COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

National Cryptologic Museum
Colony 7 Road
Annapolis Junction, MD

June 11-13, 2002

Tuesday, June 11, 2002

Board Chairman, Franklin S. Reeder, convened the Computer System Security and Privacy Advisory Board (CSSPAB) for its second meeting of the year at 9:05 a.m.

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

Peter Browne
Lynn Bruneau
Charisse Castagnoli
Mary Forte
Richard Guida
Susan Landau
Steven Lipner
Sallie McDonald
Leslie Reis
John Sabo

The entire meeting was open to the public. Over the three days of the meeting, there were 10 members of the public in attendance.

Mr. Dan Wolf, Director of Information Assurance, National Security Agency, welcomed the Board to the NSA facilities. Mr. Wolf noted that the role the Board plays is especially critical since the events of September 11. He wished the Board a successful meeting.

Update on the Security and Privacy Activities of the Computer Science and Telecommunications Board, National Research Council

Marjory Blumental, Executive Director of the Computer Science and Telecommunications Board (CSTB), presented an overview of the activities of the CSTB. **[Ref. #1]** The review included the Board's operating mechanism, what they provide, who their audience is and where their funding comes from. Since 1987, they have issued 70 reports covering categories such as R&D and technology trends, trustworthiness of security and privacy, economic and social impacts of IT, applications of IT, telecommunications and the Internet, and law. Current activities underway are in the trust-related areas on subjects such as critical information infrastructure protection and the law, privacy in the information age, improving cybersecurity research, and science and technology for countering terrorism in IT. Other subject areas include digital archiving and NARA, fundamentals of computer science, IT and creativity, and GIS and information technology.

One of their most recent work projects on security and privacy is the development of a report on cybersecurity today and tomorrow. It compiles understanding, knowledge, findings, and recommendations from more than a decade of CSTB reports.

The CSTB is also undertaking a study on the questions about nationwide identity systems. Dr. Stephen Kent of BBN Technologies is the chair of a 15 member IDs/Auth Study Committee. The report points out that the nationwide identity system debate has been hampered by the lack of a clear description of the goals of such a system. There are many complicated policies and technological issues around such systems and ascertaining desirability and feasibility involves answering numerous complex questions. The report's goal is to catalyze a broad discussion.

Privacy in the Information Age is the most recently launched study effort of the CSTB. This 13 member study committee on this topic is being co-chaired by Lloyd Cutler of Wilmer, Cutler & Pickering and William Webster of Milbank, Tweed, Hadley & McCloy. The broad charge of this activity is to assess threats, opportunities and balances.

The Board suggested that the CSTB might want to consider looking into the areas of the Digital Communications Act, insurance liability, implications of computer privacy and security vulnerabilities to the consumer, and measurement and metrics liabilities.

OMB Update

The scheduled speaker for OMB was unable to attend because of last minute scheduling difficulties.

Computer Security Standards

Mr. Ed Roback, Chief of the NIST Computer Security Division, posed a question to the Board for discussion: should selected Protection Profiles (PP) be made into mandatory Federal Information Processing Standards (FIPS). **[Ref. #2]** Mr. Roback presented an overview of the pros and cons of this effort. Other PP options offered were to develop NIST Special Publications (SPs), develop a subset "NIST Recommendations" series, specify not "mandatory and binding," but often used by auditors, and issuance of OMB guidance to agencies. After discussion, it was the consensus of the Board that NIST not make any PPs into FIPS.

Next, Mr. Roback spoke with the Board about the status of several pieces of legislation in Congress that would specifically affect NIST and the Board's activities. The majority of these activities centered on the reauthorization of the Government Information Security Reform Act (GISRA). Mr. Roback also reported on the status of the emergency budget supplemental package that was submitted earlier in the year and how it had funds earmarked for NIST activities. The Senate had passed a $40M supplemental for cybersecurity efforts at NIST.

Briefing on OPM E-Government and Payroll Initiative

Mr. Norman Enger, e-Government Program Director for the Office of Personnel Management (OPM) presented a brief overview of OPM's E-Government initiative. **[Ref. #3]** This effort supports the President's Management Agenda strategic management of human capital initiative by improving citizen access to federal job openings and other recruitment services, provides employees with one-stop access to training, and increases collaboration and sharing of human resource information between agencies. This initiative also supports homeland security and expanded electronic government.

