COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

September 14-15, 1999

Tuesday, September 14, 1999

The Computer System Security and Privacy Advisory Board was convened for its third meeting of the year at 9:00 A.M. by Board Secretary, Mr. Ed Roback.

Board members present:

Mr. John Davis
Mr. Addison Fischer
Mr. Joe Leo
Mr. John Sabo
Prof. George Trubow
Dr. Willis Ware, Chairman

The meeting was open to the public. There were five (5) members from the public in attendance when the meeting was called to order.

Mr. Roback reviewed the meeting agenda and associated handout materials. He discussed the status of the membership vacancies of the Board. He stated that a Federal Register announcement was being prepared to solicit nominations for membership on the Board.

He informed the Board that Dr. Miles Smid, Acting Division Chief of the Information Technology Laboratory (ITL) Computer Security Division had announced his plans to retire on October 1, 1999. Also, Mr. Paul Domich, Acting Deputy Director of the ITL office returned to his position at the National Institute of Standards and Technology in Boulder, CO. His replacement is Ms. Barbara Guttman, formerly of the ITL Computer Security Division.

Mr. Roback reported that the Advanced Encryption Standard (AES) effort was proceeding and that there had been an announcement of five finalists for the AES. These finalists have been made available for public comment until May 15, 2000.

Introduction of Outline for "Security" Metrics Workshop

Dr. Fran Nielsen
Computer Security Division, ITL
NIST

Ed Roback introduced Dr. Fran Nielsen from the Computer Security Division who will assist the Board in developing and organizing a workshop on "security" metrics. This effort is a result of a request from the Director of NIST, Mr. Ray Kammer, to identify the

specific types of security metrics and explore how such metrics might be developed and used.

In her briefing **[Ref. 1]**, Dr. Nielsen solicited the Board to identify the expected outcomes, information exchange and potential tangible products that could be expected. They discussed the target audience, meeting format and potential topic areas. Additional discussion the next day focused on the overall goals of the workshop and purpose statements; title of the workshop; identification of the target audience; and development of a presenters template. Dr. Nielsen will continue to refine the proposals and options presented and, this topic will be discussed at the December meeting of the Board.

Update on Status of National Plan for Information Systems Protection

John Tritak, Director
Critical Infrastructure Assurance Office (CIAO)

Mr. Tritak began his presentation by sharing his view of the CIAO office role and its involvement in the PDD63 effort. The CIAO's primary goal is to help the National Coordinator, Richard Clarke, in the implementation of the PDD63. He said that the CIAO comprises a collection of interagency participants from the major Departments and Agencies, including NIST. An expert review team was created at CIAO to assist agencies to identify vulnerabilities in their infrastructures and to identify goals and ways to correct them.

On the topic of the National Plan, Mr. Tritak said that the plan should be released sometime in October 1999. According to him, the federal government cannot solve the problems without participation from the private sector. This requires a new way of doing business by bringing together the federal and private sectors in a partnership effort. The comments and concerns that the Board had provided to the CIAO on the draft National Plan will be reflected in the new version, said Board Member, John Davis. He is also a member of the CIAO activities.

Chairman Ware commented that the media reported that the focus would shift from the Y2K issue to the issue of information security after January 1, 2000. He asked Mr. Tritak if those now focusing on the Y2K problem would begin to work with the CIAO on the IT issue. Mr. Tritak stated that he believes that there will be historical value gained from the Y2K experience that will have both good and bad points relating to the IT issue. He said that there will be a "post mortem" done on the Y2K effort by the CIAO and others. He also indicated that his observation was that the critical infrastructure protection (CIP) effort has bipartisan support in the Congress. He commented that he believes Congress will support the CIP initiative.

Mr. Tritak also reported on the National Infrastructure Assurance Council (NIAC) which was created by Executive Order in July 1999. The membership is made up of 30 CEO-level members representing key critical infrastructure sectors. This group serves as a 'watchdog' to advise the President on how to proceed in the implementation of the PDD63.

Transatlantic Consumer Dialogue Privacy (TCDP) Coalition Briefing

Mr. Ed Mierzwinski
U.S. Public Interest Research Group (USPIRG) and
TCDP Steering Committee Member

Mr. Mierzwinski began his presentation by giving an overview of the U.S. Public Interest Research Group activities and its relationship to the transatlantic consumer dialogue privacy coalition. Next, he covered the USPIRG's point of view on the Department of Commerce Safe Harbor proposal that US companies choose to adhere to certain privacy principles. The Safe Harbor platform is a directive on data protection dialogue that has been proposed to enable U.S. organizations to comply with the requirements of the European Union's Directive on Data Protection regarding personal data transfers to third countries.

