INFORMATION SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

The Hyatt Regency Bethesda
One Bethesda Metro Center
Bethesda, MD

September 16-18, 2003

Tuesday, September 16, 2003

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

Lynn Bruneau
Charisse Castagnoli
Richard Guida
Susan Landau
Steve Lipner
Sallie McDonald
Leslie Reis
John Sabo

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. NIST has appointed Rebecca Leng, Deputy Assistant Inspector General for Information Technology and Computer Security at the Department of Transportation and Bruce Brody, Associate Deputy Assistant Secretary for Cyber and Information Security at the Department of Veterans Affairs as government representative members of the Board. Mr. Reeder also reported on a meeting that he had with Department of Commerce Deputy Secretary Sam Bodman. Deputy Secretary Bodman expressed his support of the Board's activities. On the topic of budgetary support for NIST computer security program, Deputy Secretary Bodman acknowledged that across the federal government agencies, the Department of Commerce is at the low end of budget dollar distribution. Therefore, the likelihood of obtaining additional funding for the computer security program would have to come from other sources from within Government.

Session on "Touching Desktops Policies

Board Member Rich Guida opened the session with an overview of the topic of harmonizing the environment of the use of browsers and desktops receiving what was originally intended for the users. There are computer security and privacy implications with regard to touching the browsers. Anytime that something is put on the computer, it can expose the computer to security vulnerabilities. The questions to be addressed are what are the implications and what bad things could happen, why doesn't the federal government have a policy in place on this topic and why has Canada already done something about this risk.

Mr. Guida introduced Mr. Paul Madsen of Entrust representing Liberty Alliance **[Ref. #1]** Mr. Madsen is the Chair of Liberty Trust, Security and Privacy Subteam. The goal of Liberty Alliance is to establish an open standard for federated identity management. The scope of this identity extends beyond the original applications for which it was originally created. Technically, Liberty builds on SAML (Security Assertions Markup Language). SAML is an XML-based framework for

exchanging security information. The Liberty Roadmap is entering into Phase 2 that should be released in October 2003. Phase1 dealt with a simplified sign-on and identity federation and Phase 2 will deal with a web services framework. Future phases will include enhancement to the federation and services infrastructure. Mr. Madsen's briefing covered what "touching the browser" might mean for federated identify. He reviewed the Liberty model and profiles and the baseline and optional Liberty requirements. Mr. Madsen was asked if he believed there was a strong appetite or no appetite among the Liberty Alliance members to '"touch the browser' or was it believed to be too risky or not an issue that the Alliance wanted to address. Mr. Madsen replied that he was in no position to answer that but suggested that the Board may want to contact members from Nokia and True Pass to obtain a better perspective from them. Board member Charisse Castagnoli offered the following concerns/questions for consideration by the Board: how do we educate consumers about the concerns of use of browsers and what role could the government/NIST play on this issue; has a gap risk analysis be done, has a latency analysis been done, what is being done regarding ID theft liability?

Next, Mr. Wayne Jensen of the NIST Computer Security Division briefed the Board on the topic of browser extensions and security. Mr. Jensen reported that browsers are built with the expectations that they will be touched by other applications. He explained the risk of mobile codes and its wide and varying degrees of access to resource and different kinds of security controls. Some of the varying classes of technical code include Cage, Filter, Signature, Proof and Hybrid. Assessing the risk imposed by a particular mobile code technology begins with examining the code's context. Mr. Jensen stated that choosing whether to support and accept a particular mobile code technology must involve balancing its risks against the benefits it can provide. NIST guides have been concerned with accessing public as opposed to private or sensitive information. The focus has been on protecting government systems from mobile code threats by deploying the lowest risk mobile code technology on websites; disabling risk mobile code technologies on browsers; and, applying technical and other controls to mitigate risks. Mr. Jensen summarized his briefing by saying that 'touching the browser" is a bit of a misnomer as we regularly affect the client side by serving Acrobat, WORD and other content. Different technologies affect the browser differently and new technologies are continually on the horizon, making it difficult to pick a winner. Ultimately, federal agencies are left with the decision as to how best to interface technologically with citizens.

