COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

General Services Administration
7th & D Streets, SW
Room 5700
Washington, DC

March 5-7, 2002

Tuesday, March 5, 2002

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

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

Mr. Peter Browne
Ms. Lynn Bruneau
Ms. Mary Forte
Mr. Richard Guida
Ms. Susan Landau
Mr. Steven Lipner
Ms. Sallie McDonald
Mr. Michelle Moldenhauer
Dr. Leslie Reis
Mr. John Sabo

The entire meeting was open to the public. Over the three days of the meeting, there were 12 members of the public in attendance.

Discussion of Privacy Event Summary and Findings/Recommendations

Mr. John Sabo, Board Member, led the discussion of this topic. Board Member Charisse Castagnoli joined the discussion via teleconference.

Mr. Sabo's discussion began with a short review of the June 2001 privacy event that was held at the John Marshall School of Law in Chicago, Illinois during the meeting of the Board. The Board's focus at this privacy event was on two specific privacy issues: (1) Government privacy policies --are Government privacy policies adequate in light of technological, societal and other policy changes and influences, and (2) Government privacy management – can improvements be made to Government's ability to effectively manage systems supporting privacy rules and policies. These sessions raised a number of issues.

- Terminology and definition – most privacy discussions do not start from the same definition base;
- Review of the Privacy Act over a multi-year time period with recommended changes as needed;

- Adjustments for technological changes;
- Identification of data ownership;
- Linkage to CIOs on data privacy;
- A need for organizational authority and management;
- Leadership; and,
- Cross-Government vehicle for privacy communication and coordination.

Next, the Board members reviewed the draft paper prepared by Mr. Sabo that contained proposed Board recommendations. These recommendations included:

1. Documenting and strengthening privacy management practices across the federal Government. The Board also offered several methods that could be used to accomplish these tasks.
2. Performing an examination of national systems of records and databases, public-private sector data disclosures, data matching systems, data exchange agreements and systems, and data linkages in order to develop a complete inventory of systems that contain or process information considered private under one or more statutes, and to develop risk management assessments and provide recommendations on changes needed to the Privacy Act and other statutes and agency regulations to eliminate conflicts and improve agency adherence to such requirements.
3. Implementing an ongoing mechanism to keep abreast of and evaluate emerging private sector policies, technologies, risk management models, and operational systems and practices to evaluate their value to and impact on the Government, and to employ them as appropriate.
4. Creating mechanisms to ensure that those Government officials responsible for the protection of private information understand and can accommodate, to the extent permitted by the statute and regulation, the needs for data sharing and data matching of law enforcement agencies seeking to enhance homeland security.

Chairman Reeder invited public participants in attendance to share their opinions on these privacy issues with the Board.

The first public participant to speak was Mr. Bob Gellman, a privacy consultant with 25 years experience in the privacy arena. Mr. Gellman stated that privacy in Government goes well beyond the Privacy Act. He found the Board's Recommendation #1 was one that had not be tried before and, he thought it was an interesting exercise. Mr. Gellman also acknowledged the varied functions of Government privacy officers from one agency to another. An inside/outside approach for sharing among privacy officers can be difficult. The trend he has found is that agencies seldom share information on the outside. He feels that there is not enough outside input, influence, or discussion on what the Government is doing on any level.

Mr. Gellman said that the Privacy Act is not the end all or be all of what Government needs. It is out of date and needs to be rethought and redone. However, he stated that this isn't likely to happen, and it wouldn't make a difference even if the Act was revised.

The next public participant was Mr. John Fanning, Office of the Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services. Mr. Fanning serves as the Chair of the HHS Privacy Committee whose goal is to ensure attention to privacy as a fundamental consideration in collection and use of personally identifiable information. Mr. Fanning stated that the Government would not be establishing a Privacy Commission. He concurred with the Board's recommendation regarding the examination of national systems and databases.

