INFORMATION SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

Hyatt Regency Hotel, Bethesda
7400 Wisconsin Avenue
Bethesda, MD

March 11-13, 2003

Tuesday, March 11, 2003

Board Chairman, Franklin S. Reeder, convened the Information Security and Privacy Advisory Board Meeting (ISPAB) for its first meeting of the year at 8:36 a.m. This was the first meeting held since the name of the Board was changed from the Computer Security and Privacy Advisory Board Meeting to the Information Security and Advisory Board by the passage of the E-Government Act of 2002 in January 2003.

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

Charisse Castagnoli
Richard Guida
Susan Landau
Steven Lipner
Leslie Reis
John Sabo

Board Discussion of ISPAB Work Plan

The Board took this time to review the status of the work plan items that they had previously identified.

The first work plan reviewed was on the GISRA/FISMA activity. Joan Hash of NIST provided the update. Ms. Hash reported that NIST had analyzed the lessons learned from GISRA and identified where NIST should put their resources to assist other federal agencies. The trend being seen in current legislative efforts is a stronger push for use of NIST guidance and the possibility of making these guidance documents mandatory. The current NIST Special Publications are offered as guidance only at this time. However, the language in forthcoming legislation will reflect OMB's thoughts to have the NIST documents be more enforceable.

Chairman Reeder recommended that the Board develop a list of action items/guidance topic areas that the Board would like to see NIST do. It was also pointed out that there is a poor rate of adoption of Federal Information Processing Standards (FIPS) by the private sector. A better partnership to find the impediments to adopt more standards with industry would be useful. It was acknowledged that defining systems is a difficult task because of the tentacles that embrace systems and, therefore, the development of a common definition would be useful.

NIST will continue to provide the Board with copies of all of their draft guidance documents and request their review and comments.

The second work plan review was on the baseline standards/benchmarking activity. Board Member Steven Lipner will arrange for a session at the June meeting to provide an update on these activities. Those invited to participate in the session will be representatives from NIST,

DOD, DOE, DISA, NSA, SANS and CIS. The recent Cybersecurity Research and Development Act contains language that pushes for the adoption of a set of common baseline standards/practices.

The third work plan activity to be discussed was the privacy and e-government activity. Board Member John Sabo reviewed the project's mission to establish public trust in the security of information exchange over the Internet. There will also be an e-authentication session at the June meeting which will focus on two areas: e-authentication systems: a primer on available and emerging models, and, security and privacy issues in e-authentication.

The next work plan activity discussed was the emerging IT security issue. Board Member Charisse Castagnoli reported that it was her feeling that there was nothing more that could be done on this issue by the Board. Third party organizations have been treating this issue fairly well and in a timely fashion. Ms. Castagnoli did acknowledge that other classes of emerging issues do exist and that the Board could approach these on a case-by-case basis. It was decided that the emerging IT security topic would be eliminated from the Board's work plan list.

The NIST Handbook was the next work plan activity discussed. Board Member Charisse Castanogli reported that she had reviewed the document. The Handbook is the cornerstone foundation of NIST guidance, however, it is in need of a facelift. It was recommended that the Board work with a small subset from industry and review this issue. The goal would be to develop a new table of contents and recommend an approach to NIST for their consideration. The Board authorized Ms. Castagnoli to proceed with this work effort by conducting fact-finding exercises to provide input to the development of a proposed draft outline for a revised handbook document.

Joan Hash of NIST reported on the NIST Guidelines activity. In December 2001, NIST contracted with Booz, Allen and Hamilton for an analysis of NIST computer security guidance documents. Ms. Hash presented a brief overview of the findings of this analysis and stated that NIST was requesting a ratification of this document and would be welcome any additions that the Board would like to suggest.

The next work plan activity to be reported was on Government Paperwork Elimination Act (GPEA). Board Member Rich Guida offered two approaches for the Board to consider. One, the Board could receive GPEA activities briefings as circumstances permit from agencies such as Agriculture, Social Security and Health and Human Services. The other would be for the Board to sponsor a session at an upcoming meeting and invite agencies to present. The session could also include private sector participants to expound on their concerns. From this session, the Board could issue a white paper of its findings and recommendations. Discussion followed on the general issues that needed to be considered. Mr. Guida will develop a protocol for the data gathering necessary to pursue this session for the September meeting.

Board Member Susan Landau discussed the work plan issue on the Digital Millennium Copyright Act (DCMA). It was reported that the Board's letter to the Secretary of Commerce had been cleared by NIST and sent. The correspondence will be posted on the Board's website. No further action is needed on this topic at the present time. Dr. Landau will keep the Board apprised should their be further developments in this area.

There was no update on the work plan item regarding strategy for NIAP outside of the national security community. The topic will be addressed at future meetings.

