COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

University Place Conference Center
Indiana University-Purdue University
Indianapolis, IN
March 6 and 8, 2001

***Action items are highlighted In *BOLD/ITALIC* text.**

Tuesday, March 6, 2001

Board Chairman, Franklin S. Reeder, convened the Computer System Security and Privacy Advisory Board meeting for its first meeting of the year at 9:10 a.m.

Members present during this meeting were:

Mr. Peter Browne
Ms. Charisse Castagnoli
Mr. Daniel Knauf
Mr. Steven Lipner
Ms. Michelle Moldenhauer
Mr. John Sabo

More members were expected to be in attendance; however, an unexpected snowstorm in the East Coast prevented some of the members from traveling.

The entire meeting was open to the public. Ms. Sallie McDonald of the General Services Administration and Board member designate was in attendance. Dr. Fran Nielsen and Chairman Reeder welcomed Ms. McDonald. Paperwork is being processed to officially appoint Ms. McDonald to the Board. Dr. Nielsen reviewed the material in the members' meeting folders. The agenda was reviewed and adjustments were made because some of the briefers were absent or delayed. ***Discussion of the work plan proposal on GPEA by Board Member Rich Guida was deferred until the June 2001 meeting. Board members are to provide comments on the draft to Mr. Guida as soon as possible.***

Chairman Reeder noted that this Board meeting was held in Indianapolis, Indiana because of the National Institute of Standards and Technology (NIST) invitation to the Board to attend the National Information Assurance Partnership Government-Industry IT Security Forum on March 7, 2000.

The Chairman opened the floor for any general announcements from Board members.

Mr. Dan Knauf announced that President Bush had signed his first Presidential decision directive, NSPD#1. The elimination of the Security Policy Board and the requirement for re-justification of some other groups such as the National Security Telecommunications and Information Systems Security Committee (NSTISSC) were part of this directive. Mr. Knauf also stated that the Administration had not reached a decision on the continuation of the Critical Infrastructure Assurance Office (CIAO). The expectation is that Richard Clarke, Special Assistant to the President and National Coordinator for Transnational Threat, National Security Council (NSC), will address this issue. The Board suggested that a letter be prepared to send to Condoleezza

Rice, Assistant to the President for National Security Affairs at the NSC informing her of the direction the Board is taking in the computer security and privacy arena. ***Chairman Reeder is to draft this letter for the Board's consideration at the June meeting.***

Mr. Knauf announced that the National Information System Security Conference effort had been officially disbanded. The cancellation resulted from a mutual decision made between the National Security Agency and NIST. Information about the Spring NSTISSC conference was distributed to the Board members. Mr. Knauf said that they expect attendance to reach 250 and, he encouraged Board members to attend.

Ms. Sallie McDonald, Board member-designate, stated that she is looking forward to working with the Board. Ms. McDonald gave a brief overview of the responsibilities of her position as the Assistant Commissioner for the Office of Information Assurance and Critical Infrastructure Protection in the Federal Technology Service at the General Services Administration.

Board member Michelle Moldenhauer briefed the Board on her activities. These activities included being a member of the Government Information Technology Services (GITS) Federal Public Key Infrastructure Steering Committee and the chairperson of the Federal Policy Authority Group under the Federal Chief Information Office Council. Ms. Moldenhauer said that she would keep the Board informed of these activities.

Board member John Sabo described his involvement in a policy working group trying to develop a project to allow mapping of certification policies in more structured ways. Mr. Sabo said that an IT-ISAC was being established. The plans call for the incorporation of a board of 19 organizations, operational committees and a contracted administrative entity. Mr. Sabo indicated that it would be several months before the IT-SAC is fully operational.

Chairman Franklin Reeder reported that the Center for Internet Security will soon release their first product, a benchmark for Solaris. The announcement is due within a week. The Center also plans to hold their first general membership meeting in May 2001.

Ms. Elaine Frye presented a draft set of web pages for the revision of the Computer System Security and Privacy Advisory Board website for the Board's review and comments. The Board made several recommendations for addition and changes. Ms. Frye will these suggestions in an updated website.

