INFORMATION SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

The Hyatt Regency Bethesda
One Bethesda Metro Center
Bethesda, MD

December 16-17, 2003

Tuesday, December 16, 2003

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

Bruce Brody
Lynn Bruneau
Charisse Castagnoli
Richard Guida
Morris Hymes
Susan Landau
Rebecca Leng
Steve Lipner
Sallie McDonald
Leslie Reis
John Sabo
Howard Schmidt

The meeting was open to the public. There were ten visitors present at the beginning of the meeting.

Chairman Reeder extended a welcome to the newest members of the Board. Mr. Brody, Ms. Leng and Mr. Schmidt introduced themselves and gave a brief overview of their background, the organizations that they are part of and what areas/topics they believe are at the forefront of today's information security and privacy agenda.

Privacy Challenges – Department of Homeland Security

Ms. Nuala O'Conner-Kelly, Privacy Officer of the Department of Homeland Security (DHS) began her briefing with an overview of the organizational layout of DHS. The Department is comprised of five major divisions or directorates: Border & Transportation Security; Emergency Preparedness & Response; Science & Technology; Information Analysis & Infrastructure Protection; and Management. The Privacy Officer position is a Congressional-appointed position. The Privacy Officer reports directly to the Secretary of DHS. The Privacy Officer's responsibilities include assuring that new information technology does not erode sensitive personal information of the public. They are responsible for examining technology for the privacy impact on the civilian individual's personal privacy.

A good example of the privacy challenges being faced is the CAPS I [computer-assisted passenger system] that is in use today. CAPS II is in the developmental stage. CAPS II has

three main components to it. One of those components, the use of private sector data to do a correct authentication of a person when they make an airline reservation, is meeting with some opposition. DHS sees its role as a guardian and watchdog for issues of private sector technology and the use of personal data.

Board member John Sabo referred Ms. O'Conner-Kelly to the Board's September 2002 privacy findings and recommendations and suggested that she review it for consideration of the findings reached by the Board. The Board posed several questions and offered specific points of view for DHS to consider.

- Does DHS plan to issue a government-wide directive dealing with privacy assessment policy?
- Managing the privacy infrastructure and the advocacy role [i.e. privacy folks not talking with each other and the need for a central focus], appears to be two specific aspects to meeting the privacy challenge. How is DHS dealing with this issue of the two equally important roles.

Ms. O'Conner-Kelly stated that she believes functionality is the key to the success of building a trust agenda for the Department. The business case importance of public trust is evident by the numerous engagements the DHS Privacy Office has had with outside agencies.

The Board questioned Ms. O'Conner-Kelly on what DHS is involved with in the area of e-government and the "touching the browser" scenario. Ms. O'Conner-Kelly responded that DHS is involved in the next tier down in the authentication area. With regard to the challenges of e-mail and identify theft, DHS is planning to develop a pro-active approach reaching out to businesses and citizens [the end-user] asking for due diligence. The linkage of security and privacy is both good and bad. DHS has the advantage of being able to secure state-of-the-art technology to address these challenges, but the down side is that they have to play catch up. Ms. O'Conner-Kelly said that the next major focus area for her office will be dealing with the e-FOIA issue.

Chairman Reeder thanked Ms. O'Conner-Kelly for her presentation and extended an invitation to her to meet with the Board again in the near future. He said that the Board sees its role as looking for models of success to point to and offered to support DHS's efforts toward meeting their goals.

NIST Computer Security Division Update

The Board held a session to review the programs of the National Institute of Standards and Technology (NIST) Computer Security Division (CSD). The Chief of the Division, Mr. Ed Roback, opened the session. Presentations by each respective Division group manager followed..

Mr. Roback presented a high-level overview of the CSD identifying its mission, statutory mandates, focus areas, and budget trends. The Board noted that the budget allocation for CSD's programs was lower than the previous year. Mr. Roback explained that STRS funding would only cover 80-85% of the base salaries for the year. The remainder of the funds would have to come from obtaining Other Agency funding support. It was also anticipated that the Division would have to take another 9% hit to cover a proposed government pay raise.

