COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

March 29-30, 2000

Wednesday, March 29, 2000

The Computer System Security and Privacy Advisory Board was convened for its first meeting of the year at 9:00 A.M. by Board Chairman, Dr. Willis Ware.

Board members present:

Mr. Peter Brown
Mr. Richard Guida
Mr. Joseph Leo
Mr. Steve Lipner
Mr. John Sabo
Mr. Franklin Reeder
Prof. George Trubow
Mr. James Wade
Mr. Rick Weingarten
Dr. Willis Ware, Chairman

Also in attendance was Mr. Daniel Knauf, the NSA designated nominee to the Board. He will be replacing Mr. John C. Davis, who retired from NSA in November of last year.

The meeting was open to the public. There were eleven (11) members from the public in attendance when the meeting was called to order.

Board Secretary, Mr. Ed Roback welcomed the newest members to the Board, Mr. Lipner and Mr. Reeder. He said that Mr. Knauf's appointment process was progressing and his appointment would be final very soon.

He announced that the Information Technology Laboratory had a new deputy director, Dr. Susan Zevin, formerly from Commerce's National Oceanic and Atmospheric Administration. He announced that a Common Criteria conference would be held in May, the third AES conference would be held in New York City in April and the security metrics workshop would be held in June in conjunction with the next Board meeting.

Next, Mr. Roback reviewed the meeting agenda and associated handout materials.

"Security Metrics Workshop Update and Discussion

Dr. Fran Nielsen
Computer Security Division, ITL
NIST

Dr. Nielsen presented an overview on the objectives of the workshop and reviewed the actions taken as a result of the September and December Board meeting discussions. **[Ref. 1]**. She presented a proposed agenda for each day of the workshop. The first day will focus on the workshop's expected outcomes, various surveys of security in world class organizations and federal and private sector projects in the metrics area. The second day of the workshop will consist of government and industry case study panels. After the completion of the workshop, a follow-on report or white paper will be produced in late summer that will offer a survey of the state of practices, catalog activities and contain a glossary of terms. It will also contain recommendations of the Board addressing the need for any future workshops on this topic.

Systems Security Engineering-Capability Maturity Model (SSE-CMM) Briefing

Karen Ferraiolo
Technical Director, International Systems Security Engineering Association (ISSEA)

Ms. Ferraiolo began her briefing with an overview of the ISSEA's objectives. **[Ref. 2]** They are a non-profit professional organization consisting of an advisory council, SSE-CMM support organization and board of sustaining members. She explained that the SSE-CMM is a framework of generally accepted security engineering principles and a standard for measuring the effectiveness of an organization's practices. The model serves as a roadmap for improving security-engineering processes. The guiding principles are divided into two areas: security engineering base practices and management and organizational practices. She also identified the attributes of the organizational, project and engineering process areas. Further information on the SSE-CMM can be found at the following website: www.ssecmm.org.

Access Certificates Electronic Services (ACES), An Update

Judith Spencer, Director
Center for Governmentwide Security
Office of Information Security
General Services Administration

Ms. Spencer was unable to attend this meeting because of an unanticipated scheduling problem. She will be invited to a future Board meeting to provide her ACES update.

Recognition for Dr. Willis Ware

NIST Director Ray Kammer presented Dr. Ware with a certificate of appreciation for his years of service as the Chairman of the Board since its charter in 1989. The Board joined Mr. Kammer in thanking Willis for his tireless efforts to promote the issues of computer security and privacy and the expertise that he brought to the Board during his tenure. A reception and dinner was held in his honor later in the evening at the Hilton Hotel.

Computer Security Division Updates

Ed Roback, Acting Chief
Computer Security Division
NIST

Mr. Roback discussed the current activities of the Computer Security Division. He reviewed the NIST assessment panel process and how this advisory committee annually reviews and assesses the division's programs. The Board expressed their concern for the recent lost of senior personnel within the Division and the lack of a designated SES-level for the Division Chief position. The Board may want to engage in future discussion with NIST management about their views on this matter and other IT issues.

