COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

December 7-9, 1999

Tuesday, December 7, 1999

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

Board members present:

Mr. Richard Guida
Mr. Joseph Leo
Mr. John Sabo
Prof. George Trubow
Mr. James Wade
Mr. Rick Weingarten
Dr. Willis Ware, Chairman
Ms. Karen Worstell [December 8 & 9 only]

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

Board Secretary, Mr. Ed Roback reviewed the meeting agenda and associated handout materials. He discussed the status of the membership vacancies. There were seven nominees received as a result of the October 13, 1999, **Federal Register** request. Mr. John Davis, the NSA representative on the Board retired from NSA in November. NIST is waiting for NSA to nominate a replacement.

"Security" Metrics Workshop Update and Discussion

Dr. Fran Nielsen
Computer Security Division, ITL
National Institute of Standards and Technology

Dr. Nielsen began her briefing with a review of the issues that were discussed at the previous meeting of the Board in September. **[Ref. 1]**. Since that meeting, she has canvassed the IT community. She held discussions with the CIO Council Security, Privacy and Critical Infrastructure Protection Committee, members of NSTAK and NISSC and gained information via surfing, literature search, emails, and phone conversations. The general consensus was that there was confirmation of the need for security metrics. Along with that, however, was a wide diversity of opinion on the meaning of "metrics." The Board members offered their observations and thoughts on how they thought the workshop should be organized. It is anticipated that this workshop will be the first of several [perhaps three]. The first workshop would be information oriented followed by additional, more detailed workshops. There was discussion on the

issue of whether privacy metrics should become part of the topic area. It was decided that the privacy issues could be touched on at the security metrics workshop but not become one of the main focuses at this point. Other related areas of activities were discussed such as "best practices," readiness assurance and performance issues. Dr. Nielsen will be in touch with Board members who are interested in working with her on the program committee. She will present the program committee's recommendations at the next Board meeting.

Status of the Computer Security Enhancement Act of 1999

Mike Quear
Committee on Science, Subcommittee on Technology
U.S. House of Representatives

Mr. Quear presented an overview of current congressional activities. He said that the Congress is still struggling to bring awareness of privacy issues to the forefront. There appears to be perplexity about what is meant by privacy, especially as it relates to information collected for various database use.

One of the goals of the Computer Security Enhancement Act [HR 2413] is to reinforce NIST's role in serving as a technical advisor and resource on computer security issues and to insure a civilian role of covering non-classified computer security systems. Mr. Quear discussed the major points of the bill. Comments received as a result of a hearing held on September 30, 1999, were very positive. The bill was marked-up on October 30, 1999, with one amendment regarding federal agency plans. The expected disagreement point is on the funding issues. The bill proposes new responsibilities be carried out for which funding would be needed. It is not expected that the current funding levels would cover these responsibilities. Mr. Quear said that Rep. Sensenbrenner would like to see the legislation move by May 2000. There is also a draft Senate version of this bill. It is unclear what the Administration's stand is on this issue. However, Mr. Quear said that he expects there to be a compromise between the House and the Senate on this legislation. He feels that there is promise that something will come out of this effort because Congress does have a strong interest.

Mr. Quear indicated that he would like to see more input from the private sector in support of the computer security civilian role. Electronic commerce is a major area of focus right now. He said that there is the need to regulate it, promote it and identify what the requirements are to make it work. A major privacy concern today is the accessibility of datebases. Raising the publics' awareness of this issue is very important. Mr. Quear said that holding hearings on this would be one way to increase that awareness and perhaps lead to the development of legislative policy. He welcomed the views of the Board.

Board member Weingarten suggested that privacy could be treated as a consumer. He sees the major problem as one of how to broaden the issue to a public debate. Board Member Guida questioned the GPEA statutes that press agencies to move more toward electronic signatures, etc. However, he does believes that there should be a push for reinforcement of GPEA because agencies have taken serious notice of its requirements. Board Member Wade said that he anticipates a public outcry, especially in the area of wireless communication.

