INFORMATION SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

The DoubleTree Hotel and Executive Conference Center
1750 Rockville Pike
Rockville, MD

June 10-12, 2003

Tuesday, June 10, 2003

Board Chairman, Franklin S. Reeder, convened the Information Security and Privacy Advisory Board Meeting (ISPAB) for its second meeting of the year at 8:30 a.m.

In addition to Chairman Reeder, members present during the meeting were:

Lynn Bruneau
Richard Guida
Morris Hymes
Susan Landau
Steve Lipner
Leslie Reis
John Sabo
James Wade

The entire meeting was open to the public. Over the three days of the meetings, there were 10 members of the public in attendance.

Chairman Reeder announced that Board Member Michele Moldenhauer had resigned as a member of the Board effective immediately. The Board Secretariat will begin the process of filling the vacancy of a government representative to the Board.

Mr. Reeder reported on his meeting with Dr. Arden Bement, Director of the National Institute of Standards and Technology (NIST). Dr. Bement said that he was very supportive of the efforts of the Board and had recently testified before the House Committee on Science on NIST's support of this activity. Mr. Reeder also reported on his meeting with Robert Liscouski, Assistant Secretary of Homeland Security for Infrastructure Protection at the Department of Homeland Security. Mr. Reeder extended an invitation to Mr. Liscouski to attend a future Board meeting to meet with the members to discuss opportunities for the Board to be of assistance to DHS's in its cyber security efforts.

Session on E-Authentication

Board member John Sabo presented an overview of the panel on e-Authentication.

The first panelist to speak was Mr. Khaja Ahmed, Software Architect and Chief Technology Officer – MS Passport, Microsoft Corporation. [**Ref. #1]** Mr. Ahmed discussed the Passport approach to consumer authentication services. Passport offers different types of levels of authentication. It allows for anonymous/pseudonymous IDs and multiple IDs. It also allows for strong authenticated IDs. Passport does not perform identity verification or ID management. Mr. Ahmed's presentation also covered the economic models needed, the governance/operating rules, technology, and operations requirements that are required to have consumer e-

Authentication in place. Passport offers trusted data management. It does not mine, sell, rent or market Passport data. It does not allow secondary use of Passport data by Microsoft or anyone else and Passport facilities are not shared. The focus is on consumer empowerment. It requires participating sites to post their privacy policy and to support P3P. Passport also supports E.U. Safe Harbor. In the future, Microsoft will be exploring stronger authentication and privacy options such as certificate-based authentications, dual passwords, one-time passwords, phone-based authentications, multiple issuers of IDs and multiple authentication services in "federations'.

The second panelist to present was Ms. Christine Varney of Hogan & Hartson LLP, who represented the Liberty Alliance project. **[Ref. #2]** During 2002-2003, the consortium of members as grown to over 170 and includes the General Services Administration and the Department of Defense. At the Spring 2003 RSA Conference, Liberty Alliance brought together 20 members for an interoperability demonstration to showcase account linking and simplified sign-on. There is also a hands-on interoperability demonstration available at the Neustar facilities in Northern Virginia. Liberty also released a public draft of their Phase 2 specifications as well as drafts of security and privacy implementation guidelines and the privacy and security best practices document. These documents highlighted global privacy laws and fair information practices. These Liberty Alliance specifications offer a technology blueprint for companies that want to create innovative, identity-based web services based on a federated model. Liberty expects to release the final version of Phase 2 in September 2003. Ms. Varney reported that other Alliance initiatives in progress are in the areas of business templates, certification program: technology brand for conformance to specifications and multi-track model for identity services.

The third participant in the panel session was Lynette Millett of the National Academy of Sciences Computer Science and Telecommunications Board (CSTB). The briefing was on the NRC study of authentication through the lens of privacy. Mr. Steven Bellovin of AT & T Research Labs and Mr. Stephen Holden, University of Maryland, Baltimore County, who were members of CSTB Study Committee on Authentication Technologies and their Privacy Implications, also joined Ms. Millett during the briefing. **[Ref. #3]**

Ms. Millette explained the genesis of the study. The study committee consisted of chairman Stephen T. Kent of BBN Technologies and 15 other prominent members of the information technology community and academia. The study was launched in March 2001. Seven plenary meetings were held during 2001-2002. The motivations for the study centered around privacy as a growing concern in general. The committee was asked to look at how authentication technologies affect privacy with the caveat that affecting privacy is not always considered a violation of privacy.