Chairman Frank Reeder was next to speak on the issue of credentialing of cyber security professionals. He reported that the National Strategy to Secure Cyberspace addresses the certification issue. Mr. Reeder has prepared a draft white paper [not affiliated with this Board activity] that proposes a non-profit credentialing process. Copies of this document will be provided to the Board members for their information. Mr. Reeder indicated that there were no

specific actions that the Board could recommend on this issue. However, a briefing on the status of credentialing efforts will be scheduled for the June meeting of the Board.

NIST Information Technology Laboratory (ITL) Briefings

Dr. Susan Zevin, Acting Director of ITL, presented an overview of the programs of the laboratory **[Ref. #1]**. The presentation covered an overview of the organization, the environment of the laboratory, some specific ITL programs, the ITL community, the resources and the challenges of the laboratory. Dr. Zevin introduced ITL in mass because everything that ITL does ties into the role of the Board. Dr. Zevin said that in recent talks with CEO's and others, computer security awareness is seen from a much broader perspective. With the exception of the computer security area, ITL does not develop standards. Much of the ITL work is being leveraged toward enhanced critical infrastructure protection. There are new demands for information assurance. ITL is already looking in the area of the next revolution in computing which is going from nano to quantum. Dr. Zevin reported that the ITL program is a well-focused program with a full agenda. The funding is small so projects must be considered carefully and prioritized for funding. Chairman Reeder thanked Dr. Zevin for her briefing and is very grateful for the support that NIST provides to the Board.

Other members of the ITL divisions briefed the Board on their areas of expertise. Barbara Guttman of the Software Diagnostics and Conformance Testing Division gave a presentation on computer forensics: the Tool Testing and National Software Reference Library **[Ref. #2]**. David Griffith of the Advanced Network Technologies Division briefed the Board on resilient optical networks **[Ref. #3]**. Nader Moayeri of the Advanced Network Technologies Division reported on the NIST distributed testbed for first responders **[Ref. #4]**. Charlie Wilson of the Information Access Division discussed biometrics accuracy standards **[Ref. #5]**.

Chairman Reeder thanked everyone for the presentations saying that the briefings were all of particular interest to the Board.

The meeting was recessed for the data at 5:04 p.m.

March 12, 2003

Chairman Reeder reconvened the meeting at 9:05 a.m. and called for the approval of the minutes of the December 2002 meeting. After the acceptance of several editorial changes, the Board approved the minutes.

OMB Privacy and Security Updates

Eva Kleederman of OMB gave a Privacy update to the Board. OMB wants an automated process to match one's privacy preference against agency practice. This supports an effort to give people choice. Board Member John Sabo emphasized that it is critical to address all requirements of the Privacy Act when developing automated privacy systems. Board Member Susan Landau. mentioned the Canadian List of Fair Privacy Practices and noted that they are now looking at the implementation side.

Ms. Kleederman noted that OMB is assisting Homeland Security and surviving agencies with their Privacy policies. The focus is on routine uses since the boundaries have changed. She also noted that there is to be a nomination process for the Privacy Advocate position required by the Homeland Security Act. She confirmed that it is the first statutory Privacy Advocate.

Also, it was pointed out that although there is a liaison on the CIO Council for security, there is no comparable representative for Privacy. The Board suggested that OMB bring together groups of people to address the numerous issues on National Strategy for Cyber Security.

Next to speak was Kamela White from OMB who updated the Board on OMB security activities. Ms. White reported that OMB is doing GISRA closeout and the Annual Report to Congress is in process. It was emphasized that the FISMA attached to the E-Government Bill is the prevailing version. OMB is focusing on the differences between GISRA and FISMA in preparing its guidance for agencies. It is anticipated that the updated version of such guidance will be very close to the prior GISRA version. She reported to the Board that OMB annually approves/disapproves agency security programs via a formal letter. Ms. White noted that OMB is seeing a steady increase in overall compliance in all areas including Security Plans, Contingency Plans and Certification and Accreditation. OMB is also seeing recurring problems.

The FISMA calls for the establishment of minimum security standards and there is a strong push for a formal Enterprise Architecture. The FY2004 budget process shows security dollars increasing. If agencies fail security criteria they are put on a system "AT RISK" list. Agencies have until the end of September to show improvement. In some instances agencies have not been funded.

Board Discussion on National Strategy Plan

The Board resumed its discussion of the review of the National Strategy Plan. Comments were made and the Board developed a draft letter for the Board to send to the Director of OMB. A final document was agreed upon and will be forwarded to the Director of OMB by the Chairman on the Board's behalf **[Ref. #6]**.

