COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

General Services Administration
7th and D Streets, SW, Room 5700
Washington, D.C.

September 17-19, 2002

Tuesday, September 17

Board Chairman, Franklin S. Reeder, convened the Computer System Security and Privacy Advisory Board Meeting (CSSPAB) for its third meeting of the year at 9:00 a.m.

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

Lynn Bruneau
Charisse Castagnoli
Mary Forte
Rich Guida
Susan Landau
Steve Lipner
Sally McDonald [9/19 only]
Michelle Moldenhauer
Leslie Reis [via teleconference]
John Sabo

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

Chairman Reeder briefed the Board on his recent meeting with NIST Counsel, Mike Rubin, regarding activities of the Board. Mr. Rubin's main focus was on the draft privacy findings and recommendations report developed by the Board and the Board's proposal to conduct a Board-only teleconference for the purpose of discussing homeland security issues involving NIST. For the record, Reeder is concerned about Counsel's view that the activities of the Board are to be limited to those areas where the Secretary of Commerce would request or need advice. Another issue raised with Mr. Rubin was a concern about getting further advice and briefing about the ethics question by the members of the Board.

OMB Privacy Update

Ms. Eva Kleederman, OMB Privacy Officer from the Office of Information and Regulatory Affairs, briefed the Board on the Administration's privacy activities. The major focus is on e-government and the effects of the privacy. OMB is currently examining the Privacy Act for potential revisions. They are also looking into the privacy guidance pertaining to websites and technology tracking issues. Ms. Kleederman said that the model used by the Internal Revenue Service is a good example that other agencies could use as a starting point to conduct privacy impact assessments. After review of what agencies submit this year, OMB will decide whether to prescribe a specific assessment method for all agencies to follow. In addition to the Privacy Act oversight, OMB would also work in four or five other areas to make sure that privacy is effective.

The question was raised regarding what safeguards are in place and what is being done to assure the public that those safeguards are in place. Ms. Kleederman said that OMB has not required that agencies reveal what safeguards they have in place to the public. However, Ms. Kleederman did indicate that an interagency privacy council is being established to address these issues. The Board said that they have heard from other federal agencies that there is a need for the sharing of best practices among the agencies. Ms. Kleederman suggested that this matter could be an additional action item for the interagency privacy council to perform.

OMB is also examining ways to develop a plan of action for review of the current legal framework of available privacy laws. Ms. Kleederman has the lead role of oversight for the Privacy Act.

GAO Assignments on Privacy and Their Relationship to CSSPAB's Proposed Recommendations

Next to present was Mr. Alan Stapleton of the General Accounting Office (GAO). **[Ref. #1]**

Mr. Stapleton discussed the scope and objectives of each of their four identified privacy assignments and how they relate to the Board's privacy recommendations. They are:

(1) Conducting a comprehensive survey of 25 agencies' privacy policies and practices.
(2) Developing an executive guide on promising methods from the public and private sector that agencies can use to better protect the privacy of individuals.
(3) Evaluating Social Security Administration's policies for disclosing personal information to law enforcement agencies compared to other agencies.
(4) Updating their September 2000 Report "Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy (GGD-00-191)."

Findings of this report will be released to the requestors of the report and a follow-up report will be issued later in the year. The Board made the recommendation to Mr. Stapleton that the requestors be encouraged to release the outcome of the final report as soon as possible rather than wait into the next year for GAO to produce a final report. The Board would be very interested in the feedback received on the survey of agencies' Privacy Act Practices.

On the second assignment, Stapleton solicited any comments that the Board would like to offer to GAO.

Mr. Stapleton also provided the Board with a copy of the GAO template created for disclosing agencies' privacy policies to web visitors and asked for the Board's comments. Board Member Rich Guida expressed his concern that cryptographic issues be covered in the template.

In closing, Mr. Stapleton stated that the expertise of the Board makes it an excellent candidate to participate in the OMB study on this issue should OMB decide to focus on the GAO Report.