Follow-on Action to Congressman Horn Correspondence

At the December 2000 Board meeting, the Board recommended changes and additions to an earlier draft of a proposed letter to Congressman Horn regarding his issuance of a report on federal agencies' computer security program effectiveness. The letter was amended to include the Board's changes and forwarded to NIST for appropriate clearance. Dr. Nielsen briefed the Board on her meeting with NIST Counsel, Mike Rubin, and his concerns regarding the Horn correspondence. In her meeting with Mr. Rubin, he also expressed some concerns about the recent change of the Board's meeting venues. He was concerned about keeping the meetings open to the public, as well as the cost effectiveness of travel compared to conducting the meetings at the NIST facilities. After discussion among the Board, Chairman Reeder proposed that the Horn letter be sent out as the Board had previously agreed at its December meeting. A meeting will be scheduled among Mr. Rubin and Mr. Ed Roback, Dr. Nielsen and Chairman Reeder so that they may address the issues raised by Mr. Rubin and, Chairman Reeder can express the opinions of the Board in this regard. It was also suggested that Mr. Rubin be invited to a future Board meeting to meet the members and present his views of the Board's responsibilities and authority.

Reorganization of NIST Computer Security Division

Dr. Fran Nielsen, NIST Computer Security Division

Dr. Nielsen's presentation covered the Division's reorganization as well as its plans for Critical Infrastructure Protection research and development, the Computer Security Expert Assist Team (CSEAT) and the Critical Infrastructure Protection grants program. [Ref. #1] As a result of the approval of the FY2001 budget, the Computer Security Division will receive an increase to its budget in the amount of $12M to be used for the three aforementioned programs. The Division CSEAT Program Manager is Ms. Kathy Lyons-Burke [kathy.lyons-burke@nist.gov], and the Division Critical Infrastructure Protection (CIP) Grants Program Manager is Dr. Don Marks [donald.marks@nist.gov].

During the discussion of CSEAT, Mr. Knauf asked what business model the government should be following for its program security reviews for the CSEAT effort. The Board is very interested in the long-term strategy of this program and may want to weigh in on the program security review process. ***Dr. Nielsen is to follow-up on this with Ms. Lyons-Burke.***

Next, Dr. Nielsen briefed on the CIP Grants Program. Infrastructures are generally provided by the private sector and, there is a need to address infrastructure security concerns not cost-effective for industry. The Board recognized the challenges and difficulties of this effort and encouraged NIST to be as agile as possible in working with the public at large. The Board suggested that it would be useful to both the public in general and the proposal submitters, if NIST were to define its priorities early in the process. Dr. Nielsen encouraged the Board to share their comments and observations directly with Mr. Marks.

The third portion of the briefing covered the Computer Security Division reorganization. The Division will be expanded from two groups to four groups: Security Technology Group; Systems and Network Security Group; Security Management and Guidance Group; and the Security Testing and Metrics Group. Dr. Nielsen reviewed the key activities of each of the groups. Board member Charisse Castagnoli offered to work with NIST to get industry support for the business regional security meetings effort.

Board Discussion

At the December Board meeting, Chairman Reeder asked the Board Secretariat to prepare a review of the travel dollars associated with the Board meetings. Dr. Nielsen discussed the data that had been collected. After review of the data, the Board agreed that there was no compelling financial reason to confine all future Board meetings to NIST facilities in Gaithersburg, but noted that any travel should have some valid programmatic purpose.

Discussion of Work Plan on Privacy

Ms. Charisse Castagnoli, Board Member
Mr. John Sabo, Board Member

Board Members Charisse Castagnoli and John Sabo presented their work plans on privacy. Ms. Charisse Castagnoli presented a draft privacy and data protection work plan. The major problems with privacy and data protection are that privacy and data protection are not centralized functions, and, unlike other information technology (IT) functions, privacy and data protection are relatively new, and the responsible individuals have limited resources. The mission of the Board should be to advise the federal agencies on how to leverage disciplines learned from IT to the privacy and data protection problem area. In framing the issue, Ms. Castagnoli said that privacy is a policy issue and that data protection is an implementation issue. One cannot talk about privacy and data protection in a consistent way without methodologies and process support.

Ms. Castagnoli presented the following work plan ideas:

1) identify where the gaps are in effective privacy and data protection policy;
2) identify where and how to effectively fill the gaps;
3) leverage existing work wherever possible; and
4) identify and characterize work that is not being done.