The USPIRG is opposed to the implementation of the Safe Harbor proposal because they believe its principles are not met by a number of organizations. Also, they do not believe this proposal provides adequate protection for European citizens. Mr. Mierzwinski reported that Congress is in the process of developing legislation that will offer alternatives to the Safe Harbor approach. He is hoping for the development of an overarching privacy law from Congress. The EU advised that the Safe Harbor proposal should not be abandoned, but improved. The expectation is that the United States hopes to complete its actions on this by later in the Fall.

Federal Intrusion Detection Network (FIDNET)

Thomas Burke
Assistant Commissioner for Information Security
General Services Administration (GSA)

Mr. Thomas Burke, Assistant Commissioner for Information Security, GSA, lead a discussion on the status of their latest digital certificate effort, Federal intrusion detection network (FIDNet) **[Ref. 2]**. He was accompanied by Mr. Darwin Banks from CIAO and Ms. Janice Scott of GSA.

Mr. Burke described FIDNet as an initial phased approach to federal intrusion detection. It is part of a larger plan to address a whole range of capabilities that include patches, alternative operating systems, best practices working the CIO Council, training certification procedures for federal system administrators and continuation/expansion of expert review teams. It will incorporate present and future research and development. He reported that a FIDNet pilot is under development and that they are using a DOE model as a prototype. There will be ongoing legal review throughout the project by a group consisting of the White House Privacy Counselor, Peter Swire and representatives from GSA, CIAO, OMB and the Department of Justice.

The role of FIDNet is to look at the non-DOD systems within the federal government and the information on those systems that are owned by the government. They will also be looking at the authority of agencies to manage their own systems and delegate responsibility. FIDNet has no plans to interact with the private sector. Some of the expected benefits include correlation of intrusion/electronic events, economies of scale and better detection of low flyer.

Mr. Burke encouraged the thoughts and comments from the Board on how GSA should take the information that is being gathered and build it into something that would benefit everyone.

Overview of President's Export Control Subcommittee on Encryption (PECSENC)

Patricia Sefcik, Director
Information Technology Control Division
Bureau of Export Administration (BEA)
Department of Commerce (DOC)

Ms. Patricic Sefcik, Director of the Information Technology Control Division at BEA/DOC, gave the Board an overview of the status of the PECSENC activity **[Ref. 3]**. Mr. Jason Gomberg accompanied her. He is the BXA designated federal official for the PECSENC.

Ms. Sefcik stated that the mission of the PECSENC was to provide advice and make recommendations on ways to minimize the adverse impact of commercial encryption policy on U.S. business while balancing the interest of U.S. national security, foreign policy, and public safety. It is an advisory board and a subcommittee of the President's Export Council. It is also Undersecretary of Commerce William Reinsch's number one priority, according to Ms. Sefcik.

Mr. Gomberg continued the briefing providing background information on the PESCENC. He said that the PECSENC was chartered in May 1997 and, its current chairman is William Crowell, CEO of CyLink Corporation. It holds meetings bimonthly. There are three working groups: international policy, regulations and technology. In August of 1998, the Board developed a foreign availability paper that recommended changes to the encryption policy. He reported that in June 1999, PECSENC wrote a policy paper entitled "Liberalization 2000" which contained their recommendations for the Administration's next encryption export policy update.

Ms. Sefcik stated that the Administration was preparing to issue an announcement within the week regarding changes to the Administration's export policy on encryption. She said that the European Union plans to implement the Wassenaar arrangement, a U.S. proposal already agreed to by 33 countries.

The future topics to be taken up by the PECSENC will focus on examination of the role of encryption and encryption controls on open source software, authentication, Smartcards, and intellectual property protection.

Information Technology Security Research Efforts Briefing

Bruce MacDonald
Office of Science and Technology Policy
The White House

Mr. MacDonald briefed the Board on the most recent efforts underway in carrying out the responsibilities of meeting the research and development challenges of PDD-63 **[Ref. 4]**. The Office of Science and Technology (OSTP) has the responsibility for coordinating research and development (R&D) agendas and programs for the government through the National Science and Technology Council. The OSTP vision is to enhance the security of our nation's critical infrastructure by rapidly identifying, developing, and facilitating the fielding of technological solutions to existing and emerging infrastructure threats and vulnerabilities. In order to accomplish these tasks, the OSTP heads up the

Critical Infrastructure Protection (CIP) R&D Interagency Working Group. There are seven sub-groups based on different infrastructures. They have identified 71 programs, briefed private sector and academic community on federal program and solicited inputs and comments on the federal CIP R&D agenda as ways to help them reach their objectives. Mr. MacDonald reviewed the federal CIP-related R&D FY2000 funding and the proposed FY2001 budget process. He identified the management challenges. Several important questions being examined included:

- are existing labs, inside or outside government, sufficient,
- what R&D entity would make more sense,
- how would a new R&D entity recruit and retain top talents, and
- what are the view of private sector and academia?

