INFORMATION SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

Washington-North Gaithersburg Hilton Hotel
620 Perry Parkway
Gaithersburg, MD

September 28-30, 2004

Tuesday, September 28, 2004

Board Chairman, Franklin S. Reeder, convened the Information Security and Privacy Advisory Board Meeting (ISPAB) for its third meeting of the year at 8:30 a.m. In addition to Chairman Reeder, Board members present were:

Bruce Brody
Charisse Castagnoli
Susan Landau
Rebecca Leng
Morris Hymes
Sallie McDonald
Leslie Reis
Howard Schmidt

The meeting was held in open public session. Mr. Reeder provided the Board members with an update on the status of the membership appointments to the Board. He announced that the appointments for Rich Guida and Charisse Castagnoli would expire prior to the December Board meeting. Mr. Reeder also stated that member Lynn Bruneau had resigned from the Board due to unanticipated work commitments. The Board Secretariat staff will begin the process of seeking candidates to fill these vacant Board positions.

Work Plan Status Updates

Work Plan Item: FISMA
Board Member Bruce Brody discussed FISMA and how its implementation could improve the computer security posture of various agencies. Mr. Brody believes that this is an excellent opportunity for the Board to weigh in on in the months ahead, especially in the area of responsibilities for federal agencies CIO authority. Mr. Reeder indicated that Congressional staff had also expressed an interest what the Board's thoughts were on this topic. .

Work Plan Item: Customer Relations Management (CRM)
Board Member Leslie Reis reported that she had been working with research associate Adam Hicks to prepare a summary of the Board's previous discussions on this topic and the work that Mr. Hicks had done independently. Professor Reis stated that she would prepare an executive summary for the Board's review and comments on the next steps to take on this issue.

Work Plan Item: National Information Assurance Program (NIAP)
Board Member Morris Hymes suggested that the Board review results of the NIAP study conducted by the Institute for Defense Analysis. This would allow the Board to determine if NIAP was the best model, how to drive the vendors to that model, and review any policy structure in place.

The Board members decided to add one more work item to their existing list: Privacy Act Revisited. They will continue to build upon the findings and recommendations of their 2002 privacy report. A dedicated session on this topic will be planned for the March 2005 Board meeting.

NIST Outreach Efforts

Board Member Susan Landau lead a discussion on how to market the Board's recently issued Computer Security Division (CSD) funding report and more specifically, how do market the good works of the Division. Three areas that the Board should examine are what does NIST do in the outreach area and what are the statistics associated with such a function; discover what the other agencies know or don't know about the Division and NIST and their efforts and what is CSD doing to improve the CSD website. This topic will be part of the March 2005 meeting agenda.

Potential FISMA Enhancements
Common Security Programs, Capabilities and Tools

Board member Bruce Brody reported on some possible government-wide information security enhancements **(Ref. #1)**. Mr. Brody suggested that an agency's security program evaluation done following the language of FISMA alone might not adequately measure and credit enterprise-wide security enhancements. The CIO community may have the best leverage to promote a more practice-oriented evaluation. Mr. Brody offered the Board several potential recommendations for their consideration on this topic. Chairman Reeder and the Board members believe that this is an important area where they can make an important contribution. The Board will seek the advice of other sources as they go through the development process.

OMB Updates

Glenn Schlarman, Chief of the Information Policy and Technology Branch talked with the Board about the current computer security activities ongoing at OMB. Mr. Schlarman also addressed OMB's activities in the privacy area. He stated that the E-Government Act basically left the Privacy Act intact. OMB is looking at government privacy impact assessments. Executive Order 13353 created the Civil Liberties Board to look at the issues of the protection and security of sharing information in a timely fashion. This new Board is co-chaired by the Department of Justice and the Department of Homeland Security. It looks at privacy policies, reviews complaints and refers them to appropriate venues for resolution. OMB is working closely with this group on the privacy issues. Mr. Schlarman suggested that the ISPAB schedule a briefing by the Civil Liberties Board and extend an offer to work with them in the area of privacy. Executive Order 13356 calls for OMB to lead an information systems council to develop a plan to address the technological problems associated with sharing information. The plan is due to the President on December 25, 2004.