Mr. Roback briefed the Board on the current Presidential budget initiatives that could have an impact on the work of the Laboratory. He reported on a $3M initiative for the establishment of an expert review team to operate a program of approximately eight team members. There is also a request for $5M for critical infrastructure protection research and development activities that would start up a national information infrastructure protection project that NIST would coordinate.

Next, Mr. Roback discussed the NIST draft guidelines to federal organizations on security assurance. He noted that the document had been distributed for review and asked the Board to offer their suggestions and comments before the May 1st deadline.

The Division is developing its strategic plans for next year. Mr. Roback would welcome the Board's recommendations on what the Division should focus their efforts on in the coming year.

Mr. Roback reviewed the status of the selection of the AES algorithm. Following the April AES conference, NIST will announce which algorithm(s) they have selected and issue a paper describing and documenting their choice. Mr. Roback serves as the chair of the selection panel consisting of Computer Security Division personnel.
In addition to other factors, the final decision will also be based on comments received from the outside community.

Public Participation Period

There were no requests for public participation.

Board Discussion Period

The Board reviewed the minutes from the December 1999 meeting. They were approved unanimously.

Next, the Board reviewed the current draft version of the Government Information Security Act (S. 1993) and noted that this version did not emphasis the Computer Security Act like the House version (H.R. 2413). It was proposed that the Board review the latest version of H.R. 2413 and consider offering any comments to the House Government Reform Committee.

The Board decided on the final format of the security workshop and developed a set of questions to be addressed by the case study panels. Letters of invitation will be sent out to the invitees by April 14th.

Future Board meeting topics were discussed. They included updates on any breaking events or computer security and privacy legislation activities, updates on the national plan and CIO council activities, Security Policy Executive Committee updates, and a discussion of the ISAC financial services lab activities.

The meeting was recessed at 4:00 p.m. for the day.

Thursday, March 30, 2000

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

Board Discussion Period

John Sabo briefed the Board on International Security, Trust and Privacy Alliance (ISTPA) activities. They are a not-for-profit international organization working together to clarify and resolve existing and evolving issues related to security, trust and privacy. They are focused on defining technology that will work throughout the business enterprise, from mainframes to desktops. Four working groups are being formed to cover framework, architecture for privacy, functionality requirements and outreach. Member companies include American Express, Compaq, IBM, Intel, Motorola, NCR and TRUSTe among others. Mr. Sabo volunteered to arrange for an ISTPA briefing at the Board's September meeting. Additional information on the ISTPA can be found at the following website: www.new-istpa.org.

Next reported was information about the PKI Forum, an international, not-for-profit, multi-vendor alliance whose purpose is to accelerate the adoption and use of Public-Key Infrastructure (PKI) and PKI-based products and services. There are two main working groups: (1) the business working group; and, (2) the technical working group. The membership consists of over 52 companies. While not a part of the formal membership, the government is involved in the PKI Forum. For more information the Forum, see the following website: www.pkiforum.org.

More discussion about the security metrics workshop took place. It was decided that this workshop would be advertised as being held in conjunction with the CSSPAB quarterly meeting with the intent to follow it with a larger workshop/conference later in the year.

In identifying concerns and issues that the Board may wish to address, Steve Lipner discussed his views that the government should address operational issues in the computer security arena which now have them falling behind industry. He believes that the government should exercise more leadership in the infrastructure protection area. They are in need of better marketing practices to change the public's perception. Mr. Lipner suggested that the Board review the government's practices and policies and

management structures for protecting their own data, and identify the good ones and point to them as examples for others.

Mr. Reeder stated that the Board needs to know issues that NIST, the Department of Commerce, the National Security Council, OMB and Congress think the Board should be addressing. He suggested that this be looked into.

Mr. Leo believes that the Board should strengthen its activities by becoming more operationally.

