COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

The John Marshall Law School
Chicago, Illinois
June 19-21, 2001

Tuesday, June 19, 2001

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

Members present during this meeting were:

Ms. Charisse Castagnoli
Mr. Daniel Knauf
Mr. Steven Lipner
Ms. Sallie McDonald
Mr. John Sabo
Professor George Trubow
Mr. Jim Wade
Mr. Rick Weingarten

Mr. Reeder announced that Board Member Karen Worstell had informed him she is unable to complete her Board appointment term and had submitted her resignation. Mr. Reeder also thanked Professor Trubow for his assistance in arranging for the Board to have their meeting at the Law School facilities.

The entire meeting was open to the public. There were approximately eight member of the public in attendance at the beginning of the meeting.

The first two days of the Board meeting were devoted to sessions on privacy. Board Member John Sabo presented a brief introduction of the format for the sessions. A summary report will be produced and posted on the Board website. The following is a brief synopsis of the sessions.

Session 1: Government Privacy Policies

The first speaker was Mr. Andrew Shen, a senior policy analyst with the Electronic Privacy Information Center (EPIC). Mr. Shen presentation focused on free speech and privacy issues in telecommunications. In his overview of privacy issues he discussed critical infrastructure protection, e-government services, and online access to public records. **[Ref. #1]** The next speaker was Mr. Darrell Blevins, privacy officer at the Social Security Administration. His presentation was on the new challenges for government privacy policies.

Mr. Blevins identified two related issues; efforts to regulate private sector privacy practices and implications for government, and advances in data sharing technology and implications for privacy. Mr. Blevins concluded that widespread government sharing of personal data might soon come under much closer scrutiny. The outcome, he says, is unpredictable. If the government is going to take the lead and be pro-active then there needs to be a program of public education and public relations. There may also be a strong need for a revision of the current Privacy Act to redefine the boundaries. **[Ref. #2]**

The next group to address the Board discussed cross-sectional and cross-agency policies and how to approach the problems. The first speaker was Mr. Lee Zeichner, President of LegalNet Works, Inc. Mr. Zeichner discussed the leadership picture in the age of the Government Information Security Reform Act (GISRA). Mr. Zeichner suggested the Board redefine its mission in light of the GISRA. The Board should define the 'new space' by striking a balance between consumer protection and risk management. Another role for the Board would be to align and harmonize public and private sectors with emphasis on public-provide partnerships. The Board could issue a Call to Action to clarify consumer protection issues, said Mr. Zeichner. **[Ref. #3]**

Mr. William Cook, Partner with Winston and Strawn from Chicago, Illinois was the next to speak. The focus of Mr. Cook's presentation was on critical infrastructure protection and the law. Should the Securities and Exchange Commission require all companies to annually file a compliance statement? What is the role of insurance in setting standards? Mr. Cook said that in the private sector, they have a great impact. Should Congress legislate downstream liability for security failures? Should federal systems face liability for security violations? Currently companies are not inclined to give out information about security policies. It's a competitive advantage and, security through obscurity is still the norm. Mr. Cook presented several legal case examples of causes of actions that were brought before the courts. Mr. Cook reviewed statistical data relating to e-Commerce losses. The losses from a February 2000 DOS attack cost an estimated $1. 2 billion. Insurance companies are obligated to pay for service interruptions. There is also the issue of downstream liabilities such as smurf attacks, spamming through systems related to companies and off-site non-company BBS and chat rooms. In some cases Presidents, Managers, Boards, and System Administrators are held liable for lack of due diligence. Access is also a privacy issue. Denials will be an issue for the Government.

Session 2: Government Privacy Management

Mr. Michael Willett, Senior System Engineer of Wave Systems, Inc. and Chair of the Framework Working Group of the International Security Trust and Privacy Alliance (ISTPA) presented an update on the activities of the ISTPA framework project. Mr.Willett explained that this framework is the first attempt to define privacy services relationship to security services. It will be useful for policymakers and IT architects. This is trust at the edge of the network. The pyramid of protection covers software only; tamper-resistant software; tamper resistant firmware; hardware – static; hardware program and hardware/software cryptographic systems. It's a privacy framework that has been built to have some security integration as part of it.

The second speaker for Session 2 was Mr. Ari Schwartz, a policy analyst with the Center for Democracy and Technology (CDT). Mr. Schwartz's presentation on was Platform for Privacy Preferences (P3P) and its value as a privacy enhancing technology and its value to the government. The P3P idea came about four or five years ago to address what people wanted to see in the area of privacy on the web. The CDT is focusing on building policy requirements into the technology. This can be accomplished by the use of the power of the web to enhance notice, enable better consent mechanisms and ensure more consumer choice, building a framework for global privacy and having a common vocabulary that can translate the 'legalese.' Mr. Schwartz commented that there were already over eleven websites making use of P3P. Using P3P within the federal government will help to build trust in the government and their websites. It is consistent with the Privacy Act and subsequent policy. It would allow agencies to highlight notice and the ability to point to legal protections. More information on P3P can be found at http://www.w3.org/P3P.