Board member Howard Schmidt recalled the earlier proposal to move the Division into the Department of Homeland Security. Mr. Schmidt said that he believes that certain members of Congress need to have a better understanding of what the CSD does. There is an obvious need to educate the Congressional Appropriation Committee members.

Board member Steve Lipner asked about the comparison of the number of staff before the Computer Security Act was enacted and since then. Mr. Roback stated that the staff numbers have grown relatively. Base funding pays for about 80% of the staff of 45 employees.

Board member Morris Hymes suggested that NIST look at industry and its level of raising the security bar. Mr. Hymes doesn't believe that industry [at the interoperability product level] is stepping up to the bar, and, therefore, there is a strong need/justification for NIST to be enhanced.

Mr. Roback continued his presentation by reviewing the statutory mandates given to the Division as a result of the Federal Information Security Management Act of 2002 (FISMA) and the Cyber Security Research and Development Act of 2002. Under the FISMA, NIST is responsible for the development of a minimum standards requirement guide. Board member Rebecca Leng commented that meeting such standards would put an added burden on Agency Inspectors General to enforce. Ms. Leng asked what consequences are going to be put in place for not complying. Mr. Roback stated that the answer to that would have to be determined by the Office of Management and Budget.

Mr. Roback reviewed other work products of the Division and addressed how they work together. He also discussed the challenges that still remain. These challenges fall into the area of the development of specific technology guidelines, specifications, testing requirements, and guidance for settings of specific products and scanning tools. They also include the development of a comprehensive guidance suite and the expansion of the cryptographic toolkit and related testing.

Mr. Reeder said that the Director of NIST, Arden Bement, has expressed his interest in having feedback from the Board on the programs of the Division.

Board member Steve Lipner asked if there was much overlap between what the Division is currently doing with that of what the Department of Homeland Security (DHS) is or will be doing. Mr. Roback answered that he would be meeting with DHS officials in the near future to discuss some of the apparent areas of potential overlap.

Board member Charisse Castagnoli asked what the Division would be able to do if their funding were increased by a minimum of $5M. Mr. Roback responded that substantial contributions could be made in the areas of wireless technologies and protocol design. It would offer an opportunity to bring the federal government and industry officials together to collaborate on the development of specific solutions.

Review of NIST Management and Assistance Group Program

Ms. Joan Hash, Manager of the Management and Assistance Group, presented an overview of the group's activities **[Ref. #2]**. The focus areas that were discussed were the development of policy and management guidelines, the Computer Security Resource Center website of the Division, outreach activities, practices and checklists/implementation guides, small and medium-sized business regional security meetings, expert assistance, and the system certification and accreditation project.

Mr. Reeder suggested that NIST notify members of Congress about the small business workshops that are being held so that they might forward the information to their constituents. This would create an opportunity for the Congressional delegation to inform their constituents and would be one more vehicle that could be used to increase the visibility of the Division's work in this area. Ms. Hash stated that the Federal Trade Commission is looking to engage with the Division in the small business arena. Ms. Hash also addressed the status of the Division's CSEAT activity. Even though funding was not forthcoming for a more extensive CSEAT program, the Division is still willing to work with other agencies to review their security systems and identify areas that may need improvement. This review is being offered on a cost reimbursable basis.

Review of NIST Security Testing and Metrics Group Program

Mr. Ray Snouffer is the Manager of the Security Testing and Metrics Group **[Ref. #3]**. Three specific areas of responsibility for this group include the Cryptographic Module Validation Program (CMVP), the National Information Assurance Partnership and the Security Certification and Accreditation Project.

The President's National Strategy Plan calls for the review of the NIAP program and funding has been secured for transition of the program to the Department of Defense. NIST and DHS are seeking lots if input from the private sector. It was suggested that this issue could be a Board focus area within the coming months and a briefing by the contractor working on this transition effort could be scheduled for the Board at a future meeting.

