INFORMATION SECURITY AND PRIVACY ADVISORY BOARD
SUMMARY OF MEETING

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

June 15-17, 2004

Tuesday, June 15, 2004

Board Chairman, Franklin S. Reeder, convened the Information Security and Privacy Advisory Board (ISPAB) Meeting at 8:45 a.m. In addition to Chairman Reeder, Board members present during the meeting were:

Bruce Brody
Charisse Castagnoli
Richard Guida
Morris Hymes
Rebecca Lang
Steve Lipner
Sallie McDonald
Leslie Reis
John Sabo

Dr. Alicia Clay and Ms. Pauline Bowen of NIST served as the Acting Designed Federal Official (DFO) during certain portions of the meeting when Ms. Joan Hash, Board DFO, could not be available.

The meeting was open to the public.

NIST Computer Security Division Briefing

Mr. Ed Roback, Chief of the Computer Security Division, met with the Board to discuss the June 8, 2004, NIST letter requesting the Board's advice on several activities that could assist NIST and the Board in meeting their statutory responsibilities. The strategic areas that were identified were: budget, building effective strategic partnerships in support of homeland security, better outreach, NIAP strategy and emerging issues. Mr. Roback also presented an explanation of the Division's budget process, how they received their funding and how the funding was used.

Briefing on Cyber Security Industry Alliance (CSIA)

Mr. Paul Kurtz, Executive Director of the Cyber Security Industry Alliance, began with a brief explanation of who they are, what they do, and their role in cyber security. The CSIA has four standing committees: Public Policy; Standards; Education and Alliances; and Awareness. The CEOs of member companies chair each of these respective committees. More information on the work of the CSIA can be found at www.csialliance.org. Board member Susan Landau mentioned that the CSIA Board is also going to be putting together an R & D priorities list, which could include several topics of interest to the Board.

Development of ISPAB Work Plan

The Board members reviewed and discussed the current work items from their 2002 Work Plan. The task list was updated to include new emerging issues, the NIST strategic areas and to close out those areas that had been completed. Of the twelve task identified, seven were given priority over the others. These task areas were: FISMA, privacy management in government systems, insuring the authenticity of government websites, NIAP strategy, credentialing of cyber security professionals, NIST outreach and partnering, and CSD funding project. The current work plan can be found on the Board's website www.csrc.nist.gov/ispab/.

Briefing on Activities of the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Mr. Robert Dix, Staff Director of the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census began his briefing with general information about the subcommittee's purview and background about the Chairman, Representative Adam Putnam. Mr. Dix discussed some recent and current issues his office is dealing with, including a proposed amendment to the Clinger-Cohen Act. He stated that many of the issues they are dealing with are focused on creating, fostering, and improving market drive for the improvement of IT security in products, processes, and, therefore, the federal government. Mr. Dix discussed the mandates of the Federal Information Security Management Act and those specific mandates to NIST. He also spoke about an upcoming hearing that the committee planned to hold on small business computer security efforts and a hearing on the topic of a Federal CIO.

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

Wednesday, June 16, 2004

Chairman Reeder reconvened the meeting at 8:55 a.m.

Copies of the revised work plan matrix were distributed to the members. Board member task leaders will be expected to present updates at future Board meetings on the progress of the task activities. There was discussion among the members clarifying who the customers for the products of the Board are. This led to discussion about who the customers are for the NIST Computer Security Division products and services. It was agreed that this topic would be put on the agenda for a future meeting of the Board.

Briefing on NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems

Mr. Ron Ross of the NIST Computer Security Division began his briefing with an overview of the Certification and Accreditation (C&A) suite of documents and the C&A process. Some questions were asked about the framework of NIST documents involved with the process. The document's second public draft will be out in August. Mr. Ross gave a description of the format and content of the document, as well as an overview of the process of getting a Standard approved. He reviewed the timeline for the remaining drafts and final publication of NIST Special Publication 800-53 and the subsequent Federal Information Processing Standard 200. Questions were asked about the number, type, and quality of comments received on the first draft. Mr. Ross stated that approximately one third of the comments received were substantive and useful in development of the second draft.

Discussion of CSD Funding White Paper

The Board members spent time discussing the revised draft of the Computer Security Division funding issue paper. They collected comments and issues on the working draft document Dr. Susan Zevin, Director of NIST's Information Technology Laboratory (ITL), joined the Board during this portion of the meeting. Dr. Zevin offered a review of the historical and current funding issues of the ITL program to enhance the Board's knowledge of the CSD funding issues.

After Dr. Zevin's comments the Board began discussion of the general structure of the funding document. Upon completion of the review, the Board voted to accept the paper with the recommended editorial changes. The motion to accept the document was made and seconded. It was accepted unanimously.

The minutes of the March 2004 Board meeting were also accepted unanimously subject to minor editorial corrections.

Briefing on Trusted Computing Group Secure Platform Specifications and Implementation

The next to speak was Mr. Monty Wiseman of the Intel Corporation. Mr. Wiseman represented the Trusted Computing Group (TCG) and briefed the Board on TCG's Secure Platform Specifications and Implementations.

Mr. Wiseman began with a brief history of the TCG and its structure and activities. Explanations of Trusted Platform Modules (TPMs) and various threats (such as email viruses, computer theft, etc.) were given. Mr. Wiseman also covered some common misconceptions about TPM.

The meeting was recessed for the day at 5:20 p.m.

Thursday, June 17, 2004

Chairman Reeder reconvened the meeting at 8:35 a.m. The Board discussed several areas of interest for discussion at future Board meetings. They included updates on the Federal Enterprise Architecture program, computer security activities at the Office of Management and Budget, revisiting the Trusted Computing Groups Trusted Platform Modules effort and an industry, public, government panel on the status of Radio Frequency Identification issues.

Briefing on Draft NIST Special Publication 800-58, Security Considerations for Voice Over IP Systems (VOIP)

Mr. Rick Kuhn of NIST's Computer Security Division began his briefing by stating that this particular draft document had received more comments than many other documents in the past. The general sources for the comments received came from industry, both within and outside of the telecommunication industry.

Mr. Kuhn's overview included reasons why people are using VOIP, who is using it, and a list of possible attacks such as denial of service and compromise of gateways. Mr. Kuhn also discussed issues with using standard firewalls with VOIP. He pointed out that the real security issue here is that a port has to be opened in standard firewalls to make VOIP work.

Mr. Kuhn also explained the National Address Translation (NAT) system and process. He used an example of someone calling from a home location to someone in a business to show the steps of what happens.

To make VOIP more secure, Mr. Kuhn suggested using network tools and protecting voice data. Board Member Susan Landau pointed out that a one-day workshop or lengthier briefing for Federal CIOs and CISOs might be in order since many federal agencies are looking into VOIP systems.

Before Chairman Reeder adjourned the meeting, he extended special thanks of the Board to Elaine Frye for all of her hard work on making this meeting happen and work.

The Board also thanked Dr. Alicia Clay and Ms. Pauline Bowen for serving as the Designated Federal Official during portions of the Board meeting.

There was no request for public participation at this meeting.

There being no further business, the meeting was adjourned until September.

Joan Hash
Board Designated Federal Official

CERTIFIED as a true and accurate
summary of the meeting.

Franklin S. Reeder
Chairman

NOTE: Draft minutes taken by Tanya Brewer-Joneas