Mr. MacDonald concluded his briefing by stating that meeting the CIP challenge will require an ongoing commitment from the government, private sector and academia to strive for R&D excellence. The explosive growth in new technology means all of us cannot rest. Cooperation and collaboration with all partners doing what they do best will be essential to keep our nation's critical infrastructure secure.

The meeting was recessed at 4:45 p.m.

Wednesday, September 15, 1999

Chairman Ware reconvened the meeting at 9 a.m.

The Board started the day with discussion of plans for the proposed workshop on security metrics. These actions were reported earlier in these minutes.

Common Criteria and ITSEC Harmonization

Dr. Ron Ross
Computer Security Division, ITL
National Institute of Standards and Technology

Dr. Ross presented an update on the Common Criteria evaluation program. The program is in its final stages. All of the laboratories now undergoing evaluation by the trusted technology assessment program are very capable labs and he has a high degree of confidence in them.

He reported that the National Information Assurance Partnership (NIAP) continues to develop their scheme documentation to provide guidance to the labs. A validation body will exist to validate the evaluation process and issue certificates. The question was asked if any other countries had certified laboratories for the evaluation of their products. Dr. Ross responded that Canada, France, United Kingdom and Germany also had certified labs.

He reported on the status and scope of the mutual recognition arrangement (MRA). Five countries have signed with the expected expansion of more countries such as Australia. With regard to ITSEC, the United States has been very aggressive in working to eliminate the Orange Book activity. However, Dr. Ross reported that this is not the case

outside of the United States. The MRA will contain no reference to ITSEC; only commitment to common criteria.

There is also a health care community effort that Dr. Ross briefly discussed. The Board will hear a briefing on this topic at their December meeting.

OMB/OIRA Update

Glenn Schlarman
Office of Information and Regulatory Affairs
Office of Management and Budget

Mr. Schlarman's discussed with the Board a June 23, 1999, memo from Jacob Lew, Director of OMB, on the topic of security of federal automated information resources. The purpose of this memorandum is to remind agencies of the principles of OMB Circular A-130, Appendix III. It focuses on agency computer security practices rather than plans and the vulnerabilities to externally accessibility systems and implementation of patches to protect these vulnerabilities.

Another area that OMB will be looking at is training. A recent report of the Security Privacy Board indicated that several agencies had reduced funding for training or eliminated it from their budgets. OMB will also be looking into the area of incident response and intrusion detection activities within the agencies, asking if they are conducting any intrusion detection monitoring, and if so, how effective it is, how is it gauged, how is it tested. They are also interested in knowing how agencies have handled any intrusion detection of their systems. OMB plans to publish a report of their findings.

Mr. Schlarman also reported that OMB is working on critical infrastructure programmatic and budgetary issues. He reported some progress in this area but admits that it has its own dilemmas. Some agencies feel that OMB is trying to establish yet another hierarchy for computer security.

When asked about the possibility of Y2K money availability to cover computer security initiatives, Glenn said he does not anticipate any in the immediate future.

Discussion of the Report of the Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Public Key Infrastructure and Possible Development of Board Recommendation

Elaine Barker
Computer Security Division, ITL
National Institute of Standards and Technology

Elaine Barker presented a brief overview of the background of this committee effort **[Ref. 5]**. She reported that the document was out for comment until November 4, 1999. After the comment period closes, NIST will evaluate any comments received and then determine what steps to take. It was suggested that the document be reviewed by a panel of experts to see if it should be implemented as a standard or developed as a guidance document. It was also stated that NIST should not discard this effort but that the decision of what course to take was entirely theirs to make.

This concluded the business scheduled for the day. Because of the bad weather and potential for cancelled airline flights for Board members, the Board decided to cancel the remainder of the meeting schedule for Thursday, September 16, 1999.

Thus, the meeting was adjourned at 4:05 p.m.

References:

#1. Nielsen presentation
#2. Burke presentation
#3. Sefcik presentation
#4. MacDonald presentation
#5. Barker presentation

Edward Roback
Board Secretary

CERTIFIED as a true and accurate summary of the meeting

Willis H. Ware
Chairman

These minutes will be formally considered by the Board at its next meeting, and any corrections or notations will be incorporated in the minutes of that meeting.