Mr. Bellovin reviewed the definitions used in this report. He stated that terminology is central and that agreed-upon terminology is critical for a productive discussion. Inconsistent usage confuses the issue and terms are not as they seem colloquially. Four types of privacy are discussed in the report: information privacy, bodily integrity, decisional privacy and communications privacy.

Steve Holden was next to speak. His briefing covered system considerations including discussion of various underlying technologies such as passwords (static vs. one-time), challenge-response mechanisms, PKI and biometrics. Mr. Holden also discussed the multiple points at which privacy is affected. Chapter 7 of the report describes each of these points in detail.

The following are the major findings/recommendations of the study: context, scope, and implementation matter greatly; local contexts/use are usually more privacy-sensitive; secondary uses are particularly problematic; a toolkit for thinking through design is provided; and, a checklist for evaluating/designing authentication systems is presented.

The Government plays a unique role as a regulator, issuer of identity documents and a relying party. The Government has a unique relationship with citizens. Some of the reasons for this relationship concept is that many transactions are perceived to be mandatory, agencies cannot

choose their markets, relationships can be cradle-to-grave and individuals many have higher expectations for the Government. Foundational documents such as birth certificates are a risk from a security perspective because of the diverse issuers and no interest on the part of the issuers to ensure validity or reliability. For example, a birth certificate should not be used as a sole-based identity document.

In addition to the CSTB's authentication report, Ms. Millette also mentioned another report that looked into the questions about nationwide identity systems. Driver's licenses are a nationwide identity system facing enormous challenges because of inappropriate linkages and the likelihood of unrestricted secondary uses. The biometrics databases and samples would need strong protection.

In conclusion, the CSTB's study group overall assessment found that care must be taken to assess the privacy implications of authentication systems. Design and implementation choices weigh heavily on the privacy impact of authentication systems. They found no easy answers or panaceas.

Chairman Reeder thanked the group for their report and asked what the Board could do to capitalize on the CSTB effort to raise the level of consciousness within Government in regard to privacy assessments. Ms. Millette responded that NIST has a unique role in helping to formulated government-wide policy practices and to this end the Board could let NIST know that there is little recognition of privacy in the Government and ask that they encourage other agencies to have privacy implementations as part of whatever they design. Areas to make others aware of might be to discourage authentication when authorization is what is being requested. Avoid use of easy linked data unless it is needed for the data to take care of the mission. Consider the threat. Avoid collection of information unless it is planned for a specific purpose and avoid tracking at all cost.

The Board will invite Eva Kleederman to their next meeting brief them on the privacy guidance document that the Office of Management and Budget has been working on this past Spring. The Board would also like to hear from agencies that are using customer recovery services to complete their missions.

The next panelist to speak was Jeanette Thornton, Staff Specialist for the Office of Information and Regulatory Affairs at the Office of Management and Budget. Ms. Thornton spoke about the work being done in the recently established office of e-Government under Mr. Mark Forman. In August 0f 2001, OMB's e-Government strategy was started by an initiative that looked at the opportunities of e-Government collaboration across the Government. Twenty-four initiatives were developed including one on e-Authentication. The goal of consolidating Government payroll providers was the major reason for this endeavor. OMB looked at all types of authentication technologies. Four separate pieces of work were identified: (1) development of policies; (2) creation of common infrastructures with sharing between credential providers; (3) establishment of a policy framework; and (4) enacting the application. The resulting document will be published as a draft with a 30-day public comment period. It will contain four levels of standards for use by the Government. Ms. Thornton reported that NIST is also developing a technology document in tandem with OMB. William Burr and Tim Polk of NIST are working with OMB on the e-Authentication technical guidance. OMB is particularly interested in the infrastructure and developing a government business case for FY05. They have joined with Liberty Alliance and they are interested in the business rules and examples of memorandum of understanding. OMB proposes to accredit public/private sectors to perform certain levels of certification of credentials. They are currently working with Federal agencies that are already issuing credentials. To the question of whether the OMB guidance document will address a set of policy questions that should be developed to address the question of authentication needs, Ms. Thornton replied that OMB has not yet planned to tackle this issue. She said that Section 208 is rather broad about what a privacy impact assessment should contain.

