INFORMATION SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

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

December 6-7, 2005

Tuesday, December 6, 2005

Board Chairman, Franklin Reeder convened the Information Security and Privacy Advisory Board Meeting (ISPAB) for its fourth meeting of the year at 9:00 a.m. Other members present during the meeting were:

Daniel Chenok
Morris Hymes
Rebecca Leng
Steve Lipner
Sallie McDonald
Lynn McNulty
Alex Popowycz
Leslie Reis

Board Member Susan Landau participated via teleconference for a portion of the meeting. Member designate Joseph Guirerri was also in attendance.

Chairman Reeder reported on his recent meeting with the new Director of the National Institute of Standards and Technology (NIST), Dr. William Jeffrey. Mr. Reeder said that Dr. Jeffrey was very interested in cyber security and the Board's earlier work in the area of metrics. Dr. Jeffrey would like for the Board to consider this topic as one of their work issue items for the coming years. Mr. Reeder also discussed the upcoming personnel changes within NIST's Information Technology Laboratory (ITL). Professor Shashi Phoha is returning to an academic position at Carnegie Mellon at the end of the month. Cita Furlani, current Chief Information Officer for NIST, will serve as Acting Director of the ITL upon Dr. Phoha's departure.

Board Member Lynn McNulty presented a brief update on some of the Homeland Security Presidential Document (HSPD) #12 activities. He indicated that NIST was receiving positive comments on their efforts to get the Personal Identity Verification (PIV) Standard produced. Mr. McNulty also pointed out the significant hidden costs involved to implement this standard and that the Department of Defense would be one of the major departments financially burdened by the changes brought about by the PIV standard.

Board member Morris Hymes gave a brief update about on-going activities involving the NIAP review report. He reported that the Department of Homeland Security and the Department of Defense had tasked the Institute for Defense Analyses to prepare a report on the NIAP program activity. The report was completed in November 2005 and then reviewed by the Office of Management and Budget. The report was in the editing phase. When approved, it would be issued as an Administration document and not one that would be sent out for public comment. Mr. Hymes also said that the Government Accountability Office was conducting a survey that related to the NIAP activity. The Board will continue to follow these activities and hold discussions at future Board meetings.

Board member Sallie McDonald reported that the Department of Homeland Security was undergoing a rearrangement of former Departmental structure and reporting functions. She also reported that she is participating in a one-year Intergovernmental Personnel Act (IPA) assignment with George Mason University working on their critical infrastructure program.

Board members Lynn McNulty and Morris Hymes suggested the Board may have an interest in gather information on lessons learned in the information technology and cyber fields as a result of the effects of the disaster caused by Hurricane Katrina.

Board member Rebecca Leng discussed the status of agencies reports on FISMA. She also discussed the activities leading up to the FY06 input to the FISMA report. The Board requested that OMB be invited to the next meeting to give the Board an update on the FISMA agencies reporting issue. Morris Hymes suggested that the Board review the FISMA questions pertaining to privacy issues and possibly recommend additional questions for OMB's consideration.

NIST Hash Function Standards, Status and Plans

Mr. Bill Burr, Manager of the Security Technology Group at NIST briefed the Board on recent Cryptographic Hash Standards. [Ref. #1] He discussed hash function applications such as digital signatures, keyed hashes and key derivation. Digital signatures are perhaps the most demanding of the many applications for hash function because they are potentially subject to collision attacks. The two hash functions that are currently in used today are the MD5, invented by Ron Rivest in 1992 and SHA-1, developed by NSA in 1995. Mr. Burr stated that NIST plans to end federal use of SHA-1 by the end of 2010 in favor of SHA-256 to prevent future brute force collision attacks. He also reported on the NIST Hash Workshop that was held on October 31 – November 1, 2005. Approximately 180 people attended the workshop. The workshop focused on the status of the attacks on SHA-1 and SHA-2, new designs and design criteria and the identification of the requirements for a new hash standard. It was determined that eliminating MD5 was a high priority, and that it was acceptable to continue to use SHA-1 for a few more years in all applications but new applications must use something else. SHA-1 was not badly broken but needs to be replaced. NIST plans to phase out all 80-bit crypto by the end of 2010. FIPS 180-2, Secure Hash Standard, is already in place with SHA-224, SHA-256, SHA-384 and SHA-512.