Mr. Knauf's perspective is that the major problem is dealing with the ill-defined digital revolution. He suggested that the Board focus on identifying emerging issues as stated in the Board charter. The Board could select a few of the larger issues and sharpen the debate, and perhaps, produce a few white papers. His observation is that the government operates in three ways. They educate, mandate or throw money at the issue at hand.

Mr. Lipner suggested that the Board be prepared to address specific issues/questions at their next meeting. One of the questions might be why is the government better organized or has resources in place to deal with the next denial of service attacks, or any other issue that may come up.

Dr. Ware said that the problem for the Board is that it does not have an effective sales campaign in place to promote any of the actions that they take. He suggested that the Board look at what the government is currently doing and select one or two major issues, spend one year or more studying them and hold workshops and produce products. Mr. Knauf suggested that one of the issues that the Board could look into was in the area of individual rights and abuse of digital data. Other questions/topics suggested were on virtual office and telecommuting and issues regarding OSHA requirements and how they are met, is the government in a good posture as an e-commerce country and, is NIST in good shape in the digital and e-commerce worlds.

Mr. Wade suggested that the Board could begin to solicit input on major issues from the outside via website visibility.

As this is an election year, Dr. Ware said that the Board should correspond with the Presidential transition teams about the relevance of what they see into the next Administration.

EU Signature Directives Updates

Mark Bohannon
Chief Counsel
Technology Administration
Department of Commerce

Mr. Bohannon briefed the Board on the recent actions of the EU signature directive, which promotes European technology and standard. The three key aspects of the directive are the different level of legal effect given to electronic signatures and advanced electronic signatures, the liability rules established for issuers of qualified

certificates and the provision of a framework for cross-border recognition with third world countries. The directive does not address the conclusion and validity of contracts, form requirements in national or EU law or propose rules or limits in national or EU law on use of documents. The U.S. government has been involved. There have been site visits by the Department of Commerce and they have provided technical assistance in legislative draftings. The U.S. government has a commitment to industry leadership and for the self-regulatory, voluntary approaches to further e-commerce and international trade. Mr. Bohannon indicated that Commerce was considering requesting suggestions on how to accomplish this by issuing a Federal Register request for comments.

Mr. Bohannon reported that the European electronic signature standards initiative has been formulated with support and input from the EU Commission's DGIII. It is industry-led. There are no U.S.-based companies in leadership roles on the expert panel. The work plan is being implemented by European standards bodies, ETSI (European Telecommunications Standards Institute) and CEN (European Committee for Standardization). He pointed to a July 1999 roadmap document done by the EESSI (European Electronic Signature Standardization Initiative) experts team. It can be found at the following website: http:www.ict.etsi.org.

The concerns of the U.S. government include the leadership role of the EESSI team and whether the U.S. government's principles of technology neutrality and non-discrimination will be respected.

Another challenge is in the area of compliance testing, reported Mr. Bohannon. Appropriate public or private bodies designated by the member states should determine conformity of signature devices. There is a committee working to clarify the criteria and whether there will be national testing bodies, industry testing or self-declaration.

Over the next eighteen months, the major emphases will be the implementation of national law, to focus on real opportunities to effect market driven approaches to accreditation, to engage in development of standards for signature devices and to examine cost-effective, timely testing.

Administration Privacy Update & OMB Updates

Lauren Steinfeld
Deputy Privacy Counselor
Daniel J. Chenok and Glenn Schlarman,
Office of Information and Regulatory Affairs, OMB

Ms. Steinfeld presented an overview of the major initiatives over the last year. She noted that in September 1999 the Wall Street Journal took a poll that indicated that the American people were more fearful over their lost of personal privacy, then they were over global warming or facing war conflicts. Major privacy issues that she identified were medical records, financial records, internet privacy, government records and privacy impact assessments.