Mr. Al Stapleton of the General Accounting Office (GAO) was the next participant. He announced that the GAO was currently conducting a study for Senator Joseph Lieberman and Representative Steve Horn on privacy in the Executive Branch. The study will examine agency

compliance, adequacy of the Act, and what personal information is being collected outside of the Act. Later this month, the GAO will send a questionnaire on the Privacy Act to 25 departments and agencies. Results of this questionnaire are expected to be available later this fall. An executive guide for federal agencies on how to protect the privacy of agencies is being considered by the GAO. Mr. Stapleton indicated that GAO would be interested in the Board's thoughts on identifying principles and practices. Another report being done is in the area of privacy principles and strategies around the world and how they apply to the Federal government. That report should be available in the near future. A report on the data mapping issue is also underway. This study is being done to identify where is the Social Security Number is used within the Government.

Regional Information Security Workshops Program

Ms. Alicia Clay of the Computer Security Division at NIST briefed the Board on the regional information security workshops program **[Ref. #1]** Her presentation covered :

- goals of the regional security meetings;
- who should attend;
- what small businesses will learn;
- three common threats;
- potential consequences;
- why small businesses;
- sample meeting agenda;
- when and where; and
- next steps.

These meetings are being targeted to groups of no more than 100.

The Board members offered Ms. Clay input on how to strengthen the outreach effort of the program. It was suggested that she contact the Federal Trade Commission as they have plans to host a two-day public workshop in May to explore issues related to the security of consumers' computers and the personal information stored in them or in company databases. Board Member, Professor Leslie Reis, also expressed interest in working with Ms. Clay to host a possible workshop in conjunction with the John Marshall Law School for the local lawyer community in Chicago, Illinois.

Next on the agenda was an opportunity for public participation. There were no request for such participation, and the Board turned their attention to further review of the privacy findings and recommendations draft.

There was also a brief review of the status of current draft legislations in Congress regarding the reauthorization of the Government Information Security Reform Act and a brief review of the status the U.S. government's efforts regarding OECD's security guidelines.

The meeting was recessed at 3 p.m.

Wednesday, March 06, 2002

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

E-Authentication - An Update

Mr. Steven Timchak of the General Services Administration presented a briefing on the President's Management Agenda E-Gov Initiative on E-authentication. **[Ref. #2]** Mr. Timchak reported that this effort is in its beginning stages. Its mission is to ensure public trust in the security of information exchanged over the Internet. The goals are to build and enable mutual trust needed to support wide spread use of electronic interactions between the public and Government, and across Government; to minimize the burden on the public when obtaining trusted electronic services from the Government, and across Governments; and, to deliver common interoperable authentication solutions, ensuring they are an appropriate match for the levels of risk and business needs of each e-Government initiative. Mr. Timchak described the objective and plan of action they support to accomplish these objectives. The challenges to the success of this effort include the fostering of collaboration, the pace of technological change and user acceptance. The Board invited Mr. Timchak to brief them in the future as the project progresses.

FedCIRC - An Update

Ms. Sallie McDonald, Board Member and Assistant Commissioner, Office of Information Assurance and Critical Infrastructure Protection, gave the Board an update on the activities of the Federal Computer Incident Response Center [FedCIRC], which is the Federal government's central focal point for computer incident recognition, reporting, handling and prevention. **[Ref. #3]** FedCIRC initiatives include cyber warning information network, security collaboration capability, patch dissemination capability, security tool kit, data analysis capability and outreach activities. Ms. McDonald said that they are setting up a series of meeting with agency Chief Information Officers and below. The briefing will include a presentation on what and how to report an incident. It is anticipated that GSA will brief more than 20 agencies over the next several months.

Ms. McDonald also commented that Gov-Net had completed their review of the over 160 comments they received and were arranging to meet with Dick Clark on this issue.

Following Ms. McDonald's presentation, Mr. Steven Lipner, Board Member, presented a brief synopsis of the Simple Network Management Protocol (SNMP) issue of buffer overruns and the concerns of a potential threat to the Internet.

Freedom of Information Act vs. Critical Infrastructure Information -- Public Interest Community Viewpoint

Mr. David Sobel, General Counsel, Electronic Privacy Information Center (EPIC) presented a general overview of the public's viewpoint on critical infrastructure information. He reviewed the background of the Clinton Administration's concern about privacy of data collected by federal agencies and the use of such, vis a vis the Freedom of Information Act. Legislation first proposed by Congressmen Davis and Moran did not pass. However, it did draw attention to the issue. Senator. Bennett's draft legislation is now working its way forward. Mr. Sobel stated that the legislation might move forward attached to other legislation without hearings being held. The question at the center of concern is whether it is reasonable to assume that any reasonable collected information may be subject to disclosure under the Freedom of Information Action (FOIA). Case law states that no information collected by a federal establishment is subject to FOIA request if the provider of that information does not wish the information released.