Use of SHA-1 in PIV/PIV Biometric Decision

Mr. Curt Barker of NIST's Computer Security Division presented a briefing on the background and current status of the use of hashing algorithms in the Federal personal identity verification program and biometrics storage format selection for the Federal personal identity verification program. [Ref. #2] He addressed the processing concept and programmed changes in the key hash size requirement and other uses of hashes. The revision to FIPS 201 PIV Standard covers interim issuance based on criminal history checks and electronic indication of interim status. Conformance testing of cards built to FIPS 201/SP800-73, Interfaces for Personal Identity Verification, is currently underway as is formal National Voluntary Laboratory Accreditation Program (NVLAP) accreditation of NIST Personal Identity Verification Program (NPIVP) laboratories. Mr. Barker reported that biometric decisions for NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification, pertaining to biometrics storage formats would be based on ANSI/INCITS 378 and EER compatible with TSA requirements.

Federal Privacy Policy Review Discussion

At the September 2005 Board meeting, Board members Leslie Reis, Lynn McNulty, Dan Chenok and Frank Reeder volunteered to work together on the issue of federal privacy policy today as it relates to the Privacy Act of 1974. Professor Reis reported on her conversation with former Board member, John Sabo, and the activities of the Department of Homeland Security (DHS) Data Integrity and Privacy Advisory Board. Mr. Sabo is now a member of that Advisory Board. The DHS Board is also planning to look into the same issue. Professor Reis discussed the legal and policy framework issues and the development of an action plan with milestones and deliverables. The Board agreed on the following Statement of Scope: to examine the extent to which changes in the nature and use of information technology by federal agencies over the years creates a need for revisions to the existing legal and policy framework of the Privacy Act. It was suggested that the Board obtain a copy of agencies' privacy impact assessment reports to review and to engage the General Accountability Office to gather information. Another suggestion was made to initially review the standard privacy principles and determine if these principles are still adequate and/or identify existing gaps. Board members Leslie Reis, Dan Chenok, Howard Schmidt, Lynn McNulty and Frank Reeder will continue to support this review effort.

International/Regional Security Initiatives: Bilateral and Multilateral Outreach re Critical Infrastructure Protection (CIP) / Homeland Security

Mr. Daniel Hurley, Director of Critical Infrastructure Protection at the Department of Commerce, briefed the Board on the Department's bilateral and multilateral outreach program. [Ref. #3] He presented an overview of the program's strategic goals. Homeland security components cover national defense, law enforcement and economic security. The Department's economic security goal is to ensure that critical infrastructure protection policies, programs and activities support strong and security economy. Historically, Commerce has had existing CIP initiatives within the Bureau of Industry and Security, the International Trade Association, the National Institute of Standards and Technology and the National Telecommunications and Information Administration. CIP bilateral-multilateral activities have been in place with 12 foreign countries such as Australia, Egypt, Hungary and the Netherlands since 2000.

The meeting was recessed for the day at 4:23 p.m.

<u>Wednesday, December 7, 2005</u>

Chairman Reeder reconvened the meeting at 8:44 a.m. The Board reviewed the activities of the first day of the meeting Board Member Lynn McNulty suggested that the Board have a briefing at the March meeting on the subject of the National ID effort from a representative of the National Association of Motor Vehicles or the Department of Transportation. The Board would also like to meet with OMB to discuss the implementation requirements/process of the HSPD#12 required FIPS 201. The Board would also like to hear from OMB on the security line of business initiative, general status of the implementation of HSPD #12, and the FY07 budget process.

Computer Security Division Update

Joan Hash, Acting Chief of NIST's Computer Security Division (CSD), spoke to the Board about the activities of the Division. Ms. Hash reported that the Division had experienced a good budgetary period and that recruitment opportunities were also strong. Activities as a result of HSPD#12 were continuing and the Division was actively involved in FISMA related programs. The expectation is that this scenario should continue into FY06. Ms. Hash indicated that the Division would welcome the Board's input on identifying more collaborative efforts that the Division could engage within ITL in its entirety. The Division needs to communicate their strategy involving the science environment. Chairman Reeder indicated that the Board is very concerned about the Division's communicating externally with outside constituents. ITL is generally different from the other NIST labs and the Board recognizes that computer security and the Division are not synonymous.

Cita Furlani, Acting Director-designate for ITL, mentioned that a NIST effort is underway for defining the U.S. measurement system. How would you measure and what would you measure are key questions being addressed. Ms. Furlani invited input from the Board on this issue and will provide them with information on the project for their consideration. Mr. Reeder commented on two measurement challenges that he observes, (1) how does NIST decide what are the right points, and (2) are the correct things being measured in FISMA reporting and the Congressional report cards exercises.

The Division is also engaged in the OMB Line of Business initiative.

Board member Leslie Reis remarked that the ITL marketing strategy both internally and externally is an area that the Board may be able to offer some thoughts. Ms. Furlani said that she would welcome the Board's input.