OMB Office of Information and Regulatory Affairs Updates

Mr. Dan Chenok and Ms. Kamela White of OMB's Office of Information and Regulatory Affairs presented the Board with an update on their activities since the last Board meeting.

They briefed the Board on the status the E-Government Act of 2002 that contains the reauthorization of the Government Information Security Reform Act (GISRA), the Federal Information Security Management Act (FISMA), the Cybersecurity R&D Act and the Homeland Security Act. The House version of the Homeland Security Act proposes that the NIST Computer Security Division stay within NIST, and the Senate version proposes that the Division become part of the Department of Homeland Security.

Budget business cases are now being transmitted to OMB. OMB will be analyzing investments to determine where they are aligned to match the mission base, security base, and commonality areas. Consistency across agencies will be noted. The Office of Homeland Security has asked OMB to develop guidance on the handling of security information. OMB is reaching out to a variety of entities both within and outside of the government, and they will be issuing a guidance document. They are not creating a new class of security information but rather seek a consistent treatment across agencies by defining a small set of information categories. A draft document will be distributed for public comment in the coming months.

Ms. White briefed on the GISRA guidance status. OMB has added performance measures to this year's request. They are getting input from the 24 large agencies and many smaller agencies. The information provided by these submissions can be used in other ways such as for agencies' scorecards, for reform of the budget process, for use in making determination for approval of agencies' security programs, and for use in the development of the OMB report that is due in February 2003.

On the subject of OMB's effort in enterprise architecture and the use of security, Dan Chenok said that Norm Lorentz has identified components at each level to share across the agencies. The Board will invite Mr. Lorentz to provide an update to them on this topic at their December meeting.

Chairman Reeder asked OMB what their thoughts were on baseline standards; i.e., doing security using at least minimum standards. Mr. Chenok said that OMB is interested in talking to the Board more about this topic. Ms. White reported that the Executive Branch Information System Security (EBISS) committee addressed this topic as part of its work effort.

The Board indicated their interest in any timetable for future revisions to privacy or security mandates.

Briefing on Liberty Alliance Project

Next to speak was Mr. Chris Hankin, of Sun Microsystems, Inc. Mr. Hankin was representing the Liberty Alliance, a group organized to establish open standards for network-based identity interactions. He briefed the Board on its Liberty project. **[Ref. #2]** Liberty was designed to simplify the process of signing on to multiple sites while still preserving users' privacy and security.

Liberty is a group of specifications.

- Establishes an open standard for federated network identity through open technical specifications. Tools to do this include simplified sign-on, enhance constituent relationships, and support all devices to enable consumer privacy and support interoperability.
- Uses open Federated model: network identity and user information in various locations; no centralized control, no single point of failure and links similar and disparate systems.

It is a phased approach. Approach drivers support rapid acceptance and deployment and easy incremental adoption. Version 1.0 contains federate network identity, opt-in account linking and simplified sign-on within an authentication domain created by business agreements and security is built across all the features and specifications. Future versions of the specification will be add-ons to Version 1.0 and include permission-based attribute sharing, schema/protocols for core identity profile service, simplified sign-on across authentication domains created in version 1.0 by business agreements and delegation of authority to federate identities/accounts. Currently, the

membership of the Alliance is over 100 with members such as Bank of America, Citigroup, RSA Security and Sony. There are three membership levels: sponsors, associates and affiliates. Each level has a different membership fee. For more information on this effort, see the website projectliberty.org.

Public Participation Session

There was no request for public comments at this meeting.

The meeting was recessed for the day at 3:50 p.m.

September 18, 2002

Chairman Reeder reconvened the meeting at 9:05 a.m.

Briefing on Microsoft's .NET Passport Platform

Adam Sohn, Product Manager, .NET Platform Strategy Group, Microsoft Corporation gave the Board a Passport overview and digital identity update.

