COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

National Institute of Standards and Technology
Administration Building, Lecture Room B
Gaithersburg, MD

December 4-6, 2001

Tuesday, December 4, 2001

Board Chairman, Franklin S. Reeder, convened the Computer System Security and Privacy Advisory Board (CSSPAB) meeting for its third meeting of the year at 9:15 a.m. While the Board normally meets four times a year, the September 11-13 meeting of the Board was canceled because of the September 11 attacks on the United States.

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

Ms. Charisse Castagnoli
Ms. Mary Forte
Mr. Richard Guida
Mr. Steven Lipner
Ms. Sallie McDonald
Mr. Michelle Moldenhauer
Mr. John Sabo
Mr. Jim Wade

The entire meeting was open to the public. There were seven members of the public in attendance. Members-designate Marilyn Bruneau and Leslie Reis were also in attendance.

Office of Management and Budget Computer Security Updates

Chairman Reeder welcomed Kamela White, policy analyst in the Office of Information and Regulatory Affairs at the Office of Management and Budget (OMB). Ms. White presented an update on the recent computer security related activities at OMB. She said that Mr. Mark Forman, Associate Director for Management and E-government, had initiated an interagency task force on e-government. The task force collected and reviewed all agencies e-government initiatives. From this, OMB condensed the listing to approximately 20 initiatives for funding consideration.

Ms. White reported on OMB's role as a result of two new Executive Orders: one on homeland security and the other on critical infrastructure protection in the information age. OMB is a member of a number of new committee as a result of these actions. One of their responsibilities is to identify items in the budget affecting homeland security. The new Critical Infrastructure Protection Executive Order created the President's Critical Infrastructure Protection Board. It is chaired by Richard Clark and staffed by the National Security Council. The first meeting of the Board has been held. Ms. White reported that the Board is currently in a developing stage. Additionally, the Executive Order established the Executive Branch Information Systems Security Committee, a standing committee to be chaired by OMB.

Ms. White reported on OMB's request to agencies for their computer security plans of action and milestones. The submissions that were received in October looked good. From these reports

OMB has also been able to identify cross cutting issues that may be applicable to other agencies. Agency Inspectors General are interested in the input that OMB receives and will be working with the agencies on their plans of action and correction plans. OMB will require quarterly updates of these plans by the agencies throughout the year. The Board expressed their interest in seeing copies of the quarterly updates when they become available.

It was noted that funding for security was a large part of the budget pass back request this year. The Director of OMB will be sending a letter to heads of agencies listing OMB's security concerns.

Ms. White said that OMB is in the process of drafting FY2002 guidance on reporting on Computer Security Act requirements.

Other recent developments included the reorganization of the Chief Information Officers (CIO) Council. The Council now consists of three standing committees; best practices, education and workforce and enterprise architecture. It was decided that rather than have a separate, distinct committee on security, there would be a security coordinator in each of the three standing committees as well as one person who would report to the Executive Board of the CIO Council.

The Board expressed their concern regarding the implications of the elimination of the CIO Council Security, Privacy and Critical Infrastructure Committee. Ms. White indicated that the recently established Executive Branch Information Systems Security Committee plans to expand on the activities once performed by that CIO committee.

Ms. White announced that Eva Kleederman had been appointed the OMB privacy contact. Ms. Kleederman will be invited to brief the Board at their March 2002 meeting. Ms. White indicated that the Administration is very high on the privacy issue and that the homeland security people are especially aware of privacy concerns.

The Gov-net program is making progress. Board member Sallie McDonald reported that over 161 pieces of information had been received in response to the GSA's Request-for-Information (RFI) solicitation. An interagency evaluation group is reviewing the input and will forward their recommendations to Richard Clark by the end of January.

Board member Richard Guida asked if the Board could speak with the reviewers of e-gov business plans and present them with questions and/or directions that the reviewers may want to consider in accomplishing their tasks. Board member Sallie McDonald also suggested that the Board may want to meet with the managing partners to discuss some of the things that they may want to consider when they prepare their business cases. Ms. White recommended that the Board talk with Dan Chenok and Jonathan Womer about these suggestions.

Privacy Initiative Update

Board Members Charisse Castagnoli and John Sabo produced a draft summary of the privacy event that the Board held in Chicago, IL in June 2001. They reported that several general themes emerged: the state of privacy and auditing in the private sector; the need for a way to summarize agencies work efforts on privacy issues and a method to harmonize these efforts; and, the focus of government on compliance and the focus of the private sector on minimum requirements and the possibility of the private sector information being gathered in some type of report format for agencies to be able to know what is available from outside the government.