Next, Mr. Schlarman commented on the remarks made by Mr. Brody on FISMA and security enhancement across the agencies. He found the ideas presented interesting and he will take these suggestions back to OMB for further consideration. Mr. Schlarman encouraged Mr. Brody to pursue the concept of a security line of business approach and hoped that a privacy line of business approach would follow.

Mr. Schlarman was asked about the size of his current staff. He reported that he has 13 FTE and one privacy program employee in his Branch. They work in the areas of computer security as its relates to government-to-government and government-to-citizen.

Briefing on FCC Regulation of the INTERNET

Board member Morris Hymes introduced Mr. Harold Fuchtgott-Roth of Fuchtgott-Roth Enterprises. Mr. Fuchtgott-Roth was also the former Commissioner of the Federal Communications Commission (FCC). Mr. Fuchtgott-Roth's presentation focused on the difficulty that the FCC has in regulating the Internet. He noted some of the statutory terms governing telecommunications. Telecommunications is not often referred to alone; it is usually teamed up with another term such as telecommunications services. Information is not defined in the current statute but the term information service is. There are five areas where the Federal government is grappling with how to pursue regulations on the Internet. One area is definitions. Reciprocal compensation is another area. The others are CALEA, regulation of the Internet within the international arena and domain name registration and coordination. Mr. Fuchtgott-Roth indicated that there is no legislative push at this time to resolve any of these concerns.

Federal Enterprise Architecture Update

Board member Sallie McDonald led a briefing on the Federal Enterprise Architecture (FEA) project. Eileen Becker of Booz Allen also participated in this briefing. **[Ref. #2]**. Ms. McDonald stated that there is a need for an additional view of the FEA that addresses and highlights information security and privacy. The FEA security and privacy profile is a multi-phase collaborative effort between the government and industry. The first phase of this profile was produced in July 2004. Phase II has been called for by the CIO Executive Committee so that more detailed guidance on security and privacy for process owners, managers and other decision makers can be developed. Phase II will also leverage the NIST guidance and use a scenario to validate the FEA security and privacy profile. A methodology will be developed and presented to the CIOs by the end of December 2004.

The meeting was recessed at 4:50 p.m.

Wednesday, September 29, 2004

Chairman Reeder reconvened the meeting at 8:35 a.m.

The first scheduled speaker for the day, Amit Yoran of the Department of Homeland Security, was unable to attend. There was an adjustment to the meeting schedule for the remainder of the day.

Chairman Reeder expressed his appreciation to both Mr. Guida and Ms. Castagnoli for their excellent contributions to the Board. On behalf of the entire Board, he extended special thanks to each of them.

Trusted Computing Group (TCG) Best Practices

Board member Susan Landau briefed the Board on a draft document on best practice principles developed by the TCG's Best Practices Working Group **[Ref. #3]**. The document's purpose is to articulate the underlying design principles so as to clarify choices and guide developers to the purpose of TCG technologies. The intended audience for it is users and develops of TCG technology. The fundamental principle is the separation between Owners vs. User. There are six general principles: security, privacy, interoperability, and portability of data, controllability and ease of use. Dr. Landau reviewed each of these areas and pointed out her concerns in several areas. She encouraged the members to offer their comments before the end of the review period.

Proposed Federal Information Processing Standard on Personal Identification Verification (PIV)

Mr. Curt Barker of NIST presented an overview of the NIST work effort to develop a new standard on personal identification verification **[Ref. #4]**. Homeland Security Presidential Document #12 mandates that NIST develop a policy for a common identification standard for federal employees and contractors. The briefing described PIV threats and some representative countermeasures. The project will be accomplished in several phases. Phase I is the development of a strawman design. Phase II will be the development of implementation and critical support, and Phase III will include the development and coordination of implementing specifications and guidelines. The Board questioned the amount of funding needed to accomplish this task. Mr. Barker responded that the current effort is going to cost approximately $4 million, however, there is no start-up money available for this effort. Mr. Barker stated that Phase II will cost $4.6 million and Phase III will cost $20.6 between 2005-2007. He also said that there is a cost of $2-5 million that will continue on indefinitely. These figures are reflective of the cost to NIST only and do not include implementation costs. NIST is required to produce this standard within a given time frame. NIST also acknowledges that not all of the problems can be addressed given the short period given to produce the standard. NIST will address those areas that cannot be addressed with this standard. One of the more positive postures this standard will address is the use of biometrics. Currently there are no material biometric standards. Mr. Barker said that NIST is working with the Department of Homeland Security and the Departments of Transportation, State and Justice on design issues.