Board Member Trubow believes that the public doesn't understand how they are participating in their own invasion of privacy by their own actions. He said that it is Congress' role to stimulate ways of public education, and agreeds that hearings should be held. Even getting people together to identify what the common interests are would be a start, said Board Member Guida, and perhaps from that a common set of guidelines could be developed. Chairman Ware's observation was that e-commerce is doing just fine. He suggested that it works because there is no demand for authentication of any kind. There is consumer protection limitation through financial liability with use of credit cards over the Internet. It was pointed out that this liability coverage was limited by a specified radius of the site contacted and the location of the purchaser.

Mr. Quear thanked the Board for their input and welcomed any further comments they might have in the future.

Access Certificates Electronic Services (ACES), Electronic Public Key Infrastructure Solutions

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

Ms. Spencer briefed the Board on the ACES program **[Ref. 2]**. She reviewed the mandates for on-line access leading up to this work effort. The Paperwork Reduction Act, the National Performance Review's *Access America*, the Federal Public Key Infrastructure Steering Committee and the Government Paperwork Elimination Act all were instrumental in pointing out the need for the effort . Privacy concerns dictate the need for the federal government's particular diligence in identifying the individual requesting information or services. Ms. Spencer said that ACES is not used public to public. It is the certificate services provider for the public key infrastructure (PKI) governmentwide.

The ACES PKI provides identity proofing, issues certificates and provides on-line validation. Five categories of government to public communications have been identified by the Office of Management and Budget that could require strong authentication. These categories are: application and transfer of benefits; application and administration of grants; submission of reporting or filing requirements; exchange of personal/private/proprietary information; and procurement actions. Ms. Spencer reported that the privacy advocacy community is concerned that ACES certificates represent a further erosion of individuals rights to privacy, and that individuals have a right to anonymity and that the individual should be able to choose their certificate issuer.

Ms. Spencer asked for the Board's suggestions on what could be done to persuade the federal agencies to come on board. They suggested that GSA pay particular attention to privacy advocates identification of the social problems that may be created with the use of these services. Board member Weingarten suggested that public structured forums be held with the privacy advocates and include attendance by OMB so that they could hear the issues discussed. It was also suggested that a privacy commission be established within the federal government. Chairman Ware added that GSA consider the development of a statement of privacy concerns to be imbedded in some legislative document.

Ms. Spencer thanked the Board for their comments. She will also be asked to attend the next Board meeting to give them an update on the ACES program activities.

Healthcare Security Initiative

L. Arnold Johnson
Computer Security Division
National Institute of Standards and Technology

Arnold Johnson of the Computer Security Division presented an overview of the healthcare security initiative effort **[Ref. 3]**. He stated that there is a lack of common language to bridge the communication gap among security policy makers, standards organizations, consumers and developers. There is also a lack of common structure for expressing security requirements and assurance and a lack of accredited testing labs and recognized sources for evaluating the security properties of products and validating product compliance.

The healthcare security initiative calls for the establishment of a forum on privacy and security in healthcare for defining security requirements. The Healthcare Open Systems Testing (HOST) consortium and the NIAP are sponsors of this initiative. In response to a question regarding the identification of the threats, Mr. Johnson said that no specific process is currently in place. Identification of the threats has to be done by the organizations who are trying to protect their systems. The Board suggested that Mr. Johnson go back to the forum group and ask them to identify the security threats they are evaluating against and how they were arrived at.

Next, Mr. Johnson described the issues and challenges that lie ahead. He said that the general healthcare user community is having trouble understanding protection profile specifications—not being formulated in terms of healthcare application systems environment. Consensus building in a large and diverse industry is difficult. Mr. Johnson said that NIST is spending about 1.5 man-years on this project and that funding will cease at the end of this fiscal year. NIST sees its role as only a perpetuator of this effort.

Compuer Virus/Hacker Briefing

Rob Rosenberger
Consultant/Expert on Computer Virus Myths and Hoaxes

Mr. Rosenberger presented an overview of his credentials in the computer virus/hacker arena for consideration for membership on the Board **[Ref. 4]**.

The meeting was recessed at 5 p.m. for the day.

