INFORMATION SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

DoubleTree Hotel and Executive Meeting Center
1750 Rockville Pike
Rockville, MD

June 7-9, 2005

Tuesday, June 7, 2005

Board Chairman, Franklin Reeder convened the Information Security and Privacy Advisory Board Meeting (ISPAB) for its second meeting of the year at 8:40 a.m. Other members present during the meeting were:

Bruce Brody [6/8 only]
Daniel Chenok
Morris Hymes
Susan Landau
Rebecca Leng
Steve Lipner [via telecon 6/8 only]
Sallie McDonald
Lynn McNulty
Alexander Popowycz
Leslie Reis
John Sabo
Howard Schmidt

The meeting was held in open public session. There were ten members of the public in attendance during the meeting.

Role of the Chief Privacy Officer

The Board conducted a two-part panel session on the role of Chief Privacy Officers (CPO) in order to gain information on the pros and cons of CPO models that currently exist both within the private sector and the federal government. Panelists that participated in the private sector session were: Harriett Pearson, Chief Privacy Officer, IBM Corporation; Douglas Miller, Executive Director, Integrity Assurance, America Online, Inc.; and, Christopher Zoladz, Chief Privacy Officer, Marriott Corporation. Participants representing the federal sector were: Zoe Strickland, Privacy Officer, U.S. Postal Service; Barbra Symonds, Privacy Officer, Internal Revenue Service; John Fanning, former Privacy Advocate, Department of Health and Human Services, Robert Veeder, former Chief Privacy Advocate, Internal Revenue Service. Each of the private sector participants presented a brief overview of their organization and their respective privacy management structures. They discussed processes in acquiring channels of trust and identified skill sets that have been effective for their operations. Each of them expressed the opinion that privacy needs to be an integral part of the business strategy. The federal government representatives also described the organizational structures their respective government affiliates. Each panelist offered their viewpoint on the oversight, review and requirements that a government privacy official has/should have. They also expressed their concern that agencies needs vary because they differ greatly in mission, organization, size and types of personal information that is gathered. It was the consensus of the government panelists

that this Board should contribute to the current government privacy debate and offered several issues that could be addressed. During the Board discussion, each of the Board members stated their opinions and observations from what they had learned from the panel participants. Chairman Reeder volunteered to prepare a draft white paper on Chief Privacy Officer guidance and draft a suggested framework for managing privacy activities within the federal government.

Board Business

Chairman Reeder took this opportunity to acknowledge the significant contributions made by John Sabo during his tenure as a member of the Advisory Board. Mr. Sabo's appointment term expires as of June 30, 2005. Chairman Reeder presented Mr. Sabo with a framed certificate of appreciation from the National Institute of Standards and Technology and the Advisory Board in recognition of his stellar service to the mission of this Advisory Board.

The meeting was recessed for the day at 5:00 p.m.

Wednesday, June 8, 2005

Chairman Reeder reconvened the meeting at 8:40 a.m. with a review of the actions from the first day of the meeting.

Privacy Act Revisited

Board members Leslie Reis and John Sabo served as the facilitators for this session. Mr. Sabo opened the discussion with a brief review of the Privacy Act and a review of the Board's 2003 white paper on the subject. Professor Reis addressed several options that the Board may want to consider as Board recommendations such as identifying issues and the need for implementation guidance. It was noted that the legislative intent and effectiveness of the Privacy Act of 1974 has been eviscerated over time. Technologies and agencies' needs have changed. The world of technology then does not exist today. The members discussed these issues and identified their goals and targeted work product. Chairman Reeder volunteered to have informal conversations with key parties on some of the issues the Board raised. The Board will also work to establish possible collaboration with the Department of Homeland Security's Data and Privacy Advisory Board. Board member John Sabo is a member of the DHS Advisory Board and volunteered to serve as a liaison to facilitate this action. Dan Chenok, Lynn McNulty and Leslie Reis volunteered to work with Chairman Reeder on the Privacy Act task.

Department of Homeland Security (DHS) National Cyber Security Division Update

*NOTE: Board member Steve Lipner joined the meeting for this session via teleconference.

Mr. Andy Purdy of the National Cyber Security Division at DHS discussed two major DHS priorities, i.e.; building a national cyber response system and the National Cybersecurity Strategy Plan. These two efforts map the capabilities of the agency and what of those capabilities need to be tied more formally to a U.S. CERT on a 24/7 basis. Mr. Purdy's briefing also covered discussion on additional initiatives being pursued by DHS in the area of cyber defense capabilities, risk management, software assurance, telecommunications and NIAP direction. Chairman Reeder asked Mr. Purdy if the Board could be of value to DHS in looking at those issues that would make federal, non-classified systems more secure. Mr. Purdy suggested the following topics for the Board's consideration: security line of business and how that is going to be set up; metrics that make a difference so that agency progress can be tracked over time; forming a team to work on developing those metrics; the challenge of best practices; the question

of whether DHS needs to supplement some of the NIST standards to cut across the sectors, identification of high-level principles; configuration setting issues; and, privacy issues such as development of guidance input advice from a policy standpoint to raise accountability. Mr. Purdy also mentioned DHS' efforts in the security line of business project. DHS is working to develop the metrics that measure cyber security effectiveness. He invited the Board to work in an ex-officio capacity with DHS on this effort.