Next, Ms. Janet Dubbert, OPM's E-Government Payroll Project Manager, briefed the Board on the OPM E-payroll initiative. **[Ref. #4]** OPM's goals for this effort are to consolidate Federal payroll providers with existing systems, standardize payroll policies, modernize payroll systems

as necessary and develop a phased approach to achieve the end state, an integrated HR/Payroll system. Currently there are 18 payroll providers. Four of these payroll providers service 80% of the total Federal civilian payroll. This project has a fast moving timeline, starting in February of 2002 with a request for data call to the beginning of migration of the agencies to the consolidated provider by October 2002. The Board invited Ms. Dubbert to return later in the year to give the Board an update of their progress.

The meeting was recessed at 4 p.m.

Wednesday, June 12, 2002

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

Impact of Digital Millennium Copyright Act on Security Research

Professor Edward Felton, Department of Computer Science, Princeton University presented a briefing to the Board on the Digital Millennium Copyright Act (DMCA) and the effects of regulating computer security. **[Ref. #5]** The DMCA, Section 1201, outlaws circumvention of technology that mediates access to copyrighted material, outlaws trafficking in technologies that are primarily designed or produced for the purpose of circumventing such technology. The limited exceptions are not of much help in practice. Professor Felten reported that the DMCA has been used to muzzle security researchers. He gave three examples: Ferguson's analysis of digital TV crypto, analysis of Microsoft's DRM and Felton's team's research on watermarking. The DMCA has not been used against infringers and the Courts have ruled that DMCA violation can occur without infringement, and tools can violate DMCA even if it cannot possibly be used to infringe. Professor Felten discussed the difficulties that he and his team encountered as a result of their study of four technologies for deployment in next-generation music and players. His conclusions were that the DMCA makes it risky to analyze any technology that is used by somebody, somewhere to mediate access to copyrighted material and apparently outlaws even discussion of flaws in such technologies. Professor Felton advocates that the DMCA adopt a pro-innovation policy that would foster development of new technologies, would foster analysis, especially before deployment and would foster adoption of proven methods. An open process allows debate and education, said Felten.

Board members Rich Guida suggested that the Board consider a position that would be neither for nor against the DMCA but would identify that security research is being chilled and there is a need to look at how the integrity of such research can be achieved. The Board will continue to follow this issue in the coming months.

Board Work Plan Review

The Board reviewed their current work plan topic areas.

- Baseline standards -- Board member Steve Lipner agreed to continue leading the effort on baseline standards. He will produce a draft report on this topic for the Board's consideration at their September meeting. Members Peter Browne and Susan Landau offered to work with Steve on this effort.

- GPEA -- It was suggested that the Board could build a business case for GPEA and the E-government initiatives because of the lack of coverage in the trust area.

- Governance – The question was raised can we have any impact on recommending methods for more efficiency in this area.

- Homeland security effort – The Board needs to be more informed on the proposed department's activities. A suggestion was made to send a letter to Governor Tom Ridge with a copy to Richard Clarke to make them aware of the Board's availability to assist them. Board members Sally McDonald and Leslie Reis volunteered to draft appropriate correspondence for the Board's consideration.

- Security metrics -- The Board decided to defer further activity in this area for now.

Next, the Board took a tour of the NSA Cryptologic Museum.

NSA Information Assurance Education Initiative

Sherry Borror of NSA National Infosec Education and Training Program briefed the Board on their program activities. **[Ref. #6]** Ms. Borror cited several reasons that there are INFOSEC/IA personnel shortfalls. Many security tasked are not being adequately performed due to lack of personnel, training and tools. Critical security responsibilities are assigned to positions as additional duties and, there is a lack of comprehensive, consistent training for ISSOs security engineers, certifiers, and accreditors. A 1994 Office of Technology Assessment report and the President's Commission on Critical Infrastructure Protection both emphasized the need for such education. The NSA responded to this need by establishing the National INFOSEC Education and Training Program (NIETP). The NIETP's mission is to be a leading advocate for improving information system security (INFOSEC) education and training nationwide. Ms. Borror highlighted the NIETP activities related to Presidential Decision Direction (PDD) 63, which established the National Security Telecommunications and Information Systems Security Committee (NSTISSC). This committee has now been re-designated as the Committee on National Security Systems. The NIETP has also established a consortium of over 1000 INFOSEC professionals from government, industry and academia as a consensus building team to determine training needs for IT professionals. The role of academia is emerging with the number of colleges teaching INFOSEC increasing with integrated and stand along courses as well as whole degree programs. The NSA has partnered with academia and created the Centers of Academic Excellence in Information Assurance Education. Over 35 of these Centers of Excellence are in place throughout the United States.