Review of the Security Technology Group Program

Mr. William Burr, Manager of the Security Technology Group, was next to present his program overview **[Ref. #4]**. Mr. Burr's group consists of a cryptographic standards team, an authentication and infrastructure team and work in the area of biometrics standards. The handout material that was distributed provided an in-depth review of these activities. Mr. Burr reported that the issue of quantum computing is not expected to be a problem for some time to come. It was also mentioned that the Public Key Infrastructure standards effort was being closed out as the program has matured over time and the IETF and ISO PKI standards activities are winding down. Mr. Burr stated that he was especially interested in getting the Board's views on what areas were best for NIST to participate in because it was not possible to participate in every arena.

Board member, Charisse Castagnoli, asked if biometric standards still have need to have reliable e-authentication. Mr. Roback replied that a separate unit within NIST deals with biometrics and they could be asked to address the Board on these issues.

Mr. Roback did request that the Board provide any comments they may have on the draft Special Publication 800-53, Recommended Security Controls for Federal Information Systems and on the draft Federal Information Processing Standards (FIPS) 200, Minimum Security Controls for Federal Information Systems.

Review of the Systems and Network Security Group

Mr. Tim Grance, Manager of the Systems and Network Security Group, reviewed the IT security research trends and issues of his group **[Ref. #5]**. He discussed the overarching themes and pointed out areas of change in the computer security environment of today. The group's activities include the development of technical security guidelines, a government Smart Card program, mobile device security, wireless security standards, the ICAT metabase, an Internet protocol security project, access control and authorization management activity, automated security testing, the critical infrastructure protection grants program and a scalable quantum information network activity. The group has produced 12 guidelines in these related areas. Mr. Grance also addressed the areas of privacy and security in Radio Frequency Identification and the use of dedicated short-range communications applications and their goals.

Update on OMB Security Activities

Ms. Kamela White of the Office of Information and Regulatory Affairs at OMB discussed the security-related activities currently underway. One of the security priorities at OMB is the submission of the annual OMB report to Congress. This will be the third year that OMB has issued the annual report. It's a government-wide assessment of where we are and what's ahead

in the security area for agencies. It also provides an individual summary of computer security from individual agencies. Another priority is the issuance of standardization of the OMB guidance. Quantitative performance measures have been very useful. Inspector Generals have also provided valuable feedback on their remediation process. Ms. White said that Jeanette Thornton, OMB, had completed work on their e-authentication document and it was released today [December 16]. Agency privacy impact assessments were due to OMB by December 15. OMB must make their report to Congress on this issue by mid-March 2004. Ms. White reported that updating OMB Circular A-130 is project they will focus on in the months ahead. When drafts become available, the Board will be sent copies and asked the Board for their feedback and comments. When asked about the number of staff at OMB working in the computer security and privacy area, Ms. White responded that there are currently three people working on IT security and one employee with the assistance of a detailed government employee make up the staff looking into privacy issues.

Mr. Reeder asked if OMB has taken any official notice of the recent Congressional report cards and if there are any consequences to agencies for failing to meet expectations. Ms. White replied that OMB plays no part in the Congressional committee assessments. However, she was pleased to note that some of the agencies' grades showed some improvements. A similar methodology was used from the previous year with some positive results.

In regards to the question of consequences, Ms. White stated that security has a great impact on agencies' ability to improve their scorecards. If the agencies don't meet the minimum requirements, there can be significant embarrassment among peers and higher-level officials. Some agencies have taken steps to include compliance as part of the Chief Information Officer's performance plans. In the view of OMB, when an agency is not demonstrating plans for security shortfalls, what are the consequences to the respective agency, asked Mr. Reeder. Ms. White replied that growth management and budget tools are used in these cases to correct the observed discrepancies.