The National Vulnerability Database

Mr. Peter Mell of the NIST Computer Security Division briefed the Board on the National Vulnerability Database (NVD) that he created at NIST. [Ref. #4] The NVD is a comprehensive information technology vulnerability database that integrates all publicly available U.S. government vulnerability resources and provides links to industry resources. It is built upon the Common Vulnerability Evaluation (CVE) standard vulnerability nomenclature and augments the standard with a search engine and reference library. Mr. Mell also provided the Board with an overview of the Common Vulnerability Scoring System (CVSS). It is a universal language that conveys vulnerability severity and helps determine urgency and priority of response. It solves the problem of multiple incompatible scoring systems in use today.

Updates on the Federal Enterprise Architecture Program

Mr. Dick Burk, Chief Architect and Director of the Federal Enterprise Architecture (FEA) Program at the Office of Management and Budget (OMB) presented a briefing on the FEA Program. [Ref. #5] He discussed the future direction of citizen-centered services and provided an overview of the historical approach that primarily focused on agency-specific services and the future approach that focuses on common services, commercial provides in addition to agency-specific services. OMB's role is to encourage agencies to become more effective and efficient. FEA's five Reference Models give definition to the following areas: performance, business, service components, data and technical. It is a business-driven approach, component-based architecture. The Line of Business and Services covers management and government resources, services to customers and components of services that cut across the lines of business. The programs concept of operations includes three main areas: Architect -- develops and maintains enterprise architecture, reviews, reconciles and approves segment architecture for agency's' core lines of business and common IT services; Invest -- selects IT initiatives to define the agency's IT investment portfolio, controls IT investments, and evaluates IT investments; and, Implement – develops and maintains segment architecture, develops IT program management plan and executes IT projects. E-Gov is in three main areas: (1) lines of business operational and planning phase, (2) E-Gov initiatives, and (3) SmartBUY Agreements. In the area of IPv6 implementation, OMB Memorandum 05-22 directs agencies to successfully transition their network backbone to Internet Protocol version 6 (IPv6) by June 2008. Agencies are also required to complete specific inventories and progress reports in 2006. Mr. Burk also reviewed the capability areas covered in the EA Assessment Framework 2.0. He reviewed FEA's principle on security and privacy and the rationale and implications associated with them. There are nine service components that form the reference model for security management services. They are identification and authentication, access control, encryption, intrusion detection, verification, digital signature, user management, role/privilege management and audit trail capture and analysis. The Information Systems Security Line of Business effort has defined four common solution areas: training, FISMA reporting, situational awareness and incident response and security solutions. The goal is to establish three Centers of Excellence for each of the four common solutions. The Lines of Businesses are projected to save over $5 billion dollars in the next 10 years.

NIST's Guidance on IPv6

Sheila Frankel of NIST's Computer Security Division presented an overview on the NIST effort on IPv6. [Ref. #6] Her briefing focused on the effects of the OMB directive on IPv6 and a review of the outline of NIST's IPv6 guidance document. The advantages of IPv6, both real and perceived, include increased number of addresses, increased ease of network management and configuration, simplified/expandable IP header, end-to-end/peer-to-peer communications, mobility, security, multicast/multimedia, and quality of service. Advantages of IPsec include the ability to implement once, in a consistent manner, for multiple applications, centrally controlled access/security policies and the ability to enable multi-level, layered approach to security. IPsec also offers security that provides data origin authentication, connectionless integrity, replay protection, confidentiality (encryption), traffic flow confidentiality and access control. The NIST IPv6 guidance document will address IPv6 protocols, core services, security and privacy and deployment such as transition, integration, configuration and testing.

Board Administration Discussion Period

The motion was made and seconded to approve the minutes of the December 2005 Board meeting, as amended.

There was discussion of meeting dates for 2006. The Board will continue to hold meetings in March, June, September and December. The Board will consider holding the meetings on Thursday's and Friday's to be more accommodating to participation by the academic members of the Board. The Board Secretariat staff will distribute a list of proposed dates for 2006.

Action/agenda items for the March 2006 meeting were identified. They included a session on software assurance, update by OMB on computer security related activities and FISMA reporting, review of professional credentialing activities at DOD, briefing on the DOD-DHS NIAP review report, briefing on the National ID effort, and update on the Board activity on review of the federal privacy policy.

There being no further business, the meeting was adjourned at 5:07 p.m.

Ref. 1 – Burr Presentation
Ref. 2 – Barker Presentation
Ref. 3 - Hurley Presentation
Ref. 4 – Mell Presentation
Ref. 5 – Burk Presentation
Ref. 6 – Frankel Presentation

/s/

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate
summary of the meeting.

/s/

Franklin S. Reeder
Chairman