The Board plans to formalize its findings and prepare a recommendation to the Secretary of Commerce and the Director of NIST as well as make the report available to the public via the Board website. Board members Ms. Castagnoli and Mr. Sabo will continue to refine the report and present their results at the March 2002 meeting of the Board.

It was also reported that Chairman Reeder and Board member Sabo had met with privacy officers from the Internal Revenue Service, the United States Postal Service, the Department of Health and Human Services, Social Security Administration, and the Department of Defense to discuss privacy related issues. Chairman Reeder proposed that the Board take a position on policy coordination and/or information sharing of privacy issues. He volunteered to develop some draft language for the Board's consideration and discussion at the March 2002 meeting.

It was also pointed out that the current legal framework of the Privacy Act does not deal with individual's privacy issues even in practical ways. The Board will develop a recommendation that addresses this omission. A list of action items will be identified for discussion at the March 2002 meeting.

Board Discussion on Issues Identified during 10/04/01 Board Teleconference

Chairman Reeder led a discussion of the issues that were discussed in a teleconference among the Board members following the World Trade/Pentagon tragedies and the breakdown of telecommunications infrastructures. Emergency broadcast systems-like problems, continuity of operations and critical infrastructure protection were several problem areas that the Board could take a position on. Board member John Sabo stated that the Board might want to focus on the user community's reliance on government Internet and emails for communications during times of disaster. The Federal Trade Commission has already begun to focus on consumer security awareness.

Board member Sallie McDonald reported that there was a 50-member education awareness team that had started to meet to discuss a campaign for public awareness. This effort, however, had to be scaled back because of lack of funding. It was anticipated that Richard Clark would address this issue in his new role on the Critical Infrastructure Protection Board. Ms. McDonald also mentioned that America Online was working with Time-Warner on the education awareness effort for the public. After discussion, the Board decided to draft a letter of support for funding of this government education awareness initiative to be sent to the Secretary of Commerce.

Ethics Briefing

Carol Allen, Office of the General Counsel, Department of Commerce, presented a summary of ethics rules for special government employees. Members of the Board, other than Federal government employees, are considered to be special government employees and are subject to the regulations of such. She discussed the procedures for filing financial disclosure reports annually and the justifications for requesting waivers.

The Importance of a Security Awareness, Training and Education Program

Louis Numkin, computer security manager with the Nuclear Regulatory Commission, presented a slide show to the Board members on the tools and techniques that he uses to help educate the federal and the non-federal community on security awareness issues and techniques.

There were no public participation requests.

The meeting was recessed for the day at 4:45 p.m.

Wednesday, December 5, 2001

Chairman Reeder resumed the meeting at 9:05 a.m. Dr. Fran Nielsen introduced the resumption of the baseline standards event that was to take place September 11, 12, and 13. Because of scheduling conflicts of many of the original September participants, this December meeting could only offer a condensed version of the planned program. Participants included Paula Moore of the General Accounting Office, Jack Garnish of the Social Security Administration, William Pollack of the Centers for Medicaid and Medicare Services (CMS) of the Department of Health and Human Services (HHS) and Maria Stella representing the Federal Aviation Administration.

Ms. Moore of the General Accounting Office (GAO's) presented a briefing on their perspective on minimum information security controls. **[Ref. #1]** Topics covered in her presentation were: GAO's information security activities; GAO audit criteria and approaches; control challenges, and considerations for minimum controls. She identified a need for a handbook containing an overall view of information security framework on compliance. Another example of need is that of a clearinghouse site on regulations of the Health Insurance Portability And Accountability Act (HIPPA). GAO is also providing feedback to Congress on the Government Information Security Reform Act (GISRA) exercise.

The criteria GAO uses is a three-wave approach. One is the wave of technology; another is the wave of laws and regulations that lags behind the technology wave, and the third is the wave of communications about those things and how they get applied. A key struggle of this entire field is how to keep up with these waves and the inertia of them. A fourth wave may be the attacks.

Accepted practices that GAO uses were discussed. Board member John Sabo said that he observed that accepted practices are also a patchwork of practices. He mentioned that Canada is moving to audit framework tools and asked if GAO considered working with similar auditing frameworks. Ms. Moore agreed that such tools could be of value to GAO and indicated that she would bring this observation to the GAO's attention.