Wednesday, December 8, 1999

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

Vulnerabilities in Commercial Sofware

Rich Guida, CSSPAB Member
Department of the Treasury

Mr. Guida discussed a draft position paper that he had prepared on the subject of vulnerabilities in commercial software such as buffer overflow attacks. **[Ref. 5]**. Minimizing the existence of vulnerabilities in commercial software benefits all federal (and non-federal) customers. It is his feeling that the Board may want to offer a strategy that they could suggest to NIST to deal with common problems and promote research and functional solutions. He offered a three part strategy that covered identifying and listing the most commonly experienced product vulnerabilities, research of those problems at the front end of the software loading process with accountability on the companies that produce it if vulnerabilities are found and research that would provide the correct protocols or development of tools to assist programmers to avoid the problems. Mr. Guida said that he would work with the CIO Council to build the momentum to move this initiative forward. He asked for the Board's recommendation on this matter. Members suggested the establishment of a framework that would allow industry to work with the government on the solution of these vulnerabilities. Awareness issues would be the first step that should be considered. It was also proposed that tests be developed that the vendors could implement as they make their products.

Mr. Guida thanked the Board for their feedback and will keep the Board members informed of his progress.

Briefing on S. 1993, Government Information Security Act of 1999

Deborah Cohen-Lehrich
Counsel, Committee on Governmental Affairs
U.S. Senate

Deborah Cohen-Lehrich, Counsel for the Committee on Governmental Affairs briefed the Board on S. 1993 legislation on government information security **[Ref. 6]**. She reviewed some of the things that the Committee may want to consider adding to the legislation. One of these was the issue of interoperability. They will have the General Accounting Office take a look at this area. Board Member Guida referred to the work effort in the PKI arena and how it deals with interoperability. He said that any legislative reference to the topic of interoperability would be of benefit to this work effort.

Board member Weingarten said that there is a need to collect more information about incidents, vulnerabilities and create a database that agencies could use as a reference. Tools and references are needed for managers to carry out their mission. The Board offered additional comments to Ms. Cohen-Lehrich. They included consideration of extending the annual review process from a one-year period to a two-year period, making it implicit that the responsibilities of the CIOs are theirs and not others, and asked for a more discretionary capability in reporting any material weaknesses. It was also suggested that guidance be developed, possibly by OMB, on what should be reported in the 'annual' assessment document.

Members were encouraged to provide any additional comments to Ms. Cohen-Lehrich.

CC^2 and Cyberspace Situational Awareness

Tim Bass
President and CEO
SilkRoad

Mr. Bass briefed the Board on CC^2 and cyberspace situational awareness issues **[Ref. 7]**. His briefing covered high level constructs, state-of-the art IDS overview, construct summary, example of simple blackboard for CC^2, a process flow diagram, cyber attack construct, systems inputs, situational awareness outputs and practical CC^2 next steps.

OMB Updates

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

Mr. Schlarman reported on the outcome of the June 1999 memorandum for the Director of OMB, Jacob Lew on the topic of federal security practices. He said that good information had been provided from all the agencies and that the status of computer security within the agencies is mixed. OMB plans to continue with this activity and look at externally accessible systems. In particular, they will be looking at those systems that support the 43 high impact programs that have been identified in the Y2K remediation process.

As part of an overall three-part strategy that OMB is taking to adjust to how they look at computer security, Mr. Schlarman said he is planning to develop eight or nine security principles. Each agency would then have to demonstrate that they have met these principles before they could obtain continued funding or funding for any new system. Among these principles would be to demonstrate that security is part of the agency's information architecture; to demonstrate that life cycle security cost are understood and incorporated into the life cycle funding. These principles would be a requirement for budget submissions for FY02.

Mr. Schlarman reminded the Board that health care regulations were out for public comment and encouraged the Board's input.

Trusted Computing Platform Alliance (TCPA) Briefing

David Chan
Technical Committee Chair
Hewlett-Packard

Mr. Chan presented an overview on the TCPA program effort **[Ref. 8]**. The goal is to raise the level of trust and security on mainstream computers, not inventing a new standard, but looking at the missing pieces to have a security platform. He reviewed the mission and problems being addressed. The Alliance is very task focused. Membership in the Alliance is open and includes private sector vendors (industry) and other interested parties such as government and academia. He did state, however, that the current membership of over 70 is comprised of members from the private sector. There are conferences planned for January, March and June of 2000. The Alliance plans to have their specification proposal completed by the second quarter of 2000. Mr. Chan will be invited back to the Board to present a status update on this activity.