INFOSEC Assessment Methodology Training and Rating Program

Mr. Wilbur Hildebrand, Chief of the INFOSEC Assessment Services at NSA, discussed their defensive information operations, a life cycle approach to improved information technology (IT) security health. The services of this operation include awareness, assessment, attack and solutions and performance of vulnerability discovery objectives. Their customers are organizations within the DOD, DOD contractors and civilian agencies whose systems having national security implications. Mr. Hildebrand said that one of the problems that NSA is facing is limited resources and authority to perform INFOSEC assessments for all the customers who need them. NSA is attempting to solve this problem by entering into partnerships with others outside of NSA.

Next, Mr. Hildebrand described NSA's INFOSEC Assessment Training and Rating Program (IATRP). The assessment is done in a three-phase approach: (1) pre-assessment; (2) assessment; and, (3) post assessment. The assessment methodologies cover 18 baseline INFOSEC categories that include documentation, identification and authentication, telecommunication, personnel security and virus protection. The IATRP also offers a two-day INFOSEC Assessment Methodology Training and Instruction and Group Exercises program.

The meeting was recessed at 4:00 p.m.

Thursday, June 13, 2002

Chairman Reeder reconvened the meeting at 8:35 a.m. He extended the Board's thanks to Elaine Frye, Tanya Brewer-Joneas, and Fran Nielsen for their efforts and assistance with this meeting. Mr. Reeder also thanked Board Member Mary Forte for NSA's hospitality in hosting the meeting at the Cryptologic Museum.

Panel on Baseline Standard Practices

Board Member Peter Browne opened a session on review of agencies' baseline standards practices. Mr. Browne presented a brief overview of the prior baseline standards work that the Board had reviewed.

- **IG Community Perspective**

The first panelist to speak was Mr. Russell Rau, Assistant Inspector General for Audits with the Federal Deposit Insurance Corporation. **[Ref. #7]** His presentation covered information security risks, statutory framework, program level security standards, information security program assessment matrix, information security program assessment matrix, system level security standards, and information systems assessment matrix. Mr. Rau said that there were lessons learned complying with GISRA. These included a focus on partnership with the Chief Information Officer, business operations and development of OIG capabilities. He expressed his concern to be aware of the proliferation of guidance documents and the overlapping review requirements that impact on CIO resources and operations.

Rebecca Lang, Office of the Inspector General, Department of Transportation, was the next briefer. **[Ref. #8]** Her comments focused on the Department of Transportation review as a result of the Government Information Security Reform Act. They reported their computer security program as a material weakness with a pledge from the Secretary of Transportation to remediate these identified computer security weaknesses in their FY03 performance plan. Ms. Lang said that OMB identified the lack of senior management attention as one of the common security weaknesses found across agencies. Agencies must be able to communicate to senior management if they want to succeed in computer security management. They also need guidance to help them with their resource needs. Generally, agencies don't know how to assess how much it will cost to secure their systems. Ms. Lang suggested that the Board encourage NIST to develop such guidance. In summary, Lang said that much remains to be done in securing government computer systems and OMB and NIST need to continue to provide the critical leadership.

Mr. John Lainhart, former Inspector General for the U.S. House of Representatives, and now a consultant with Price, Waterhouse and Cooper, briefed the Board on information assurance issues. **[Ref. #9]** An information assurance program should include an assessment and diagnostic service, management services, architecture services, implementation services, incident investigation and assurance services. Mr. Lainhart described a program called COBIT™, control objectives for information and related technology. Topics covered included an IT control framework, management guidelines developed through the use of maturity models, critical success factors, key goal indictors and key performance factors. Lainhart also reviewed a program called SysTrust℠, a systems reliability assurance service used by the American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants. This program is used to manage internal risk and third party risk. It is a benchmark on controls and an opportunity to identify control weaknesses. The International Federation of Accountants uses a

international information technology guideline for managing security of information. The core principles of this guideline are accountability, awareness, multidisciplinary, cost effectiveness, integration, reassessment, timeliness, and societal factors. Mr. Lainhart also covered the activities of the Center for Internet Security. The Center is developing best practice benchmarks that define the specific technical settings that will provide increased security for Internet-connected systems; a security ruler that defines which of those specific settings will increase the relative security of systems; and, automated tools to continuously monitor the security status of systems.