It was asked who is held accountable within the agencies for making sure that the GAO findings are held to task. Ms. Moore responded that each agencies' Chief Information Officer should have that responsibility. She noted, however, it may differ agency to agency.

Agency discussions followed Ms. Moore's briefing. First to speak was Jack Garnish of the Social Security Administration (SSA). He said that while the current method of doing business at SSA was face-to-face, the desire was to do more business electronically. They participated in a Project MATRIX exercise and satisfied a critical infrastructure protection checkmark. He explained the process of the review. Project MATRIX gave SSA a framework to manage security, both physically and programmatically. The SSA has several ways that they document policy. They have a handbook of policies and procedures, an audit trail system and an integrity review system. Another of their best practices is their procedure for protection of outside use systems by former employees. Working through the SSA personnel system, when an employee leaves their computer password is automatically suspended, an alert is sent to the security officer and the employee's profile is removed from the system.

Next, Mr. William Pollack of the Centers for Medicaid and Medicare Services (CMS) of HHS addressed the Board. The Center's Chief Information Officer, Gary Christoph, has a background in computer security. The information security area is receiving funding. They have two employees dedicated to working on the information security program within CMS. They have in place an information Internet security policy that does not permit them to use the Internet to transmit secure data, and they provide extensive virus checks regularly. CMS provides in-house computer security training for all employees and have a password change policy in effect requiring changes be made every sixty days. The ROADMAP project issued within the agency for contracting purposes.

In the area of privacy process implications and safeguards both the SSA and CMS seek the approval of their respective agency's privacy officer.

Maria Stella, representing the acquisition and communications systems area of the FAA, was the next to speak. The FAA turns its attention to availability rather than confidentiality. Air traffic controllers and pilots rely on open communications regarding the decisions that have to be made. Ms. Stella's office has an information security policy in place. Using protection profiles, they review their systems individually. They believe that a sound procedural policy is important along with awareness and training policies. She said that it would be very useful if agencies had a set of minimal baseline standards. The FAA has 30 security policies in place with accountability driven down from top management. The air traffic controllers are working with Legacy systems. They perform over 100 security assessments on this system.

After the agencies completed their briefings the Board engaged in dialogue regarding the minimal baselines standards issues. The FAA has ISS architecture with a list of principles and generic protection profiles are being developed in plain language. The Centers for Medicare and Medicaid Services is developing a tool listing all that is required of them. Board Member Michelle Moldenhauer of Treasury stated that the Internal Revenue Service contracted a certification and authentication tool. Treasury is also trying to develop a tool that will fit their 15 disparate groups. Their auditors are planning to use the tool and the IG's are being brought into the development process. SSA's Jack Garnish stated that baseline standards development in dealing with the public depended upon what you are doing with the public. Providing information to the public is no problem. Receiving information from them presents the problem of who is responsible for the protection of the information.

To the question of what problems are trying to be controlled in setting a minimum set of controls, Mr. Reeder replied that most of the damage, loss of data, denial of services, compromise of security, occurs as a consequence of exploiting vulnerabilities that are known about and for which the remedies are widely understood.

Ms. Moore recognized that there are already many controls available as guidance. However, none are deemed mandatory. She suggested that the Board many want to review what guidance is already available, identify any gaps, and perhaps recommend that guidance should be made mandatory across the government. Board member Michelle Moldenhauer suggested that the OMB should be the agency to issue directives of this nature in conjunction wit the homeland security effort.

Accountability of such controls and how to get agencies to meet any baseline standards requirements was identified as a major concern. One suggestion made was to evaluate and showcase the agencies that already have some minimal controls in place. Another suggestion that was made was for the Board to make a recommendation for action on this issue to the newly established Critical Infrastructure Protection Board.

Next, Board member Charisse Castagnoli presented a short briefing on several emerging technologies that she had the opportunity to review over the past few months. The first one she reviewed was distributed denial of services (DDOS). Topics covered included the limitations, statistical analysis and protocol analysis. The next update was on intrusion detection services (IDS). She mentioned that a new solution being developed included the use of mobile agents for verification and response. Also, host based IDS is working on signature-based issues. She noted that the overall trend was that software is moving into hardware and that the focus is on management.

The meeting was recessed at 4:15 p.m.