Mr. Sobel said that EPIC has been dealing with this issue for over one and one-half years. No one on the Hill or in the Administration could provide examples of types of information that the public would want to be shared. The public not only expressed FOIA concerns but liability concerns as well. The National Security Telecommunications Advisory Committee (NSTAC) has weighed in with the Administration on this issue. Mr. Daniel Burnham, an NSTAC Committee

member, wrote to President Bush to say that NSTAC believes legislation needs to be in place to address the FOIA and liability concerns.

The industry position is that there are things that they want to share with the Government that are not protected. But if the Government thinks the information should be protected, please identify it.

Board Member Michelle Moldenhauer of Treasury cited examples in the banking industry regarding the sharing of vulnerabilities of the banks with Treasury where sharing has not happened. The banking industry still has questions regarding the Government's need and use of such information. Treasury has established a small group to create a secure network at the classified level so that sharing of some of this information can be accomplished. However, sharing of information is weak. A serious missing link is that there is no explanation has been given as to what the benefit is to the private sector for sharing such information with the Government.

Chairman Reeder reported that the National Research Council (NRC) was working on a report on law and critical infrastructure protection and it was due to be released soon. The Board would like to hear from NRC about this and will have the Secretariat contact Marjory Blumenthal of the Computer Science and Telecommunications Board to arrange a briefing for the Board once the report is final.

Board member Michelle Moldenhauer asked what information is being collected via the Information Sharing and Analysis Center (ISAC). While Mr. Sobel reported that there didn't appear to be must output from the ISAC community, Board member Peter Browne indicated that the Government does get anonymous information from the financial ISACs and that energy ISACs also appear to be forwarding information.

Mr. Sobel encouraged the Board to get involved. EPIC has spoken to people drafting legislation, industry representatives, White House staff and the President's Commission Critical Information Protection Board on this issue. Mr. Sobol reported that Richard Clark has said that he would support a very narrow FOIA exemption He also said that the Federal Energy Regulatory Commission has issued an official notice of query for formal rulemaking in the Federal Register.

Mr. Sobel thanked that Board for their efforts in this debate and encouraged them to maintain their focus on privacy issues.

The Need for an Academic Discipline of Network Security Policy and Management

Mr. Jeffery Hunker, Dean of the H. John Heinz III School of Public Policy and Management at Carnegie Mellon University, addressed the Board on the need for network security policy and management academic studies.

Mr. Hunker presented some background on the activities of the Heinz School. The School is recognized across the country as one of the best schools of public affairs in the nation. The school has been ranked #1 in Information Technology and #3 in Criminal Justice Policy and Management. The faculty is made up of researchers in the areas of operations research, science computer science, economics, psychology and sociology. The School tries to work on the integration of policy and management. Crime and violence researchers make up a large part of the population. The School was also part of a national consortium on violence research funded by the NRC. The consortium consists of approximately 60 researchers representing more than 40 universities.

Dr. Hunker stated that Heinz will soon announce a master program in information security. It will be a joint effort between the School of Computer Engineering and the School of Public Policy and Management. It will be the first technically rigorous masters degree program that will have a policy management track. It is expected to be three-semester program. The curriculum will begin with a common core between the students taking the security engineering/technology track and policy management track followed by a technical core, network management, distributed operating system, and programming language. Next, students will have a choice of electives leaning toward either a more management or engineering side. Management emphasis will be on development of security policy and issues of network risk management. The audiences they are targeting are those with technical backgrounds and several years working experience. The first program is scheduled to begin in September 2002. Dr. Hunker would like the Board's guidance on how to best shape this program to meet the needs of the federal agencies and for outreach to minorities. The Heinz School has a large service scholarship program that Dr. Hunker hopes will be utilized.

Dr. Hunker reviewed the paper **[Ref. #4]** that described the need for an academic discipline of network security policy and management. It covered examples of security policy/management problems and creating the research community around network security policy and management. The paper provided descriptions of activities supplemental to distribution of research grant.