Federal Information Security Management Act of 2002 (FISMA) and the NIST Role

Ed Roback, Chief of the NIST Computer Security Division presented a briefing on the NIST strategy for implementing key provisions of the Federal Information Security Management and the Cyber Security R&D Acts **[Ref. #7]**. In his overview Mr. Roback discussed the changes that FISMA made to the Computer Security Act. He also covered the provisions of the respective Acts that the Computer Security Division will be required to carry out. FISMA tasks NIST to develop standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; develop guidelines recommending the types of information and information systems to be included in each category; and, develop minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category. Mr. Roback reported that planning is already underway for each of these activities. Federal Information Processing Standard (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," will be published no later than December 2003. Special Publication 800-60, "Guide for Mapping Types of Federal Information and Information Systems to Security Categories," will be published no later than June 2004 and a public workshop is being planned on the topic. Federal Information Processing Standard (FIPS) Publication 200, "Minimum Security Controls for Federal Information and Information Systems", is due for final publication no later than December 2005. Other documents being planned are Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" and Special Publication 800-53A, "Guide for Verifying the Effectiveness of Security Controls in Federal Information Systems." An update to Special Publication 800-26, "Security Self-Assessment Guide for Information Systems" is also planned. The R&D Act does not provide any funding for carrying out the stated NIST tasks. There has been some discussion, however, to work on the Cyber Security Checklist requirement by instituting some type of web-based clearinghouse for products, similar to a search engine, that would bring up checklists for specific products. Mr. Roback welcomed the Board's

advice and opinions on this approach and he noted that this effort might be a great way to show a public-private partnership.

Briefing on Proposed Federal Information Processing Standard (FIPS) 199, Categorizing of Federal Information and Information Systems

The next speaker was Mr. Ron Ross of NIST's Security Testing and Metrics Group. Mr. Ross brought the Board up-to-date on the draft FIPS 199 **[Ref. #8]**. Mr. Ross presented a brief history of the document and its purpose. Board member Rich Guida, referring to the Atomic Energy Act of 1954, asked how this FIPS was going to address that type of information that is not "classified" but is considered "national security" information. Mr. Ross suggested that NIST might have a workshop where these types of concerns could be addressed and discussed with the expert attendees before reaching a final resolution on how to address such concerns. Mr. Ross discussed the three levels of risk, low, moderate and high, and how they are to be determined. Discussion between Mr. Ross and the Board followed his presentation.

Public Participation

Chairman Reeder called for any public participation. There were no requests to present.

The meeting was recessed at 5:10 p.m.

March 13, 2003

Chairman Reeder reconvened the meeting at 8:40 a.m. The Board discussed the action items to be included on the agenda for the June 10-12, 2003, meeting of the Board.

Critical Infrastructure Protection Project Briefing

Dean Mark Grady of the National Center for Technology and Law, George Mason University (GMU) School of Law briefed the Board on GMUs' critical infrastructure protection project **[Ref. #9]**. Dean Grady reported that GMUs approach combines technical solutions with legal and policy solutions. The recent fire in a Rhode Island nightclub was used as an example. Various standards are supposed to prevent this type of accident and do reduce the risk of it occurring, e.g., building codes, fire codes, product flammability standards, insurance standards, civil liability (tort) standards. Comparisons were made between cybersecurity and other situations such as hurricanes, smog/clean air, earthquakes, traffic/driver behavior, etc. Following dialogue with the Board members, Chairman Reeder thanked Dean Grady for his informative briefing.

Update on U.S. Postal Service (USPS) Business Impact Assessment Program

Zoe Strickland and Peter Myo Khin of the USPS gave the Board an update on the business impact assessment program **[Ref. #10]**. Chairman Reeder praised the USPS for integrating privacy policies into their business processes. Ms. Strickland began her briefing with a short background of the Postal Service, their privacy program, and their security program. A comparison was asked for and made between the USPS and other countries such as Canada, France, Germany, Singapore, China and Australia. Ms. Strickland said the USPS appears to be more creative in that they put privacy into their business model unlike many of the European countries. Those countries seem more focused on compliance alone. Questions were addressed regarding the USPS's systems and policies in place such as the password policy and remote accessibility. Ms. Strickland and Mr. Khin also addressed questions regarding data management issues, network borders and security programs in place.

Briefing on the General Services Administration (GSA) Multi-Tier Security Profiles (MTSP) Initiative

Mr. David Jarrell, FTS Office of Service Development at GSA, briefing the Board on their Multi-Tier Security Profiles (MTSP) Initiative. This briefing provided the Board with an update on how GSA-FTS is addressing the requirement to increase security in the services being delivered to their customer agencies. The original effort began with the desire for a government only Internet (Govnet). Even though Govnet is no longer active, the need to improve information security government wide still exists. GSA is working with vendors to provide the multi-tier security services. To date, three tiers are available and the fourth tier is expected to become available sometime in the fourth quarter of this year. The Board invited Mr. Jarrell to return in September to provide another update of this activity.

There being no further business, Chairman Reeder adjourned the meeting at 12:45 p.m.

Ref. 1 – Zevin presentation
Ref. 2 – Guttman presentation
Ref. 3 – Griffith presentation
Ref. 4 – Moayeri presentation
Ref. 5 – Wilson presentation
Ref. 6 – Letter to Director of OMB
Ref. 7 - Roback presentation
Ref. 8 – Ross presentation
Ref. 9 – Grady presentation
Ref. 10 – Strickland presentation

Joan Hash
Board Designated Federal Official

CERTIFIED as a true and accurate
summary of the meeting.

Franklin S. Reeder
Chairman