Professional Credentialing Updates

Board member Bruce Brody briefed the Board on the Cyber Security Practitioner Professionalization Program established at the Department of Veterans Affairs **[Ref#5]**. Mr. Brody believes that the Board may want to advocate the value of professionalizing the work force through some form of professional accreditation. The Board could address whether or not there is a need beyond encouraging agencies to get credentials established or identify specific incentives such as pay increases for those employees who seek credentialing. The Board discussed the possibility of inviting the Office of Personnel Management to brief them on the potential for training/credentialing activities governmentwide. Other sources the Board may want to hear from include the ACM, who are opposed to credentialing of software people, and DOD's Centers of Academic Excellence. This topic will continue to be part of the Board's work plan for the coming months.

NIST Guides on Investigation of Computer Security/Computer Crimes Issues

Ms. Susan Ballou of NIST's Office of Law Enforcement Standards (OLES) discussed the collaboration between the Computer Security Division (CSD) and the OLES, especially in the certification effort pertaining to computer forensics **[Ref. #6]**. Ms. Ballou presented the Board with an extensive overview of OLES activities in forensic sciences such as DNA and firearm forensics. OLES personnel review draft documents from the CSD for the Department of Homeland Security. This eliminates duplicate work and educates each of the groups on other expertise at NIST. The CSD also participate on OLES projects. More specifically, they participate on technical working groups and are provided with a view from law enforcement and the inherent legal constraints. In the future, OLES will be inviting CSD to participate in additional working group activities.

Board Discussion

The minutes of the June 2004 Board meeting were approved with an edit to note that Board Member Howard Schmidt was present via teleconferencing for the vote to approve the CSD funding report.

The Board also took the action to develop a letter in support of the NIST effort to develop the PIV standard and to point out some of the risks associated with the deadline given to develop the standard. Specific concerns were noted and the motion was made to adopt in principle the concepts as outlined and develop a letter for the Chairman's signature. The motion passed.

The meeting was recessed for the day at 5:40 p.m.

Thursday, September 30, 2004

The meeting was called to order at 9:15 a.m.

Discussion with Chief Privacy Officer of the Department of Commerce (DOC)

Mr. Dan Caprio, Chief Privacy Officer and Deputy Assistant Secretary at the Department of Commerce presented the Board with his perspective of the management of privacy aspects within the federal government. Mr. Caprio was formerly with the Federal Trade Commission. Currently with DOC's Technology Administration (TA), Mr. Caprio stated that one of their roles is to maximize technologies contributions to the economy. TA works and partners across agency Bureau's serving as a portal for them. They are currently involved in looking at outsourcing issues. TA is also looking at shared responsibilities and principles of suppliers and operators in the cyber security networking arena noting behavior changes, giving practical tips, building better software, encouraging higher education in the field and elevation of the enterprise. Mr. Caprio emphasized that there is a need for a catalyst for the development of a process that everyone can agree to use. There is not going to be a one size fits all solution. The Board asked what the challenges were to trying to be an overseer/advocacy person for Commerce and how does this work and how does Mr. Caprio see it working across the federal government. Mr. Caprio responded that DOC created the privacy officer position four years earlier and tries to lead by example. The DOC privacy model works in partnership with the DOC's Chief Information Officer. Mr. Caprio believes that no matter what the issue, it always comes down to technology and best practices as well as seeking private sector solutions. It was also pointed out that most agencies do not have dedicated Privacy Officer positions, but work privacy issues through their individual Chief Information Officer offices.

Mr. Caprio identified areas where the expertise of the Board would be of benefit to Commerce. They included the sharing of information, especially technology solutions, identifying things are working and those that are not.

Public Participation Period

There were no requests to speak from the public attendees.

There being no further business, the meeting was adjourned at 11:00 a.m.

Ref. 1 - Brody presentation
Ref. 2 - McDonald presentation
Ref. 3 - Landau presentation
Ref. 4 - Barker presentation
Ref. 5 - Brody presentation
Ref. 6 - Ballou presentation

/s/

Joan Hash
Board Designated Federal Official

CERTIFIED as a true and accurate
summary of the meeting.

/s/

Franklin S. Reeder
Chairman