OMB regarding its concerns with appropriateness of the framework and the lack of any special certification of privacy for individuals. Rebecca Leng suggested that the Board should consider writing to the new administration. A final agreement was reached to define an implementation plan for the document. A motion to proceed was taken with 7 Board members in favor and 4 abstaining.

- FISMA Metrics – The Chair initiated a discussion on writing to OMB re. FISMA Metrics. The Board agreed that it is worthwhile to continue monitoring the progress of FISMA. But they also agreed that FISMA is paperwork intensive and the measure is proving to be insufficient. A motion was taken with 11 Board members in favor and 1 abstaining.

The Board revisited yesterday's discussion on CPO and CIO. The conclusion was that there is no consistency in the positioning in the organization chart and authority level of these positions among all agencies. If it is to include CPO under CIO, it is not rational to consider that CPO is only involved in privacy issues. Most importantly, it does not really matter where CPO is placed in an organization chart as long as CPO can function effectively. It would be worthwhile to put together an industry panel of CPOs for the next meeting and/or to write a white paper on training for CPOs.

Telecommuting – it is worthy to include this topic as part of a recommendation letter to the transition administration. As we are increasingly replacing desktops with laptops, telecommuting may gradually gain sufficient importance to warrant attention for awareness. Telecommuting has lots of consequences relating to privacy and security. The focus is information and not applications. The Board will keep this subject for future review.

For the meeting agenda in December, Lynn McNulty, Joe Guirreri, Alex Popowycz, and Fred Schneider are to prepare a draft letter stating the Board's concerns and observations to the transition team after the upcoming election.

CSIS paper – the Board shall review the paper and include it for discussion in the next meeting's agenda.

Rebecca Leng reminded the Board to send a Thank You letter to the Deputy Secretary, Department of Transportation.

The Chairman adjourned the meeting at 3:11 P.M.

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting.

Daniel Chenok
ISPAB Board Chairman