Thursday, December 6, 2001

Chairman Reeder reconvened the meeting at 8:30 a.m.

Presentation on Privacy Issues in the U.S. Postal Service

Zoe Strickland of the U.S. Postal Service (USPS) presented a briefing on the privacy program of the USPS. **[Ref. #2]** Mr. Charles Chamberlain who is the secure electronic services manager accompanied her. He briefed the Board on the USPS' electronic postmark products and certificate authority effort. Ms. Strickland reported that the USPS program looks at the people, the policies and the processes. A USPS privacy advisory board was established. Its membership consists of the Chief Privacy Officer, a position created in November 2000, the Manager, New Business Programs, Inspector in Charge of Computer Crime and Commerce from the Inspection Service, the Chief Information Security Officer, CTO, the Manager, Internet Services of eBusiness Integration, CTO and the Manager, Advertising.

Business development was a major undertaking of the USPS last year. They developed a privacy toolkit that covered relevant statutes and policies and data classification as well as security in the areas of sensitive systems, business-controlled systems and non-sensitive systems. The attacks of September 11th impacted marketing and business issues. She referred to a recent Forrester report that indicated that 60% of the public still has strong concerns about on-line privacy. Purchasing on-line has also declined as well as the use of the Internet for 'surfing.'

The USPS has created a Customer Data Committee to try and understand who has what data is where. They are looking at audits, enterprise-wide privacy policies, data practices, Privacy Act systems for customer databases and customer personalization.

Ms. Strickland also reported that all of the Postal Governors had recently written to President Bush to request postal reform be given high priority in his Administration.

Government Paperwork Elimination Act (GPEA) Work Plan Discussion

Board Member Rich Guida presented a discussion of the GPEA effort and findings the Board could consider recommending to the agencies. He reviewed the actions of the Act to date. Final OMB guidance was published in April 2000 as required by the Act. The OMB also required agencies to report the status of their GPEA compliance by October 2000. Agencies responded with varying degrees of detail and substance. The agency reports are not publicly available. Currently, OMB is receiving updated information from the agencies. In August 2001, OMB formed an e-government task force. After review of the agencies' submissions, the task force selected 22 projects that they intended to push to e-enable, including e-signatures where appropriate.

The Board members discussed observations and concerns that they could share regarding the GPEA effort. They included the concern that there was no longer going to be a CIO Council committee dedicated to security and privacy issues and that e-authentication issues needed to be addressed. Possible roles seen by the Board were to respond to OMB and agencies when they request our advice and assistance, focus on the OMB selected 22 projects, and offer to review the processes that are going to be used to conduct these projects. It was also suggested that the Board offer to review the agencies' GPEA submissions to be followed up by the review of the 22 projects and provide feedback to OMB.

Chairman Reeder and Board Members Rich Guida and John Sabo volunteered to discuss the Board's proposal with appropriate staff at OMB and report back to the Board at the March 2002 meeting.

Board Discussion Session

The Board discussed the working draft of the proposed letter to the Secretary of Commerce in support of the national awareness campaign program. Edits were made to the draft and the letter was approved for forwarding to the Secretary of Commerce. A copy of it will be posted to the Board website.

The list of proposed meeting dates for calendar year 2002 were reviewed. It was noted that the meetings would be held at the National Institute of Standards and Technology (NIST). However, there is the possibility of scheduling up to two meetings at different venues.

The Board also reviewed a list of potential topics for the March 2002 meeting agenda.

Computer Security Division Update

Mr. Ed Roback, Chief of NIST Computer Security Division, provided an update on the current activities of the Division. **[Ref. #3]** He reported that the specific focus areas of NIST's security program were cryptography, testing, research, management guidance and assistance and outreach. He reviewed the Divisions key federal and industry activities in each of these focus areas. NIST is improving security by raising awareness of the need for cost-effective security, engaging in key U.S. voluntary standards activities, developing standards and guidelines to secure federal system and providing a national leadership role for security testing and evaluation through its cryptographic module validation program and the national information assurance partnership. Mr. Roback also reviewed the Division's budget trends over the past four years.

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

Ref. 1 – Paula Moore's presentation
Ref. 2 – Zoe Strickland's presentation
Ref. 3 – Ed Roback's presentation

Fran Nielsen
Board Secretary

CERTIFIED as a true and accurate
summary of the meeting.

Franklin S. Reeder
Chairman