Board member Rebecca Leng expressed her concern that the topic of computer security in the e-government scorecard may get lost in the midst of other scorecard items. She is also concerned that given all the other responsibilities that agencies are dealing with, agencies may have difficulty sustaining a sound level of computer security accountability. Ms. White said that with the agency performance measurement data being collected quarterly, OMB could notify an agency when they notice any slippages and provide feedback to the agency heads. This would allow for appropriate adjustments to be made prior to the reports cards being issued.

Mr. Reeder thanked Ms. White for her informative update.

The meeting was recessed for the day at 5:19 p.m.

Thursday, December 18, 2003

The Chairman reconvened the meeting at 8:37 a.m. The meeting began with a review of the draft minutes from the September 2003 Board meeting. The minutes were approved with modification.

Board Discussion Period

The Board discussed the presentations from the Computer Security Division presented to the Board the previous day. Board member Susan Landau expressed her concerns about the lack of support being given to the Division. Mr. Reeder and Mr. Schmidt agreed to assist Dr. Landau on this effort. The agenda for the March 2004 Board meeting will have a period of time dedicated to this activity. It is anticipated that a draft paper will be produced and distributed to the Board members for adoption at the June meeting of the Board.

Board member John Sabo noted that there is some excellent work being performed in the Division but he does not see these efforts being touted to the outside world. He suggested the possibility of organizing a one-day workshop to feature the positive output of the work effort coming from the Division.

Another area the Board could take a look at would be the development of alternate financing strategies, suggested Mr. Reeder.

Board member Rich Guida noted that there may be some flexibility within NIST's internal funding allocations. One of the missing elements that he has observed has been the cry for help from the customer/consumer. There have been no complaints from the customers/consumers that they are not getting their needs met and. Mr. Guida also said that it would be highly unlikely that any complaints of this nature would be forthcoming from federal sources.

The Board will continue to discuss this topic at their March 2004 meeting.

Briefing on GAO's Report on the Privacy Act

Ms. Linda Koontz, Director of Information Management Issues at the General Accounting Office (GAO) discussed the recently issued report on the results of their review of the compliance of federal agencies with the Privacy Act **[Ref. #6]**. Three surveys at 25 departments and agencies were performed. These surveys were looking at agency-wide practices, samples of systems of records, and information outside Privacy Act systems of records. GAO also solicited documentation or explanations for a random sample of responses to the surveys and they convened a forum of agency Privacy Act officers. To improve agency compliance, GAO recommended that the Director of OMB direct agencies to correct the identified deficiencies in compliance with the Privacy Act, oversee implementation of actions to correct these deficiencies, and, monitor overall agency compliance with the Act. To address implementation issues, GAO recommended that OMB assess the need for specific changes to OMB guidance (especially with regard to electronic records) and update it as appropriate. It was also suggested that OMB raise the awareness and commitment of senior agency officials to the importance of the principles that underlie the Privacy Act.

Ms. Koontz stated that since the report was issued, OMB had convened at least one meeting of the Privacy Act Officers with the plans to have these meetings on a regular basis. GAO also gave OMB their compliance issue findings for OMB to handle as they deemed appropriate.

Mr. Reeder encouraged GAO to look at the adequacy of the Privacy Act in how it is dealing with changing technologies such as systems of records and agency use of information that is held by third parties. Ms. Koontz said that GAO plans to have a report issued on the use of third party information sometime after the New Year.

Review of Board's Customer Relations Management (CRM) Planning Session Effort

Board members Leslie Reis and Lynn Bruneau reported on the preliminary fact finding effort they have done on the CRM issue. With the assistance of Mr. Adam Hicks, a research associate from the John Marshall Law School, Ms. Reis reviewed the purpose of the effort. As the federal government becomes more involved in its e-government agenda, Professor Reis believe that private sector CRM methodologies can be useful for enhancing government services in a positive way. For the purposes of this effort, CRM will refer to strategies that can be used to promote eht e-government initiatives and enhance government-to-citizen services. The processes to be used to perform this exercise will be contact management, relationship management [data mining] and knowledge management. Professor Reis stated that four major issues involving the amount of

the various types of information being collected using the CRM approach might actually be in violation of the spirit if not the letter of the Privacy Act.