Microsoft's role in this effort is to develop software to help individuals and organizations manage multiple identities. The fundamental tenets are the user in control, enterprises make trust, infrastructure decisions, Federation between providers; and protocol-based interoperability.

Mr. Sohn described Passport as an Internet-scale authentication service. It solves hard problems and provides flexible service for partners. Its Windows active directory allows for integrated enterprise identity management and simplifies security and management.

The elements of Passport include:

- Authentication – provides persistent token to key to customer relationship, end user convenience
- Profile service – frequently entered data can be stored and shared with sites at sign-in with user consent
- Kids passport – help partners comply with COPPA
- Passport express purchase service – form filler over secured channel for convenient checkout (scheduled retirement March 2003)

It was built to:

- Unify Microsoft's authentication islands
- Enable cross-partner orchestrated experiences of Microsoft authentication islands
- Enable cross-partner orchestrated experience (web services)
- End user benefit – less abandoned registrations, forms
- Deeper digital relationships with customers.

Security factors include:

- Protected data centers
- Credential information never shared with partner sites
- All traffic is encrypted over the wire or package is encrypted
- Sophisticated monitoring
- Moving to an auditable operational framework (SAS-70).

The meeting was temporarily recessed for the Board to attend the Public Key Infrastructure (PKI) certificate launch ceremony.

Board Discussion Period

The meeting was reconvened at 2 p.m. with general Board discussion.

The first topic discussed was the letter from NIST to the Board requesting their assistance in several areas of computer security. The areas were:

- The Government Information Reform Act (GISRA) and improvement of agency IT security programs
- Baseline standards/benchmarking
- Privacy and e-government
- Privacy and third-parties (outsourcing)
- Identification of new emerging IT security issues
- Updates to the NIST computer security handbook
- Development of NIST guidelines (and standards where needed).

Ed Roback, Chief of the NIST Computer Security Division, presented a short overview of these activities. The top three priorities for NIST were: GISRA, baseline standards/benchmarking, and development of NIST guidelines. After discussion on this issue, the Board produced a list of work items to take action on in the coming months. The list included the following:

1. Government Information Security Reform Act (GISRA)
2. Baseline standards/benchmarking
3. Privacy and E-government
4. Emerging security issues
5. NIST Handbook update
6. NIST guidelines
7. Government Paperwork Elimination Action (GPEA)
8. Digital Millennium Copyright Act (DMCA)
   Strategy for National Information Assurance Partnership (NIAP) outside of the national security community
9. Credentialing of cyber security professionals.

Members reviewed the list and voted on those topics that they were interested in leading or participating on **[Ref. #3]** The task leaders are to provide outlines to the Board before the next meeting. These outlines will be reviewed at the December meeting.

The Board tabled their action to send a letter to Governor Tom Ridge of the Office of Homeland Security until such time as the Department of Homeland Security becomes an official department. The Board will plan to have a briefing on homeland security from the Office of Homeland Security Chief of Staff or CIO and the Board will offer their assistance to this effort at that time.

The minutes of the September Board meeting were approved with corrections.

The next topic the Board discussed was digital rights legislation. Board member Susan Landau proposed that she and Board member Rich Guida take the issue paper **[Ref. #4]** they drafted on the subject of digital rights legislation and prepare correspondence to transmit the Board's findings to the Secretary of Commerce with copies to Congressional committees that the Board deemed appropriate. The letter would inform the Secretary of Commerce of the concerns of the Board and indicate that the Board is taking action to review these issues.

The meeting was recessed for the day at 4:50 p.m.

September 19, 2002

The Chairman resumed the meeting at 8:30 a.m. The Chairman and the Board thanked the Secretariat staff for their support of this meeting.

The Board reviewed the latest version of the privacy white paper prepared by John Sabo **[Ref. #5]**. Mr. Sabo also reviewed the comments that had been received as a result of the exposure draft of this document. The members offered minor editing suggestions to the draft report. Mr. Sabo will make the corrections of note and prepare a final text document.

