# INFORMATION SECURITY AND
# PRIVACY ADVISORY BOARD
# SUMMARY OF MEETING

**Hyatt Regency Hotel, Bethesda**
**7400 Wisconsin Avenue**
**Bethesda, Maryland**

**December 14-15, 2004**

## Tuesday, December 14, 2004

Board Chairman, Franklin S. Reeder, convened the Information Security and Privacy Advisory Board Meeting (ISPAB) for its first meeting of the year at 8:40 a.m. In addition to Chairman Reeder, Board members present were:

Morris Hymes
Steve Lipner
Sallie McDonald
Leslie Reis
John Sabo

The meeting was held in open public session. There were seven public attendees present during the meeting. Mr. Reeder updated the Board members on recent legislative activities involving privacy issues. He also reported that NIST had received a funding increase for their computer security program. Mr. Reeder mentioned that he had met with the newly appointed director of the NIST Information Technology Laboratory, Dr. Shashi Phoha. Dr. Phoha will be invited to meet with the Board at their next meeting in March 2005.

### Update on FIPS 201, Personal Identity Verification (PIV) for Federal Employees and Contractors

Mr. Curt Barker of the NIST Computer Security Division discussed the progress being made in the development of the PIV Standard [**Ref. #1**]. Homeland Security Presidential Directive #12 directed NIST to develop a policy for a common identification standard for Federal employees and contractors. The mandate called for the policy to be in place no later than February 27, 2005. Agencies will be given eight months to implement the requirements of the standard. The Office of Management and Budget (OMB) will issue an implementation guide for agencies to follow. Mr. Barker also reported that NIST's goal is to have NIST Special Publication 800-73, Integrated Circuit Card for Personal Identity Verification, issued at the same time as FIPS 201 is approved. Mr. Barker reviewed the PIV requirements and threats and representative countermeasures. He explained the FIPS development process and timeline that NIST was working with to produce the final standard. The first phase of the effort is to produce the standard by the required date of the HSPD #12. The second phase will cover the implementation and critical support efforts and the third phase will cover the development and coordination of implementing specifications and guidelines. Mr. Barker also indicated that the standard would contain policy pertaining to managing various types of credentials.

Following his presentation, the Board members exchanged their comments and questions with Mr. Barker. The Board commended Mr. Barker and NIST on their efforts in developing this standard and the accompanying guidelines.

## Next Generation Internet Banking and Computer Security Issues

Mr. Stephen Lange Ranzini, President and Chairman of University Bank and Michigan Business Development Company, briefed the Board on standards activities at University Bank and the banking infrastructure projects in which he participates. His briefing topics included global junk email practices, the economics of spam and phishing, spam, domain authentication technology and identity theft and privacy issues. He also identified business problems that arise as a result of these Internet uses and possible resolutions to some of these problems.

## ISTPA Privacy Framework Update

Board member John Sabo briefed the members on the International Security Trust and Privacy Alliance (ISTPA) Privacy Framework activity. The privacy framework is an open policy configurable set of collaborating services and capabilities used to guide the analysis, design and implementation and assessment of privacy solutions and infrastructure. The frameworks services and capabilities cover the following: audit, certification, control, enforcement, interaction, negotiation, validation, access, agent and usage. After significant discussion with members of the ISO JTC-I Group, the ISTPA will work jointly with the Privacy Enhancing Technology and Testing Evaluation Project to enhance the framework effort. A work plan is to be developed in January 2005. Mr. Sabo also presented an overview of the Consolidated Appropriations Action of 2005, Division H Transportation/Treasury, Section 522 calling for each agency to have a Privacy Officer. Mr. Sabo reviewed the Privacy Officers responsibilities as outlined in the Act.

## Department of Homeland Security Privacy Initiatives Overview

Mr. Peter Sands, Director of Privacy Technology for the Department of Homeland Security (DHS) described the Department's current privacy efforts. Mr. Sands noted that the DHS Privacy Office was the first Congressionally-mandated privacy office in the Federal government. Nuala Connor-Kelly heads up the privacy office with a small staff at the Department and 450 people located in positions throughout the agency. Tasks are organized along specific legal lines that cover both international and national issues. Major focuses are on transparency and responsible use of information. The DHS's responsibilities span from fighting terrorism to dealing with natural disasters. The new challenge troubling people today is the fear of the unknown. Information will lead to knowledge that will lead to action that will lead to better security. There are some that view privacy as a barrier to security. This level of fear in the world is what dictates how people respond to use of privacy. Mr. Sands said that information privacy is one privacy concept that you can do something about. For instance, by looking at people's transactions you can see what they have been doing. The success of good information privacy should be to know precisely what the information is and agreement on how it is going to be used. With regard to the establishment of Privacy Officers in each agency, Mr. Sands said that DHS's legislation defined their privacy officer role and responsibilities and suggested that other agencies used a similar or more generalized definition of DHS' for themselves.

## CRM Update

Board member Leslie Reis reviewed the draft white paper that she had prepared for the Board's consideration. The document tracks the use of customer relations management (CRM) techniques used by certain federal agencies and is not intended to be a comprehensive research project effort. This first draft lays out the issues, provides some examples and possible recommendations for the Board's consideration. Overall, it appears that a number of the agencies are embracing the government-to-customer and government-to-government services by adding new services or by making current services more effective. The citizen's awareness of

Privacy Act implementation is raising some issues to the surface. Some recommendations that agencies might want to take into consideration are the requirements of the Privacy Act and the spirit of the intent of the Act at the front of end of any development of government-to-customer service and develop clear cut guidance to educate the citizen/consumer in order for them to make an informed decision or take part in obtaining a service. Also, identifying any alternative low-tech ways to obtain services without having to personal data put into a database would be useful. The Board will review the draft document and provide Professor Reis with any suggested changes or additions by the end of January 2005. The topic will be discussed at the March 2005 Board meeting.