Bob Sunday, Lead Architect of the Secure Channel (SC) Project Management Office, Public Works and Government Services of Canada was the next panelists to speak **[Ref. #4]** The mission of the Secure Channel Project is to provide electronic access to the Government of Canada's (GoC) current and future applications to citizens, businesses and trusted partners in a secure and client-centric fashion. The broad challenge is in creating a secure, high-performance electronic environment through which Canadians willingly engage in the activities of government. Mr. Sunday described the conceptual model and the service broker model. There are three services lines offered with Secure Channel: SCNet (common network services), epass Canada (common registration services), and Receiver General Buy Button (common payment services). Mr. Sunday reviewed the security of SC infrastructure covering the network, security zones, platform safeguards, core infrastructure services and security management issues. Also discussed was the mechanism in place for Departmental adoption and deployment of SC that consisted of an Opportunity Review Board and Client Implementation Teams.

Mr. Ari Schwartz, Associate Director for The Center for Democracy and Technology (CDT) was the next member of the panel to address the Board. Mr. Schwartz discussed CDT's interim report on privacy principles for authentication systems. **[Ref. #5]** This report focuses on consumer initiated transactions and government concerns. As the government develops authentication systems to enhance citizen-centered government, it should also be sensitive to the concerns by the citizens of the government's use of personal information and the creation of a centralized identify system or card. The interim report states that privacy principles for authentication systems should provide user control, support a diversity of services, use individual authentication only when appropriate, provide notice about the collection and use of information, minimize collection and storage, and provide accountability. Mr. Schwartz noted that currently the vendors are on board with these principles and the next version of this report will bring the government players to the review table. It is anticipated that this next version will be released sometime late in the Fall of this year. Several of the Board members suggested that other areas that could be addressed in this report could include informed consent as it relates to government and diverseness of services. It was also suggested that liaison with governments of European countries might be useful. It was observed that possible fallout for moving to this public/private sector relationship is that it could give the unintended appearance of moving around the Privacy Act. The safeguards that the public expects may be able to be circumvented unintentionally by these privacy principles.

The last presenter of the e-Authentication session was Ms. Ruchika Agrawal who represented the Electronic Privacy Information Center (EPIC). **[Ref. #6]** The presentation covered EPIC's case study regarding Microsoft's Passport services that identified information practices that were misrepresented by Microsoft. To correct these misrepresentations, the Federal Trade Commission issued Consent Orders directing Microsoft to address these issues. Ms. Agrawal's briefing included discussion regarding Article 29 Data Protection Working Party's guidelines on on-line authentication systems. Additionally, the presentation included an Appendix that contained database best practices that had been excerpted from Peter Wayner's Translucent Databases document. Ms. Agrawal mentioned that EPIC is preparing a document for the IEEE dealing with the development of architecture for privacy to minimize data collection and, she will inform the Board when the document is finalized.

Chairman Reeder expressed the Board's thanks to all of the panelist and especially to members John Sabo and Susan Landau for the development of the session.

The meeting was recessed at 5:10 p.m.

Wednesday, June 11, 2003

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

Board Discussion/Review of Activities from Day 1

The first item discussed was the membership vacancies on the Board. There are three vacancies to be filled; two vacancies in the federal category and one vacancy in the private sector other than large IT company category. NIST will review all nominations that have been received. Current Board members who would like to nominate anyone for membership consideration should pass on that information to Joan Hash and/or Ed Roback. The chairman extended special thanks and appreciation to Board member James Wade for all of his service to the Board during his tenure as a member. His appointment term expires on August 11, 2003.

Next, the Board discussed their views from the e-Authentication session held the first day. It was noted that there seemed to be some convergence or consensus on a set of principles coming out of the National Academy of Sciences CSTB report. It was observed that the public doesn't understand the privacy issues of such an effort between e-Government and e-Authentication. The Board is interested in looking at specific Customer Relationship Management (CRM) issues and the identifiable information used in linkage to see if there is secondary usage of information in any inappropriate ways. The public should have a better understanding of what is happening with the information that the Government collects on them. The Board will plan to devote a portion of their September meeting to discuss the CRM issues before they go forward with a specific recommendation or finding report to OMB. The current legal framework of e-Authentication is inadequate to deal with issues such as use of third party, and large data stores are beyond the reach of the laws that apply to the federal collection of data. The question is should there be guidance issued to cover these issues or should there be changes made to the Privacy Act to cover them. The Board will prepare a letter to the Director of OMB to address their concerns of these issues. Additional topics the Board will review are data mining and the issues raised by use of linkage with focus on CRMs. The Board would also like to look into the new uses of data for domestic security.

Another topic that the Board would like to address is the use of applets that become part of an individual's computers without their knowledge. The Government should have a policy in place such as the policy relating to the use of cookies. Board member Rich Guida volunteered to put together a panel session for the next meeting to explore this topic.