Chairman Reeder asked what this Board could do to enhance this effort. Dr. Hunker responded that he would welcome the Board's assistance in refining and sharpening the content of the consortium, and, if the Board felt that this effort was a good one, they could express their support of it to those that the Board reports to. The Board could make the recommendations that there be some effort put forth to make this consortium a reality. Chairman Reeder suggested that the Board could also help define the research agenda.

Dr. Hunker can be reached at jhunker@andrew.cmu.edu and 412/268-2159

The meeting was recessed at 4:35 p.m.

Thursday, March 07, 2002

The Chairman reconvened the meeting at 9:10 a.m.

Baselines Standards Discussion

Dr. David Nelson, Deputy Chief Information Officer of the National Aeronautic and Space Administration (NASA) and Mr. Alan Paller of the SANS Institute were next on the agenda to discuss baseline standards issues.

Dr. Nelson presented a review of NASA's performance-based IT security effort. **[Ref. #5]** NASA does run a vulnerability and scanning program every month. They send a report to management and require clean up of the identified programs or they are taken off the system. Dr. Nelson said that NASA doesn't tolerant systems that drop below a certain standard level.

NASA requires security plans of every new system beginning in the developmental stages of planning. They provide templates and training on how to prepare security plans. They are also planning to implement an automated tool in the very near future.

It was noted that NASA has a robust security program with 5% of their budget allotted to computer security efforts. Dr. Nelson indicated that there is always a use for additional funds, but

that NASA was doing quite well. He said that NASA believes in training as the number one priority.

Dr. Nelson shared his viewpoints with regard to the baseline standard issue. He believes that there are specific things that all agencies should do and these things are cloneable. All users should have training and security plans. Law requires these. Also it is known that there are vulnerabilities on machines. Users should have knowledge of what is going on in the intrusion detection area. Dr. Nelson agrees that more effort is needed to support a minimum set of metrics. He recommended that the Board work with agencies Inspectors General (IG) to develop a set of minimum metrics that should be followed and also assist the IGs to develop a mechanism for monitoring the effort within their agencies. Mr. Alan Paller added that in conversations with various agencies IGs, the IGs want the Office of Management and Budget to define the baseline standards and let the IGs test the standards against what has been defined.

The Board will plan to engage the audit community and IG's at their next meeting. The Board will also plan to develop an exposure draft on this topic similar to Privacy issue paper just completed.

Mr. Paller presented an overview the SANS Institute Internet Storm Center. In 2001, the Institute created Incidents.org, a virtual organization of advanced intrusion detection analysts, forensic experts and incident handlers from across the globe. The organization's mission is to provide real time "threat-drive" security intelligence and support to organizations and individuals. The Storm Center, the tool used by Incidents.org, employs advanced data correlation and visualization techniques to analyze data collected from more than 3,000 firewalls and intrusion detection systems in over sixty countries.

Mr. Paller suggested that the Board look at the current legislation [HR 3844, HR 3394, S. 1900, S. 1901, S. 803, etc.] to see if they contain any operational work and if they are backed financially. Mr. Paller also suggested that some of the Board members could contact the Information Technology Association of America (ITAA) and express their concern of the ITAA's viewpoint.

Chairman Reeder also reminded the Board of the Federal Trade Commission notice on an upcoming public workshop on Consumer Information Security and the opportunity for any of the Board members to participate.

Board Member Rich Guida noted that he has discovered that when security professionals are actively employed in operational modes of the program there is less conflict. He suggested that there should be a way to emphasize having the people interwoven from both sides.

The education, outreach and training of lawyer/auditors to educate them in the technical ways would be useful, suggested Board member Leslie Reis. Mr. Paller suggested using methods such as webcasts to draw larger interest rather than spending a lot of time conducting classes that would likely be attended by few.

Board Discussion Time

Discussion began with a review of the Privacy exposure draft. The December Board meeting minutes will be revised to include a more substantive section of the Board recommendations on the privacy issue paper.