The Department of Health and Human Services (HHS) has the responsibility for rulemaking regarding medical records. There have been over 66,000 comments received on HHS's proposed rules. Ms. Steinfeld indicated that the comments she has seen have been mixed.

In the area of financial records, the Administration is in favor of financial privacy legislation. Customers should be given notice as to what is going to be done with their information and banking financial institutions should enforce this. They are in the rulemaking stage and have until May to reach finalization.

The Administration favors self-regulation of the internet and is looking to industry to come up with ways to protect privacy on line. The Federal Trade Commission (FTC) and Georgetown University did two surveys on privacy policies. The FTC is conducting another survey on this issue and, it should be available within the next several months.

Ms. Steinfeld reported that upon initial review, 40% of government websites had privacy policy statements. Following an OMB issued memo mandating that agencies have a privacy policy on their websites, 100% compliance was reached in September 1999.

In the area of privacy impact assessments, a set of specifications that should be used in the creation of new IT systems should be developed. Ms. Steinfeld indicated that this is an ongoing work effort. She also indicated that there is an effort being discussed to create a 'seal of approval' but at this time there is no firm activity.

Of all of these efforts, the Administration is trying to get as much done as quickly as possible on all of them. However, their first priority is on medical record privacy followed by financial privacy.

Next, Dan Chenok and Glenn Schlarman presented an overview of OMB issues.

The security issue is the current hot issue. They discussed the February 28, 2000, memorandum from OMB Director Jacob Lew regarding incorporating and funding security in information systems investments. The objective of this is to support more effective agency implementation of both agency computer security and critical information infrastructure protection programs. A set of instructions that agencies will follow will be produced. They also anticipate having this directive eventually incorporated into Appendix III of A-130.

They reported on current legislative activities. S.1993 (Lieberman) codified a large part of A-130. OMB continues to work with the Hill on the document. Action is expected on the House floor before the spring recess. Other members of Congress such as Sensenbrenner, Gordon and Morella are also working on promoting additional computer security legislation. Also, it was noted that Rep. Steven Horn is proposing to grade agencies on security in a manner similar to what happened during the Y2K initiative effort.

OMB is about to issue guidance on the implementation of the Government Paperwork Elimination Act (GPEA). They are working with the CIO Council on this issue and the President issued a memorandum in December 1999 on implementing the electronic government.

In response to a question on FidNet, Mr. Schlarman said that there is no FidNet now, and that no funds have been appropriated for it at this time. It is, however, part of the FY01 budget request for GSA.

Best Practices Update

Jim Craft, U. S. Agency for International Development
Chair, CIO Security Practices Subcommittee

Mr. Craft gave the Board an overview of the status of the Federal best security practices program. **[Ref. 3]** This is an initiative of the CIO Council to share security assurance while lowering the total cost of security practices. It came about as a result of the convergence of three best security practice initiatives: critical infrastructure protection, model information systems security program and the CIO Council's strategic objectives. A security process subcommittee (SPS) was formed consisting of representatives from the CIAO, OMB, DOD (DISA), NIST, NSA, GSA, OPM, CFO Council, Justice, State, USAID, HRSA, IRS, GAO, U.S. Senate and the U.S. Courts. Mr. Craft described the major components of the best practices program and how they all work together. He said that there are many challenges to accomplishing this task. They meet every two weeks. Work is continuing on the Web-repository to ease electronic submission and search capabilities. They are issuing interim documentation and developing outreach material.

Mr. Craft said that the Board could help by providing their feedback on the issues, identifying groups to work with and perhaps, co-sponsor a workshop to identify potential best security practices. The group is also working with the Chief Financial Officer Council, the Federal Computer Security Program Managers' Forum members and others to get their input also.

There being no further business, the meeting was adjourned at 4:00 p.m. by Chairman Ware.

References:

#1. Nielsen presentation
#2. Ferraiolo presentation
#3. Craft presentation

Edward Roback
Board Secretary

CERTIFIED as a true and accurate summary of the meeting

Willis H. Ware
Chairman