The Board discussed the location of future meetings. It was decided that meetings should be held in the Washington, DC area whenever possible for the purpose of allowing more participation by government officials. It was also noted that at least one meeting a year should be held in a location outside of the metro area to allow other constituents to participate. The Board Secretariat will propose a set of dates for 2003 meeting dates and coordinate future meeting site plans.

Agency Briefing on GPEA Compliance

Board member Rich Guida opened the session with a brief overview of the history of the Government Paperwork Elimination Act (GPEA). He introduced Mr. Len Baptiste of the Internal Revenue Service (IRS), Office of Security Policy Support and Oversight. Mr. Baptiste presented an overview of security and privacy at the IRS. **[Ref. #6]** There are three executive-led security offices within the IRS. The oversight focuses on 15 security capability areas in the Treasury/IRS security assessment framework. Their mission assurance offers enhanced security incident response capabilities, emergency preparedness capabilities and new certification and accreditation strategies. The Privacy Advocate's office ensures that IRS policies and programs incorporate taxpayer and employee privacy concerns. It enables business owners and system developers to identify and evaluate privacy risk through the Privacy Impact Assessment tool and communicate privacy objectives to the public and their representatives. The Disclosure Office reviews systems under certification for compliance with the Privacy Act and IRS confidentiality requirements and makes determinations on whether a new Federal Register system of records notice is required. The Safeguards Office provides security guidelines to agencies and outside contractors that process, store, or transmit federal tax information under the provisions of Internal Revenue Code Section 6103. They also provide onsite reviews of recipient facilities for compliance with safeguard requirements.

Next to speak was Mr. Terence H. Lutes, Director of Electronic Tax Administration at the IRS. **[Ref. #7]** Mr. Lutes addressed the IRS's efforts in electronic filing of tax returns. He said that although the IRS is exempt from GPEA, the efforts are very much the same. There are plans for accepting forms, schedules and other information collection instruments electronically and plans to accept electronic signatures. Challenges that they face include cost and complexity, technical infrastructure, taxpayer adoption and security and privacy issues. The IRS defines authentication as a security measure designed to establish the validity of a person, system, transmission, etc. They define signature as an act undertaken by an individual to indicate the person's identity. Trusted third parties will undertake a stringent application and certification process. Mr. Lutes said that to the extent practical electronic signature needs to be as easy as signing a paper return. For the taxpayer, authentication/signature on a tax return should be no more complex than making a purchase from a commercial web site.

The Chairman thanked Mr. Baptiste and Mr. Lutes for their presentations and would like to invite them to return for a future meeting to update the Board on these activities.

Board Discussion Period

Board member John Sabo presented the amended version of the Board's report of findings and recommendations on government privacy policy setting and management. A motion to approve the final report was made by Board member Charisse Castagnoli and seconded by Board member Michele Moldenhauer. The motion was unanimously approved.

Board member Sally McDonald briefed the Board on her attendance at the ceremony held earlier in the week to announce the President's draft National Cyber Security Plan. She expressed a concern that the draft plan does not adequately reflect the government's GISRA responsibilities. Chairman Reeder recommended that the members review the document and submit their own individual comments, as the time frame for comments on the draft did not allow the Board sufficient time to develop a consolidated Board reply.

There being no further business, the meeting was adjourned at 12:30 p.m.

Ref. 1 - Alan Stapleton's presentation
Ref. 2 - Chris Hankin's presentation
Ref. 3 - Matrix of CSSPAB Work Issues
Ref. 4 - Draft Issue Paper on digital copyright protection
Ref. 5 - CSSPAB White Paper on Privacy Issues
Ref. 6 - Len Baptiste's presentation
Ref. 7 - Terence Lutes' presentation

Fran Nielsen
Board Secretary

CERTIFIED as a true and accurate
summary of the meeting.

Franklin S. Reeder
Chairman