Board Business

The motion was made and seconded to approve the minutes of the March 2005 Board meeting. The minutes were unanimously approved.

Department of Commerce (DOC) Radio Frequency Identification (RFID) Effort

Mr. Douglas Devereaux of the Technology Administration briefed the Board on the RFID program activities at DOC. **[Ref. #1]** He discussed the DOC-issued paper "Radio Frequency Identification, Opportunities and Challenges in Implementation that they produced in April 2005. The paper provides a summary of RFID technology, the policy issues surrounding the use of the technology, and explores the technology's implications for international trade, standards, spectrum, small- to medium-sized enterprises, intellectual property rights, and economic growth. Mr. Devereaux also discussed their April 6, 2005 Workshop: RFID in 2005: Technology and Industry Perspectives. The objectives of the workshop were to engage stakeholders and industry in discussions that included the benefits of RFID technology, technology development efforts, current and future applications, privacy and security considerations and industry's experiences in implementing RFID technology. In his closing remarks, Mr. Devereaux stated that the DOC is interested in offering itself as a resource to members of the Board and to their particular interests; through partnering, on proposed studies, and through availability on issues related to RFID.

Government Line of Business Initiative Overview

Mr. Mike Smith of the Department of Homeland Security presented a brief overview of the recently established initiative. The three themes expressed throughout the initiative were consistency, efficiency and improvement of security. He reviewed the vision of the effort and discussed the goals and objectives they hope to achieve. The Board discussed possible actions that they could take on this issue based on their observations at this time. After further deliberation, the Board withdrew an earlier motion to develop and send a letter to OMB expressing their concerns. Instead, the Board requested to be updated on this initiative at its September meeting.

Public Participation Period

There were no requests to speak from the public attendees.

The Chairman recessed the meeting at 4:45 p.m.

Thursday, June 9, 2005

Acting Chairperson, John Sabo, reconvened the meeting at 8:45 a.m. A motion was made and unanimously approved to send a letter to the Director of NIST and the Deputy Assistant Secretary and Chief Information Officer of the Department of Treasury, to recognize the outstanding service Ed Roback performed for the National Institute of Standards and Technology and the Computer Security Division and the federal government as a whole. The Board wishes Mr. Roback great success in his new assignment with Treasury.

Presentation on Phoenix Technologies, Ltd.

Board Member Lynn McNulty introduced Mr. Albert E. Sisto, President and CEO of Phoenix Technologies. Mr. Sisto presented an overview of the company that covered its vision, business strategy and products. Founded in 1979, Phoenix Technologies Ltd. is a developer of core system software, tools and applications that define, enable, protect and recover PC server, information applicant and embedded systems. Mr. Sisto also distributed and discussed a white paper on Phoenix's cME TrustConnector, a software product that enables seamless, built-in authentication of x86 devices to a network while enhancing the protection of identity credentials for Windows applications.

SCADA Briefing

Mr. Keith Stouffer of NIST's Manufacturing Engineering Laboratory presented a briefing on NIST industrial control system security activities.**[Ref. #2]** The US National Plan for Information Systems Protection and a report by the Government Accountability Office cited industrial control systems as critical points of vulnerability in America's utilities and industrial infrastructures. NIST is working with industry to develop standards and test methods to enable the integration of security engineering in to the industrial automation life cycle, including design, implementation, configuration, maintenance and decommissioning. The NIST industrial control systems (ICS) security activities Mr. Stouffer discussed included a process control security requirements forum, SCADA protection profiles and an ICS vendor security checklist program. The program's efforts include collaboration with two other NIST labs; i.e., the Electronics and Electrical Engineering Laboratory and the Information Technology Laboratory. NIST also collaborates with the Department of Homeland Security and the Department of Energy. Additionally, there is testbed collaboration with the National SCADA Testbed (Idaho National Engineering and Environmental Laboratory and Sandia National Laboratory). The Board is interested in following this activity and invited Mr. Stouffer to attend the September Board meeting for another briefing.

Review of Actions for September 13-15, 2005 Board Meeting

The Board discussed items that they wanted to pursue for their September meeting. These items included:

- Privacy Act – Board's Next Steps
- Role of Government Privacy Officers – Findings and Recommendations
- Update on OMB's Government Line of Business Initiative
- Review and Modification of Board's Work Plan Tasks
- NIAP Final Report Briefing
- Update on Activities of the NIST Computer Security Division
- Possible Collaboration between Board and Department of Homeland Security's Data Integrity and Privacy Group

There being no further business, the meeting was adjourned at 11:50 a.m.

Ref. 1 - Devereaux Presentation
Ref. 2. – Stouffer Presentation

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting.

Franklin S. Reeder
Chairman