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

## Wednesday, December 15, 2004

Chairman Reeder reconvened the meeting at 8:40 a.m.

### Board Discussion

The Board members discussed the language of Section 522 of the Consolidated Appropriations Act of 2005. They agreed to produce a letter offering their comments and advice on this issue. They were encouraged that the Bill recognizes the distinction between privacy and security.

### Public Participation Period

Ms. Jeniffer Wilson of the General Accounting Offices' (GAO) Information Technology Division addressed the Board. Ms. Wilson noted that her group at GAO primarily works on computer security issues. Her questions for the Board were what authority, if any, do agencies/organizations have to make information publicly available when privacy standards say otherwise, and can agencies assume the risk of disclosure? Chairman Reeder suggested that Ms. Wilson speak with members of the Board individually to gather their perspectives and experiences in this area. The Board as a whole has not taken a position on this issue. It was noted that Ms. Wilson's issues raises serious issues apart from the legal requirement of disclosure and that the Board may want to return to this issue at a future meeting for further exploration and possible action.

### Briefing on the US-Visit Program Activity

Mr. Steve Yonkers, US-Visit Privacy Officer, Department of Homeland Security, briefed the Board on the U.S. visitor and immigrant status indicator technology effort **[Ref. #2]**. He stated that the goals of the US-Visit program are to enhance the security of citizens and visitors, facilitate travel and trade, ensure the integrity of the U.S. immigrant system and protect the privacy of visitors to the U.S. Their mission is to collect, maintain, and share information, including biometric identifiers, through a dynamic system, on foreign nationals to determine whether the individual should be prohibited from entering the U.S., can receive, extend, change or adjust immigration status, has overstayed or otherwise violated the terms of their admission, should be apprehended or detained for law enforcement action and/or needs special protection/attention (i.e. refugees). Mr. Yonkers reviewed the variety of security measures that DHS has in place and he explained who is processed under this program. He identified the positive impacts and successes that have occurred. The US-Visit Office reports to the DHS Privacy Office and consists of a privacy office and a security office. The privacy program's key elements consist of foundational privacy principles, organization, policy, systems development and security, awareness and training, monitoring and compliance and redress and response. As required by Section 208 of the

E-Government Act, US-Visit completes Privacy Impact Assessments to analyze the impacts that their systems may have on privacy and the ways in which any adverse impacts may be mitigated.

## Common Criteria Discussion

Board Member Steve Lipner, and Stuart Katzke of NIST Computer Security Division conducted this session. Also joining Mr. Lipner and Mr. Katzke in this discussion was the Director of the National Information Assurance Partnership (NIAP) Jean Schaeffer. Mr. Lipner began the common criteria (CC) discussion by explaining that he had assumed responsibility for common criteria evaluation at Microsoft. While primarily a national intelligence security effort, Mr. Lipner suggested that there was an opportunity for a government agency to use the process as a seal of approval for their individual efforts. It was his observation that the Board might want to weigh in and make some recommendations about the potential for common criteria reform to move things in a positive direction for both industry and the government information technology community. Dr. Katzke said that he was one of the originators of the CC and the NIAP program efforts and was speaking for himself and not as a representative for NIST. Dr. Katzke felt that in order for these efforts to continue to be successful, the CC paradigm needed to be evaluated to discover what people are using CC today and what could they be using it for. However, CC will continue to evolve and be useful even if evaluations are never performed. Common criteria schemes need to pay more attention to the cost/benefit issues of CC evaluation processes and provide better support to the most important users: system integrators and developers. There needs to be more focus on consensus-based standards/requirement sets, conformance tests and test methods, and security checklists/implementation guides and configuration settings. There is also a need for improvement in product/system development approaches and product/systems evaluation and testing.

The NIAP program is currently undergoing review by the Institute for Defense Analysis. When asked if they would recommend eliminating either the NIAP or CC efforts, the speakers all agreed that implementation difficulties existed that could be changed, however, the programs should still exist. Dr. Katzke also pointed out that there have been questions raised regarding the CC evaluation process with respect to the evaluation criteria mandated by FISMA requirements.

The Board will keep this issue on their list of topics to bring to their attention again at a future meeting.

## Professionalism Credentialing Briefing

Mr. George Bieber of the Defense-wide IA Program at the Department of Defense (DOD) spoke to the Board on the IA training, certification and workforce management efforts at DOD. **[Ref. #3]** He presented some background material on the program and identified the objectives and certification targets. Mr. Bieber said that one of the more significant benefits of accreditation is that it helps develop confidence by attesting in an independent, measured, and documented manner that an institution meets or exceeds current professional standards based upon a periodic thorough review and "site" inspection conducted by experts. He encouraged the Board's support and endorsement of the use of certification standards within the government.

## Board Discussion

The Board reviewed and agreed upon the proposed meeting dates for 2005. The approval of the minutes from the September meeting was deferred until the March 2005 meeting.

The Board identified topics for their March 2005 meeting. It was also noted that by that time the three vacancies on the Board should be filled.

There being no further business, the meeting was adjourned at 4:00 p.m.

Ref. 1 - Barker presentation
Ref. 2 - Yonkers presentation
Ref. 3 - Bieber presentation

Joan Hash
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting.

Franklin S. Reeder
Chairman