Board members Lynn Bruneau and Leslie Reis will put together a panel session for the September Board meeting to explore the CRM issues mentioned earlier.

Topics of other sessions that the Board would like to hold included the following:

- Examination of integration of information requested from the public sector and to find out how this information is being used beyond the specific purposes for which it was initially requested. Board member Morris Hymes agreed to coordinate this effort.
- Examination of NIAP extension activities. Morris Hymes and Steve Lipner agreed to coordinate this effort.

The Board reviewed the minutes of the March Board meeting and approved their adoption pending a minor editorial change.

Update on Security Benchmarks, Checklists and Guidance

Chairman Reeder briefed the Board on security benchmark activities that are currently underway at the Center for Internet Security.

Board member Steve Lipner introduced the participants of this session. They included Tim Grance of NIST, Terry Sherald of the Defense Information Systems Agency (DISA) and Jay Wentworth of ManTech working with the State Department.

Mr. Grance (NIST) presented a briefing on security checklists for commercial IT projects. **[Ref. #7]** He reviewed the drivers and challenges of the effort, the operational concept, the granularity or levels of checklists, the implementation and submission of details, the issues for producing checklists and issues for NIST and future steps that will be taken by NIST.

Mr. Sherald (DISA) presented a briefing on DISA's security technical implementation guide (STIG). **[Ref. #8]** The guide is a compendium of security practices and best practices for securing operating system or application software. Mr. Sherald reviewed the scope and lifecycle of STIG. There are STIGs available that cover a variety of networks/perimeters, operating systems, and applications. There is also a security handbook STIG available for the user. Currently, there are nine draft STIGs covering areas such as wireless, network infrastructure and virtual machines. There are four new STIGs to be developed in FY03 in the areas of voice over IP, optical, biometrics and MAC. Mr. Sherald discussed DISA's implementation of a Gold Standard that is applied to the STIGS and a Gold disk tool that is available. Lessons learned that were identified included the observations that settings still break things, there is not enough time to be as active as is needed and there must be contingencies for specific settings. The benefits identified were the involvement of vendors, the improvements to the STIGs and the focus on non-native environments vs. native W2K.

Mr. Wentworth shared his personal views on the security benchmark issues, and in particular, those issues he has seen at the State Department that have an impact on the variety of networks and risks of access of foreign nationals versus citizens access to these networks. The development of lengthy passwords is also a more sensitive issue for the State Department. General policies and templates are often used. Operationally templates have caused outside problems with the networks that use them. Version identification has helped aid in correcting problems that arise. Templates do not eliminate the need for manual steps to be taken. Another important thing to do is to scan to see that the template settings are being applied.

Mr. Lipner thanked the presenters for their briefings. The Board concluded that progress had been made in this area since the Board reviewed it in 2002. However, two challenges continue to face this effort. Many are still not applying the latest applications of software that are available to them. The other problem area lies in the process area and the cost of development of research.

Introduction of Accuracy of Databases Session

Board member Susan Landau presented the objectives for this session. The participants in this session included Joyce Schaul and Carolyn Myers of the Social Security Administration (SSA) and Tim Bouma of CGI Management Consulting Group of Canada.

Ms. Schaul was the first to brief the Board. **[Ref. #9]** She gave a historical overview of the tradition of privacy within SSA. The SSA Office of Quality Assurance has a 98% accuracy record in the area of personal payments that include accuracy of addresses, names, and other data beside monetary distribution to individuals. SSA is working on a pilot program for the deployment of the use of on-line forms use for data such as calculation of retirement benefits. A hybrid session is currently available for retirees to use. To the question of proposals to change

the use of Social Security Numbers (SSN) with regard to identity theft situations, Ms. Schaul stated that SSA does not control the use of the SSNs. Verification services are available at SSA but it is not their main business. Current verification requests are primarily in the area of homeland security verifications. Ms. Schaul indicated that SSA has also been working with Eva Kleederman of OMB on the privacy implementation guidance document.

The next presenter was Carolyn Myers, who presented a briefing on the SSA's Death Master File (DMF). **[Ref. #10]** The DMF contains over 72 million records. It also contains beneficiary and non-beneficiary data. It was explained that 90% of the data reported comes from family members and funeral directors. Five percent of the data comes from States and two federal agencies. The remaining 5% comes from returned reports from banks and other financial institutions or as returned mail marked deceased. To ensure the accuracy of the data, SSA performs numerous audits. All reports must match data in the SSA database of Social Security numbers. Ms. Myers noted that there is a strong push to make the DMF data available for purchase by other entities. SSA does not exchange the information they collect with the States. However, the States are working on an initiative to match birth records with death records. The SSA has a disclaimer in place that protects them from being liable for information that it not determined to be accurate in the DMF. SSA is also working on the development of an electronic death registration program.