Some first steps that could be taken were identified. They included looking at other privacy frameworks such as the one for the International Security Trust and Privacy Alliance, looking to see if common criteria for privacy and data protection can be built, serve as a technology conduit to bring new technologies to the attention of organizations with implementation responsibilities, and thoroughly review the Privacy Commission Act (HR 583) and offer comments. Reexamination of the original Privacy Act was also suggested. ***George Trubow has the action to develop a suggested procedure for this activity.*** Steve Lipner suggested that initial review of the Act be based on questions such as: is the law adequate; are agencies implementing it; if so, how are they implementing it; and does the law need to be reexamined. The activity should include a review of whether there has been an appropriate shift from paper to the electronic paperless world. Additionally, because the Electronic Communications Privacy Act of 1986 (ECPA) offered no built in exceptions for areas such as critical infrastructure protection, questions arise about other potential notable exceptions and the types of safeguards that a law should contain.

John Sabo also presented his work plan for Board efforts on privacy. Mr. Sabo said that there is the need to build the right sets of policies and that there are political, business and societal issues to be addressed. There are also definitional and structural issues as well. The resolution of these issues involves working to develop constructs, standards and architectures that will enable systems to support a full range of privacy policies transparently, effectively and with trust. He identified some of the reasons why the resolutions of these issues will be difficult; new trust systems are emerging and the scope of privacy issues is expanding, there are consumer advocacies and concerns, there are global privacy drivers and confusion between privacy and security in general. Mr. Sabo suggested that a privacy framework is needed. In networked systems, privacy requirements must be supported across jurisdictional, business and consumer preference boundaries. Privacy regulations and business policies require a disciplined, interoperable set of technical enablers. Mr. Sabo suggested that a tool could be built to understand the business processes and controls needed to meet the full range of privacy requirements. Another tool could be built for developing technical mechanisms needed to support data protection policies and fair information practices in today's e-business world.

The issues presented by Ms. Castagnoli and Mr. Sabo will assist ***the program committee in developing their agenda for the privacy session at the June Board meeting. Members of that group are: Charisse Castagnoli, Rich Guida, Fran Nielsen, John Sabo, George Trubow, and Rick Weingarten.***

Public Participation

There were no requests for public participation at this meeting.

The Chairman recessed the meeting at 4:45 p.m.

Thursday, March 8, 2001

The Chairman resumed the meeting at 9:05 a.m.

Board Discussions

The discussion of the work plan proposals on GPEA and Governance were deferred until the June Board meeting.

On February 13, 2001, U.S. Representative Asa Hutchinson introduced a bill to establish the Commission for the Comprehensive Study of Privacy Protection (H.R. 583). At the current time, the Office of Management and Budget is not taking an active interest in this bill. There was discussion on whether the Board should develop a position on the bill and the value of the establishment of a Privacy Commission. For now, the Board deferred taking any action. The Board will keep track of the bill's progress through Congress.

In general discussion about upcoming legislation, Mr. Knauf stated that when computer security or privacy legislation is proposed that the Board should take a position regardless of any immediate activity or the chances of the legislation passing through Congress. Mr. Knauf noted that privacy issues are becoming more prolific with the Congress and the Board should have a presence and an opinion on legislative actions. The Board decided that the June privacy session might assist them in producing a formal opinion on this issue.

Review of Plans for June Privacy Event

Charisse Castagnoli and John Sabo led the Board in developing an outline for the June privacy event. The purpose of the session is to bring together experts in areas of privacy critical to the national debate on who will define gaps in law, policy and implementation as well as provide recommendations to the Board on positions and solutions. Four issue areas were identified:

1) Managing a plethora of regulations and diverse cross-agency privacy policies within government, e.g. Gramm-Leach-Bliley vis-à-vis Health Information Privacy Protection Act, competing jurisdictions.
2) Managing implementation of privacy policies by government agencies, including process management and information technology systems, e.g., agency operational procedures, architectures, individually identifiable information vs. aggregated information, federal-state-local data flows, and technologies such as "cookies", P3P and wireless.
3) Enforcement and audit challenges within government, e.g., frameworks for privacy audits, appropriate controls, and recourse.
4) Informed public awareness of the seriousness of privacy issues and policy balances necessary to achieve resolution, e.g., economics of privacy.

The expected deliverable is identification of the three most important challenges of each issue that government should address with a suggested national agenda or roadmap to meet these challenges.

The Board identified potential points of contacts who could address these issues and the planning committee will follow-on and work with the NIST secretariat to develop the session agenda.