Computer Security Division Update

Ed Roback
Acting Chief, Computer Security Division
National Institute of Standards and Technology

Mr. Roback briefed the Board on NIST's role in computer security **[Ref. 9]**. NIST's mandate in this area is to develop standards and guidelines for the federal government and to improve the competitiveness of the American IT industry. The areas of security standards development include cryptography, policies, management and operational controls, best practices, common criteria, public key infrastructure, and cryptographic module validation. Mr. Roback provided a thorough overview of the Division's efforts in key security standards development, key security testing, new security technologies, and assistance and guidance. He also provided a listing of those entities that the Division works with in carrying out its computer security program. He said that NIST is improving security by raising awareness of the need for cost-effective security. They are engaging in key U.S. voluntary standards activities, developing standards and guidelines to secure federal systems and providing a national leadership role for security testing and evaluation. New efforts proposed by the President include the establishment of an Expert Review Team at NIST to assist governmentwide agencies in adhering to federal computer security requirements. This team will also consult with OMB and NSC on plans to protect and enhance computer security for federal agencies.

Mr. Roback also asked the Board if they would like to recommend any new chapters that could be included in the NIST computer security handbook.

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

Thursday, December 9, 1999

The Chairman called the meeting to order at 9:05 a.m.

Critical Infrastructure Protection: Toward an Effective Research and Development Agenda - An Update

Lt. Col. Steve Rinaldi
Office of Science and Technology Policy
The White House

Lt. Col. Rinaldi updated the Board on the research and development (R&D) agenda to meet the challenges of Presidential Decision Directive 63 (PDD 63) **[Ref. 10]**. He said that key milestones of the PDD 63 include initial operational capability in 2000 and by May 2003 to achieve and maintain capability to protect the nation's critical infrastructures. Looking into the future, the focus will be on the FY2001 budget endgame. The R&D initiatives for FY01 include threat, vulnerabilities and risk assessment, system protection, intrusion monitoring and response, reconstitution technologies, National Information Infrastructure Protection Institute, and a potential future initiative on education. There are plans for workshops on cross-cutting R&D themes such as response, recovery and reconstitution, intrusion detection, metrics and insider threats.

With regard to the establishment of the National Information Infrastructure Protection Institute, the President's Committee of Advisors on Science and Technology (PCAST) has proposed that a non-profit R&D entity, run by the private sector, with federal funding, could meet the challenge of keeping cutting edge CIP R&D relevant and cope with the explosive growth of technology. The Institute for Defense Analyses, under contract to OSD, examined key questions, consulted extensively with government, private sector and academic experts. The OSTP and PCAST sponsored a meeting of chief technology officers to obtain senior technical leadership's perspectives. The general consensus was supportive of PCAST's proposal.

Col. Rinaldi reviewed the management challenges ahead which included ensuring proper R&D coordination among government agencies and keeping up with the rapid march of technology. Meeting the CIP challenge will require an ongoing commitment from the government, private sector, and academia to R&D excellence, and cooperation/collaboration with all partners doing what they do best, will be essential to keep our nation's critical infrastructures secure.

Panel Discussion: Fair Information Practices and Privacy Protection

Robert Gellman, Privacy & Information Policy Consultant
Marc Rotenberg, Executive Director, Electronic Privacy Information Center (EPIC)
George Trubow, CSSPAB Member and Professor of Law, The John Marshall Law School

The panel was brought together to discuss the current role of fair information practices and privacy protection. Mr. Robert Gellman led the discussion. He sees two specific categories: autonomy of decision making and information disclosures The problem with dealing with privacy is that it does not have any clear definition of boundaries. The term "data protection" does give us a grip on what we are talking about, said Mr. Gelman. He sees fair information practices as an organizing theme for the protection of privacy and a checklist for recordkeepers. The principles of fair information practices that he has are openness, disclosure, individual participation, collection limitation, data quality and the principle of finality, security and accountability. Mr. Gellman believes that what has happened is that over the years, fair information practices have overtaken at least the information policy world.