Mr. Reeder noted the need to characterize tension inherent in this issue. This might be an important observation that the Board should take into consideration as they pursue this topic. The Board should take note of the perceived boundary condition of the government doing what the private sector may already be doing or competing with the private sector. This observation should be noted but not pursued in this current CRM exercise.

Mr. Adam Hicks offered his observations on how to improve government services to the public. He reviewed how CRM is being deployed within agencies. The E-government Act, building on the Government Paperwork Elimination Act, provides better interoperability. The Act calls for agency privacy impact assessments, the posting of privacy policies by agencies, and calls for the establishment of the Office of Electronic Government under OMB. The President's management agenda endorses a more market-based approach to government services. During the past year, OMB has provided progress updates as a result of monitoring how agencies deployed e-government strategies.

Professor Reis said that their research found that there was limited public opinion available. However, there was a report issued by Excellence in Government that indicated there was some concern expressed by the public to proceed slowly in matters affecting their privacy. Thus, the marketing process should be done with the awareness of the public's fear factor perception.

A Presidential initiative from last summer endorsed e-government programs within the United States Postal Service (USPS). The USPS was directed to develop an intelligent mail system for the purpose of tracking mail as a result of the Anthrax attacks. The Internal Revenue Service (IRS) has several data sharing initiatives underway such as e-filing of individual tax returns. The Department of Housing and Urban Development (HUD) is engaged in a homeless tracking service. Other agencies that are involved with CRM efforts include the General Services Administration [reverse auction and equity issue and on-line property disposal], the Department of Energy, Social Security Administration and the Department of Veterans Affairs. Board Members Reis and Bruneau discussed possible structure of a white paper and need for an informational briefing in March.

Department of Veterans Affairs Cyber Security Program Overview

Mr. Bruce Brody, Associate Deputy Assistant Secretary for Cyber and Information Security at the Department of Veterans Affairs (VA) presented an overview of the VA Cyber Security and Privacy programs **[Ref. #7]**. Mr. Brody reviewed the history and mission of the program. The Enterprise Privacy Program is one of six services in the Office of Cyber and Information Security. The program supports the VA's need to comply with various laws related to privacy controls, especially the Health Insurance Portability and Accountability Act (HIPPA). The Board was impressed with the professionalism aspect of the VA program. Mr. Brody said that the VA is the only agency currently using such a practice and he would like to see this practice used throughout all of the federal agencies. It was suggested that the Board may want to review this issue and make a recommendation that the Office of Personnel Management look into the establishment of such a practice across the government.

Board Discussion Period

Dr. Landau briefed the Board on a committee within the Computing Research Association (CRA), the Committee on the Status of Women in Computing Research. The goal of the committee is to take positive action to increase the number of women participating in Computer Science and Engineering (CSE) research and education at all levels. Dr. Landau is a member of this committee. She reported on the conference on "Grand Research Challenges in Information

Security and Assurance that was held on November 16-19, 2003. A small group of academic and industry computer researchers got together to frame computer security questions in ways that were simple to explain. The group identified four challenges that they believed worthy of sustained commitments of resources and effort. They were to eliminate the widespread attacks by viruses, worms and email spamming within the next ten years; the establishment of the trustworthiness of the Internet so that it could be used for large societal interactions; ubiquitous computing of small devices and the development of measurement of risk analyses for computer security within the next decade.

The Board reviewed their action items from the meeting and decided on the topics to be included on the agenda for the March 2004 meeting.

There being no further business, the Chairman adjourned the meeting at 3:40 p.m.

Ref. 1 Roback presentation
Ref. 2 Hash presentation
Ref. 3 Snouffer presentation
Ref. 4 Burr presentation
Ref. 5 Grance presentation
Ref. 6 Koontz presentation
Ref. 7 Brody presentation

/s/

Joan Hash
Board Designated Federal Official

CERTIFIED as a true and accurate
summary of the meeting.

/s/

Franklin S. Reeder
Chairman