Board Annual Report

Board Annual Reports have been produced for 1989-1995. ***To bring the reports up to date, Dr. Fran Nielsen volunteered to draft a 5-year report covering 1996-2000 Board activities***. ***An outline will be developed and sent to the Board for their consideration***. The Board discussed the format for future annual reports. They would like to see the focus reflect the six topic areas identified by the Board's 2000 work plan***. Dr. Nielsen will work with Chairman Reeder to develop an appropriate outline.***

Discussion of Work Plan on Security Metrics

Dr. Fran Nielsen, NIST

Dr. Nielsen reported that the intent of the security metrics plan is to promote the advancement of the state-of-the-art of measurement of the security of information systems. To achieve this goal there is a need to identify and/or develop security metrics and measurements of performance. Dr. Nielsen identified the problem as the lack of agreed-upon security metrics and the identification of what security metrics exist. There is a need for collection, clarification, completion, consolidation and communication of potential measures of effective security programs.

The security metrics project is expected to expand the security measurement continuum by helping to identify and define more quantitative measures and to refine the granularity of qualitative measures.

Dr. Nielsen suggested proposed actions and milestone activities that could be endorsed by the Board. These activities included the following:

- Development of a website that could serve as an information resource on security metrics; create project page, identify links to other appropriate sites and review contents for broken links.
- Create and maintain a contact/interest list
- Host the 2nd metrics workshop event in Spring 2002
- Generate issues/topics list for further break-out discussions
- Create taxonomy of models
- Evaluate models
- Write discussion papers
- Encourage user organizations to use and provide feedback on metrics
- Partner with academia to encourage research in security metrics.

Dan Knauf suggested that the website also be used to sponsor specific study topics. Mr. Knauf stated that the partnering with academia was an excellent approach and referred to the NSA's National INFOSEC Education and Training Program effort where over 14 universities have been designated as Centers of Excellence in Information Assurance Education. Other recommendations included working with the Federal CIO Council and user organizations such as SRI I-4.

Discussion of Work Plan on Baseline Standards

Mr. Steven Lipner, Board Member

The objective of the work plan on baseline standards is to identify a set of baseline agency best practices for security. Mr. Lipner stated that to be useful, the focus would be on the baseline security controls that any agency needs and on the low-level processes that are needed to use them effectively. Mr. Lipner proposed that public and private sector best practice practitioners be solicited to share their perspectives and experience with the Board at a workshop. Identification of best practices should be by rating according to the General Accounting Office and/or Congressional committee scorecards [for government] and perhaps by self-nomination of candidates who would then be qualified by an anonymous survey of security consultants from the private sector. Selected presenters would submit papers or documents on their best practices and baseline controls in advance. As a result of this workshop a document could be produced that includes concrete best practices that agencies can read, tailor very slightly and emulate. Mr. Lipner proposed that this workshop be held during the September or December Board meeting. The Board suggested a change in the title of the work plan to eliminate the word "standards" to avoid the appearance of any implied standards development. One suggested title was "minimum accepted practice (MAP)." ***Mr. Lipner volunteered to develop a draft letter from the Board to NIST requesting that NIST assist the Board with this workshop activity***.

Action items from this meeting are listed below.

1. The work plan proposals on GPEA by Board Member Rich Guida and Governance by Board Member Peter Browne were deferred until the June 2001 meeting.

2. The Board suggested that a letter be prepared to send to Condoleezza Rice, Assistant to the President for National Security Affairs at the NSC informing her of the direction the Board is taking in the computer security and privacy arena. Chairman Reeder is to draft this letter for the Board's consideration at the June meeting.

3. The Board is very interested in the long-term strategy of the CSEAT program, and may want to weigh in on the program security review process mechanism. Dr. Nielsen is to follow-up on this with Ms. Lyons-Burke

4. Reexamination of the original Privacy Act was suggested. George Trubow has the action to develop a suggested procedure for how this might be accomplished and circulate it to the Board in advance of the June meeting.

5. The program committee responsible for developing the agenda for the privacy session at the June Board meeting are: Charisse Castagnoli, Rich Guida, Fran Nielsen, John Sabo, George Trubow, and Rick Weingarten.

6. To bring the annual reports up to date, Dr. Fran Nielsen volunteered to draft a 5-year annual report covering 1996-2000 Board activities. She will work with Chairman Reeder to develop an appropriate outline for future annual reports.

7. Mr. Lipner volunteered to develop a draft letter from the Board to NIST requesting that NIST assist the Board with this workshop on baseline security controls.

There being no further business, the meeting was adjourned at 2: 53 p.m.

Ref. 1 Nielsen presentation

Fran Nielsen
Board Secretary

CERTIFIED as a true and accurate
summary of the meeting.

Franklin S. Reeder
Chairman