Board Member Guida noted the obvious absence of someone within the federal government who could address this issue. Mr. Guida said that Jeanette Thornton of the Office of Management and Budget (OMB) had indicated that this issue was not on the radar screen of the federal government at this time. Mr. Guida suggested that the Board might want to consider sending a letter to OMB to identify this matter as a potential technological issue that should be addressed. While OMB does have a "cookie" policy in place, cookies are not active code and the policy does not cover the extent of potential risks that are there with the use of touching the browser.

After further discussion, the Board decided to prepare and send a letter to the Director of OMB to share their observations and concerns on this issue.

Discussion of Public/Privacy Databases and CRM Activities

Board Member Leslie Reis began the discussion of the Customer Relations Management (CRM) activities. The primary focus for Board discussion on this was the issues of the enhancement of e-government. Professor Reis provided the members of the Board with a variety of material covering this topic. The articles covered the Privacy Act of 1974, customer relations management in general, CRM in the public sector, and CRM activities being done by the U.S. Postal Service. It was noted that four major privacy relation issues arise out of the use of CRMs. The first is the amount and types of information using CRMs approach tools that could potentially be in violation of the Privacy Act. The second issue is that the use of CRMs may promote the view of customer and customer information as a commodity. The third issue is that the use of CRMs to enhance e-government to e-government services may provide competition for the private sector and that many outside of government feel that this is not the role that the

government should be in. And fourth, the use of CRM's has great potential for unauthorized secondary use of information collected by citizens under the guise of CRM.

The Privacy Act seems to be a tool that does not have a lot of teeth to it, reported Professor Reis. The absence of reactive enforcements that the law provides and the failure of the law to keep up with the manner in which data is currently used are clearly two weaknesses. A recent General Accounting Office report identified many problems with the current Privacy Act and the issues that resulted.

The Board members agreed that they would like to continue to explore this topic. In particular, they would like to look at the potentially serious implications that could arise as a result of CRM collections that take personal information for a specific topic and then use that information for a secondary topic in an enhanced mode of operation. The Board's next steps will be to obtain briefings from federal agencies that may be use CRM practices. The Treasury Department's U.S. Mint, the Departments of Transportation and Labor, and the U.S. Postal Service may be agencies to hear from. Board members Leslie Reis and Lynn Bruneau volunteered to lead this effort and this will be one of the agenda items for the December 2003 Board meeting.

Briefing on Cyber Security Professional Certification

Board chairman, Franklin Reeder, briefed the members on the proliferation of credentials being seen in the cyber security world today. Many of these credentials fail to meet the primary criteria for such certifications. Some type of independent credentialing has been proposed to raise the level of certification. The recent National Cyber Security Strategy noted this issue and the Department of Homeland Security has been given some responsibility to address this. The Board previously heard from Hun Kim of the Navy who served as a participant on ad hoc committee with the responsibility to address professional certification. The Department of Defense (DOD) has spent over six months working to develop a policy of credentialing their information assurance employees. The DOD has a draft policy that will categorize certification functions and required credentials. To address the problem of training, DOD has engaged the Center for Internet Security (CIS) to work with them to develop a multi-step process looking into the work that has already been done followed by the establishment of some type of a consensus that work. A job skills analysis would be done and then that would be mapped back to show how specific skills could be tests. CIS has compiled a comprehensive list of all certification and credentialing entities. The list includes both vendor specific and non-vendor specific certifications. At the end of the process steps, if there is no general convergence, DOD will work with the individual groups to come to some type of agreement. The DOD has also worked through the Institute for Defense Analysis for the purpose of convening the various stakeholders. These workshops have been predominately attended by those in the certification business. By the end of 2003, DOD hopes to be able to issue a final directive. Mr. Reeder also said that new Board member Bruce Brody of the Department of Veteran Affairs is pursuing a certification policy within the VA and perhaps Mr. Brody could provide an update to the Board on his agency's efforts sometime in the near future.

Before recessing the meeting for the day, the Board approved the minutes of the June 2003 meeting and approved the draft letter to OMB on the topic of touching the browser that had been prepared by Board member Guida.