The last presenter of the session was Mr. Tim Bouma who presented an overview of the National Criminal Justice Index project (NCJI). **[Ref. #11]** The topics that were covered included data integrity and privacy, risk and governance analysis, privacy impact assessment, governance-based access control and memorandum of understanding details. In conclusion, Mr. Bouma reported that better information sharing has now become a priority for all government agencies. The NCJI is a first step to better information sharing between agencies in the criminal justice community. As a result, common infrastructure sharing standards and frameworks are only now emerging (e.g., RBAC, GBAC, etc.).

Chairman Reeder thanked all of the participants for their insightful presentations. It was suggested that the Board prepare a letter to the Director of OMB and the Department of Justice regarding what the Board has learned about the NCJI effort and the accuracy of criminal records. The Board agreed to have Chairman Reeder prepare a draft for consideration.

Professional Certification Briefing

Mr. Hun Kim briefed the Board on the National Information Technology Security Professional Certification effort. **[Ref. #12]** This project got its impetus from the then White House Office of Homeland Security and is being directed under the auspices of the Department of Homeland Security. Mr. Kim was a member of the President's Critical Infrastructure Protection Board (PCIPB) Standing Committee on this effort. Core members of the group were from the Government. Meetings were held with organizations such as CIS, ISC^2 and the Learning Tree. The group is currently reviewing ways to transition people who already have some type of Information Technology certification credentials. Consultations are still continuing with a variety of stakeholders. Mr. George Bieber, formerly with DOD, is working with various agencies on training and awareness issues across agencies and trying to promote the use of rigorous certification credentials. The group is working with the Office of Personnel Management to add references to certifications as a desired element for employment of applicants. The Board expressed an interest in being kept informed on this topic and was pleased to know that NIST had a presence on the Working Group.

Chairman Reeder announced that it was unable to attend the meeting on Thursday. Board Member Rich Guida will serve as Acting Chairman in his place.

The meeting was recessed at 5:00 p.m.

Thursday, June 12, 2003

Acting Chairman, Rich Guida, reconvened the meeting at 8:34 a.m.

Board Discussion/Review of Actions from Day 2

The Board focused on the review of the proposed letter to be sent to the Director of OMB on the subject of the Board's finding from the e-Authentication session. **[Ref. #13]** After deliberating on the content of the letter, the Board approved the letter.

The Board reviewed the items for the agenda for the September meeting based on the Board's earlier discussions. Sessions will be organized on 'touching the desktop' policies, public/private databases and CRM activities, NIAP in the unclassified community and use of data for domestic security. The Board will invite the Department of Homeland Security Privacy Officer, Nuala Connor-Kelly to attend the next meeting. They would also like to hear from the Department of Homeland Security's cyber security person at the next meeting.

National Science Foundation (NSF) Activities in Cyber Trust

Carl Landwehr, Program Director with the National Science Foundation (NSF) presented a briefing on NSF's cyber trust vision. **[Ref. #14]** Cyber trust programs include data and applications security, network security, trusted computing and embedded and hybrid systems. Dr. Landwehr reviewed the recent Cyber Security Research and Development Act (CSRDA) and the programs that it authorized to be carried out by both NSF and NIST. The NSF plans to direct approximately $15 million to increase their Cyber Trust research programs. In addition to these programs, NSF already has other activities underway related to Cyber Trust. NSA believes that now is the opportunity for increased investment in the areas of trusted computing, trustworthy computing, CSRDA and DHS.

Public Participation

Acting Chair Rich Guida called for any public participation. There were no requests to present.

As there was no further business, Acting Chair Guida adjourned the meeting at 11:15 a.m.

Ref. 1 – Ahmed presentation
Ref. 2 – Varney presentation
Ref. 3 – Millett presentation
Ref. 4 – Sunday presentation
Ref. 5 – Schwartz presentation
Ref. 6 – Agrawal presentation
Ref. 7 – Grance presentation
Ref. 8 – Sherald presentation
Ref. 9 – Schaul presentation
Ref. 10 – Myers presentation
Ref. 11 – Bouma presentation
Ref. 12 – Kim presentation
Ref. 13 – Letter to Director of OMB
Ref. 14 - Landwehr presentation

/s/

Joan Hash
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting.

/s/

Franklin S. Reeder
Chairman