- **Good Examples**

Session coordinator, Board Member Peter Browne, reviewed a series of questions that had been posed to the two invited agencies who briefed the Board. These questions were:

(1) How is the Agency IA program organized, staffed and structured?
(2) What is the budget and what is the percentage of overall IT spending?
(3) How would you rate the Agency's IT security/information assurance program? Why?
(4) What are YOUR tops three "best practices"?
(5) Do you operate under the concept of "baseline standards"? What are they?
(6) How is security measured? What are the key performance indicators {kpi's)? What other metrics do you use?

The Board heard first from Dr. David Nelson, Deputy Director of the National Aeronautics and Space Administration (NASA), who presented NASA's perspective on baseline standards. Dr. Nelson reported that over the past several years, NASA has been working in a labor-intensive reactive mood. Security is integral to carrying out the agency mission program. NASA does verification and validation of software. Dr. Nelson's view is that minimum standards implies that one size fits all however difficult that may be to do. He believes that NASA needs the following to meet their minimum baseline standards goals:

- security training [user awareness, manager training, system administrator training]
- security policy and plans
- system administration
- intrusion detection and response, and
- performance measures.

Next, Mr. James Wade, Vice President of Information Technology Planning and Standards for the Federal Reserve briefed the Board on his agency's activities. **[Ref. #10]** Twelve independent reserve banks form the Federal Reserve System. It includes a Federal Reserve Board of Governors. The Federal Reserve operates under a risk-based security initiative. Their new information security policy framework covers the principles and practices for standards as they move toward a business-based risk environment. Mr. Wade's briefing also included discussion of a new security architecture and description of their information security risk management model.

Following these two briefings, the Board members held a question and answer session. On the question of communications security, Dr. Nelson responded that the Department of Transportation and the National Security Agency operated within totally isolated communications networks and pointed out that denial of service attacks are the most common problem for communications.

Rebecca Lang noted that a good start toward a common theme for standards was already underway through the efforts of Office of Management and Budget's Committee on Executive Branch Information System Security.

Dr. Nelson said a collection of standards is what NASA is focusing on and Dr. Nelson indicated that NASA would be willing to assist the National Institute of Standards and Technology with the standards development work.

It was noted by Russell Rau, that former Federal Reserve Chairman, Paul Volcker, had noted that the government has lost sight of its principles when developing and setting standards.

The session concluded with the Board's thanks for the input the participants provided on the baseline standards topic.

Board Discussion Session

As a follow-up up to baseline standards topic, the Board discussed several options for consideration. The Board should prepare a report that contains the Board's on its findings and recommendation. Examples of excellence have been presented. The report should include experiences of small agencies. A draft outline of this report to be prepared by Board members Steve Lipner, Peter Browne and Lynn Bruneau, should be ready for discussion at the September 2002 meeting of the Board.

The draft privacy paper will be issued as an exposure draft and made available for public comment for a 30-60 day period prior to the September meeting of the Board. All comments will be considered and a final exposure draft will be issued and discussed at the September meeting.

Having been presented with one point of view on the Digital Communications Millennium Act, the Board would like to have other points of view presented. Board Members Susan Landau and Rich Guida are to develop a draft posture paper to address the leading questions the Board believes most effect the computer security research community. Members were asked to identify those on the technology side of this issue as potential invitees. This topic will be added to the agenda for the September meeting.

The Board reviewed the other action items from this meeting to be included on the September 2002 meeting agenda. They agreed to revise the dates of the September meeting from September 10, 11 and 12, 2002, to September 17, 18 and 19, 2002, to avoid any potential conflicts associated with commemorating the attacks of September 11, 2001.

Board member Sallie McDonald invited the Board to hold its September meeting at the General Services Administration facilities in Washington, DC.

Public Participation Period

There were no requests for public participation at this meeting.

There being no further business, the meeting was adjourned at 1:40 p.m.

Ref. 1 - Marjory Blumenthal's handouts
Ref. 2 - Ed Roback's handouts
Ref. 3 - Norman Enger's handouts
Ref. 4 - Janet Dubbert's presentation
Ref. 5 - Ed Felten's handouts
Ref. 6 - Sherry Borror's handouts
Ref. 7 - Russell Rau's handouts
Ref. 8 - Rebecca Lang's handouts
Ref. 9 - John Lainhart's handouts
Ref. 10 - James Wade's handouts

`

/s/

Fran Nielsen
Board Secretary

CERTIFIED as a true and accurate summary of the meeting.

/s/

Franklin S. Reeder
Chairman