Marc Rotenberg referred to a 1993 Health, Education and Welfare (HEW) report statement of the goal of privacy protection. He believes it to be the best analysis statement yet today. He quoted David Flaherty's statement on the significance of the HEW committee effort and the statement by Justice Michael Kirby on the significance of OECD guidelines in this area. Critical to the success of understanding fair information practices was the ability to understand that privacy protection was the goal, said Mr. Rotenberg. He said that they there is a very high level of common sense behind fair information practices that makes them resonate in the public and political realm. Fair information practices are brief and culturally neutral.

As far as shortcomings of fair information practices, Mr. Rotenberg said that the biggest challenges to their enforcement are about privacy protection and notice and choice. He believes that the results have been a race to the bottom and a lowering of privacy policies.

Mr. Rotenberg believes in the future of fair information practices. He says that they are alive and well and that they will play a significant role in global critical information protection. The real key is their implementation and enforcement. The principles are right, they work, and they have been adopted. The question always is will the safeguard be realized. He said that public awareness is now broader and deeper than it was 25 years ago.

Mr. Gellman said that he doesn't see fair information practices as one size fits all but rather as a policy which will vary. All the same principles will apply but all may not be needed at all times. A criticism of fair information practices is that there is not enough emphasis on disposing of personal records. There should be a policy in place that would expressly address this issue. He also believes that the single biggest problem is the word 'purpose' in use and disclosure. The question is who defines the 'purpose.' Mr. Rotenberg said that there is a study on fair information practices of the top 100 websites that will soon be released. This study does address these types of purpose statements.

Mr. Rotenberg said that there are two very different views of what privacy protection is all about. His view is that fair information practices exist independent of the data subject. Advocates will say that laws are needed. Industry will say that people need to be given information on the market approach. He said that fair information practices give responsibilities to data collectors and rights to data holders. EPIC is pushing to establish anonymity as a baseline for online activity.

Professor Trubow 's concept is one of equitable trust. There is the question of 'source.' There is the idea out there that if you get information from a public source then your right to do with it whatever you want is unlimited. While he does not see any trend in that direction, there is also no ongoing or proposed legislative activity that covers this issue.

Mr. Gellman pointed out that the Europeans talk about privacy as a human right. However, he does not feel that the United States understands it from that perspective. He also said that he does not expect that a national identification card will become a reality. The government should not be the issuers.

Both Mr. Gellman and Mr. Rotenberg believe that fair information practices still have applicability and are still relevant. The open question is still how we go about doing things. The view of the privacy advocates outside of the United States is that we need to update and refine fair information practices standards. However, the view from within the United States is that baseline standard should be in place first.

Board Discussion Period

The minutes from the September board meeting were approved unanimously.

Board Member Karen Worstell informed the board of a metrics project that had been recently launched by ISF and said that the I4 is also working on a metrics project. These contacts will be included in the NIST metrics workshop effort. They reviewed the action items that were due to Fran Nielsen for the metrics workshop effort.

The ‘think piece’ on vulnerabilities proposed earlier by Board Member Guida will be redrafted and Guida will provide an update to the membership at a later date.

The board discussed areas of interest to be pursued at future meetings. They included:

- ACES update
- GPEA update
- Briefing on activities of the office of the Administration’s privacy counselor
- Systems security engineering-capability maturity model briefing/case study
- Y2K postmortem
- Security issues in connection with copyrights
- Update on Trusted Computing Platform Alliance activities

This concluded the business scheduled for the day. Thus, the meeting was adjourned at 1:55 p.m.

References:

1. Nielsen presentation
2. Spencer presentation
3. Johnson presentation
4. Rosenberger presentation
5. Guida presentation
6. S.1993 Legislation
7. Bass presentation
8. Chan presentation
9. Roback presentation
10. Rinaldi presentation

Edward Roback
Board Secretary

CERTIFIED as a true and accurate summary of the meeting

Willis H. Ware
Chairman