Board Member John Sabo will take the Board's comments and provide an edited version of the draft to the members within one week. A motion was made by Board member Lynn Bruneau, and seconded by Board member Rich Guida that the Board approve the release of an exposure draft in substance subject to review for editorial suggestions only. There were no objections and the motion passed.

Next, the Board reviewed a copy of a draft transmittal letter to Secretary of Commerce. A motion was made by Board Member Lynn Bruneau and seconded by Board Member Susan Landau, to transmit the exposure draft and letter to the SOC as a courtesy. There were no objections and the motion passed.

The minutes of the December 2001 Board meeting were approved as amended.

OMB Updates

Mr. Norman Lorentz, recently appointed OMB Federal Chief Technology Officer and Mr. Dan Chenok and Ms. Kamela White of the Office of Regulatory Affairs at OMB were next to address the Board.

Dan Chenok reported that OMB is still focused on the e-Government initiative and computer security and privacy are a major element of that function. Two components OMB will be looking at are: how the agency is doing and how agencies' capital planning incorporates security needs both current and for the future. Mr. Chenok provided a brief review of activities of Project Matrix and the Government Information Security Reform Act report. He said that computer security and privacy are issues that can impede the success of e-Government and that multi-faceted strategies are needed to address the issues.

Mr. Chenok introduced Mr. Lorentz. Mr. Lorentz was named OMB Chief Technology Officer in January 2002. In this position, Mr. Lorentz is responsible for identifying and coordinating the technology supporting the 24 e-Government initiatives and the technology needs of the Office of Homeland Security. Mr. Lorentz was formerly the Chief Information Technology Officer with the U.S. Postal Service. He described himself as a pragmatic technology person.

Mr. Lorentz briefed the Board on the activities of the 24 e-Government initiatives. Ms. Debra Stouffe, a detailee from the Department of Housing and Urban Affairs, will be working on architecture development for cross cutting technologies. The CIO council architecture framework document is also being updated to make it operational.

In the area of privacy issues, Mr. Chenok said that P3P is a preferred standard for insuring machine-readable privacy. Agencies are moving toward it and commercial sectors are adopting it. OMB will be reviewing the Liberty Alliance approach to insure that the citizen's privacy is protected. The focus will be on the requirements of the citizen stated Mr.Lorentz.

Ms. White briefed the Board on the GISRA report. Six common Government-wide security weaknesses were identified. An increase in security funding did not necessarily equate to better security practices. Chairman Reeder brought up a question of consistency of numbers problem. Ms. White responded that the FY02 budget was the first that they received security cost for the GISRA report. She indicated that OMB Circular A-11 guidance will be coming out later this year to give agencies more directions in reporting their budget numbers.

The President's Executive Order for Critical Infrastructure Protection called for the establishment of an OMB Executive Branch Information Systems Security Committee, reported Ms. White. This effort is in the working stages and will include representatives from across the Government working on computer security. The first meeting of the Committee is planned for early April.

Reeder mentioned the Board's activity on baseline standards metrics and the fact that members of the Board will want to meet with staff of OMB to dialogue with them on this issue. He also suggested that OMB discourage agency-to-agency comparisons by individual agencies.

OMB would welcome receiving information on Board's privacy issue.

Mr. Chenok said that the security coordinator of the CIO Council is Ron Miller of FEMA. Mr. Miller will also be a member of the new OMB Executive committee.

Mr. Reeder stated that the Board felt there should be money allotted for the national awareness campaign and, that they plan to carry forth this message in conversation with GSA, FTC and other entities working on this project.

Mr. Reeder thanks the OMB representatives for their informative briefing and their time to address the Board.

Discussion of Agenda for June 2002 Meeting

The Board reviewed the action items from this meeting to be included on the June 2002 meeting agenda. The meeting will be held on June 11, 12 and 13, 2002 and hosted by the National Security Agency at their National Cryptologic Museum.

There being no further business, the meeting was adjourned at 3:05 p.m.

Ref. 1 – Alicia Clay's presentation
Ref. 2 – Steven Timchak's presentation
Ref. 3 – Sallie McDonald's handout
Ref. 4 – Jeffery Hunker's handout
Ref. 5 – David Nelson's presentation

Fran Nielsen
Board Secretary

CERTIFIED as a true and accurate summary of the meeting.

Franklin S. Reeder
Chairman