The meeting was recessed at 4:19 p.m.

Wednesday, September 17, 2003

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

Board Discussion on Issue of Planning Meetings

The Board discussed focused ways to handle future meetings and the development of specific agenda sessions. Chairman Reeder proposed that the Board members gather names of those members of the public and press that the Board believes would be interested in its activities and provide these names to the Secretariat for furnishing future meeting agendas. The Board should identify what issues constituents want to hear about. More specifically, agencies should be invited to attend the Board meetings and address the issues identified in the Board's correspondence to the Director of OMB on the topic of using Web-based transactions to provide 'e-government' services to members of the public. Chairman Reeder reported his plans to meet with Karen Evans, the new Director of the CIO Council, to engage the CIO Council in meeting with members of the Board.

It was also determined that each meeting of the Board follow three specific focus areas. One session would focus on immediate, quick-time issues, one on long term issues and one on informational updates.

The Board will resume its discussion on the CRM issue in December with the plan to have a dedicated session on this topic planned in either March 2004 or June 2004. Board member Leslie Reis volunteered to have researcher from The John Marshall Law School work with the Board on the development of this session.

Industry Overview of Information Sharing Issues for Homeland Security

Board Member John Sabo updated the Board on activities of the IT/ ISAC (Information Sharing and Analysis Center), a forum for trusted sharing of vulnerability and alert information, as well as best practices. It is also a forum for sharing threat related information, and ways to protect against those threats. Mr. Sabo is a member of the IT/ISAC Board of Directors. Mr. Sabo reported that more and more ISAC's are relying on IT systems and there is a strong interest in cyber security. There are 11 major ISACs being formed in the following areas: financial services, telecommunications, electricity, energy, surface transportation, public transportation, water, chemical, health care and trucking. Areas of particular interest are in the business privacy area as it pertains to the sharing of threats and vulnerabilities experiences among the infrastructures/companies. Mr. Sabo said that some of the identified business management issues that the ISACs have play back to some of what was reported in the Board's earlier written privacy white paper. The creation of a two-way interchange of information between the ISACs and the government about such threats and vulnerabilities could lead to the establishment of a new level of security sensitivity between all entities. Currently, the Department of Homeland Security, ISACs, and other private sector organizations are beginning to address these issues. However, no operational infrastructure has been put in place at this time.

Because the private sector operates most critical infrastructures, Mr. Sabo's main objective in his briefing to the Board was to make them aware of the new set of security issues and the new era of sharing of information between public and government systems and the protection of the information that is collected.

The Board agreed that this topic should be put on the 'to be watched' list and they want to continue to be keep informed. Also, sometime in the future, the Board would like to hear from the Department of Homeland Security on their work with the ISAC community.

Review of NIST Draft Special Publication 800-60

Mr. Curt Barker of the NIST Computer Security Division briefed the Board on the draft guideline for mapping types of information and information systems to security categorization levels (SP 800-60). **[Ref. #2]** This report looks at the privacy viewpoint from the sensitivity angle in two ways. The first harm identified is the reputation and trust issue and the other is the specific harm that can occur to individuals resulting form the compromise of their credentials such as identity

theft. The Board acknowledged that the mapping effort was a daunting task and commended Mr. Barker for the great job he had done. Mr. Barker also briefed the Board on the status of FIPS 199, Standards for Security Categorization of Federal Information and Information Systems. The Board noted that they had been kept informed and thoroughly briefed on this document during its development and will send a letter to NIST sending kudos to the Computer Security Division for their work on this effort. Mr. Barker also reported that NIST guidance Special Publication 800-60 and FIPS 200 will include privacy implementation. The Board endorsed the use of early workshops to gather pertinent information from across agencies.

The meeting was recessed for the day at 4:45 p.m.

Thursday, September 18, 2003

The last day of the meeting was cancelled because of the unexpected hurricane activity in the area.

Ref. 1 - Madsen presentation
Ref. 2 - Barker presentation

/s/

Joan Hash
Board Designated Federal Official

CERTIFIED as a true and accurate
summary of the meeting.

/s/

Franklin S. Reeder
Chairman