The third speaker for Session 2 was Judy Droitcour, Assistant Director, Office of Applied Research and Methods at the General Accounting Office (GAO). Ms. Droitcour briefed the Board on an April 2001 GAO report covering records linkage involving person-specific data conducted under federal auspices to generate research or statistical information. **[Ref. #4]** Record linkage has flourished with technological advances and the growing recognition of 'linkage power." Privacy issues are relevant because linkage occurs at the person level and new data on individuals is created. Ms. Droitcour discussed issues such as how record linkage generates new statistical and research information, why record linkage heightens privacy concerns, what tools might be helpful in building a privacy protection toolbox and how data stewardship strategies might enhance linkage privacy. Ms. Droitcour identified other issues that could be studied further. They included: scope of federal linkage efforts; barriers to linkage, legal and regulatory frameworks for linkage, advantages/disadvantages of various privacy-protection techniques, the possible need for other kinds of techniques and identification of criteria for "best practices" in data stewardship.

The fourth speaker for Session 2 was Drummond Reed, Founding Director of XNSORG and Chief Technology Officer of OneName Corporation. Mr. Reed's presentation was on XNS – Extensible Name Service and XNSORG and the implications for government. **[Ref. #5]** Mr. Reed reported that Extensible Name Service (XNS) is a new global communication service that makes it easier for people and businesses to exchange, protect, and synchronize data than ever before. It solves problems such as identify, privacy and data protection, data exchange and synchronization by its web agent linking technology, XML document structure and a global network of agents and agencies.

Mr. Reed also presented an overview of the XNS Public Trust Organization (XNSORG). The XNSORG is an independent non-profit standards body that establishes XNS technical and operational standards. It manages the XNS root agency and oversees the XNS general namespace as well as serves as the XNS education and communications hub.

In his review of the XNS and the ISTPA framework relationship, Mr. Reed said that XNS encompasses eight of nine services in the privacy framework. XNS supports the legal relationships that provide accountability for data protection and XNS privacy contract vocabulary meets the jurisdiction requirements. XNS is an open, vendor-neutral, platform-neutral standard.

The web site address for XNSORG is www.xns.org.

The fifth speaker for Session 2 was Peter Reid, Partner in the privacy practice of Fiderus. Mr. Reed's presentation addressed the topic of auditing web sites for privacy violations. **[Ref. #6]** In his introduction, Mr. Reed explained that Fiderus is a consulting company that focuses totally on security and privacy. Fiderus has an established partnership with IDcide and is using the IDcide Privacy Wall products to provide comprehensive web site privacy vulnerability assessment services. Mr. Reid briefed the Board on the functions of the IDcide PrivacyWall™ product. Collection of sensitive or identifying personal information through the web site, COPPA violations, non-secure transmission of personal information, accidental identification of supposedly anonymous personal information through improper use of cookies are several examples of types of violations that are commonly detected. Mr. Reid said that many of these violations are not intentional but the results can be just as devastating resulting in negative media coverage, loss of trust and law suits. In his conclusion, Mr. Reid stated that the Fiderus service provides a comprehensive web site audit capability to quickly and easily detect privacy violations on any web site.

The last two speakers of Session 2 were Mr. Marty Staks and Mr. Brett Williams of Andersen, LLP. The discussion topic was privacy audits – state of the art view from the community. Their major involvement is with the security side of auditing rather than the legal/policy side. Both Mr. Staks and Mr. Williams are members of Anderson's internal protection working group and they work more in the area of EU and Safe Harbor issues. They highly recommend that organizations make privacy a part of their business strategy. Questions they ask their clients include where does privacy and data protection fit as part of the business strategy, what is the relationship to maintaining customer relationships and what is the cost of having a privacy program versus the risk of not having one? Mr. Staks reviewed the fundamentals of an audit and the current regulatory landscape. He also shared his concern about the limited level of knowledge of privacy officers overall. The government serving as a role model is tenuous. Recent reports indicated that 23 federal agencies still have 'cookies' on them as well as lack privacy policy statements on children's sites. These types of situations make it difficult to for the government to be a good example. Mr. Staks and Mr. Williams recommended that delay is a major factor in implementing privacy regulations. They believe that the right thing to do is to promote the good things that have taken place.

The Chairman recessed the meeting at 5:30 p.m.

Wednesday, June 20, 2001

The Chairman resumed the meeting at 9:10 a.m. The meeting continued with privacy presentations.

Session 3: Privacy and the Citizen

Professor Leslie Reis, Director and Adjunct Professor of Law of the Center for Information Technology and Privacy Law at the John Marshall Law School arranged for the Board to observe a moot court exercise on a privacy/citizen case. Law students Desiree Berg and. Brian Williams served as the attorneys who presented the case of Mr. Blanco C. White versus the State of Lincoln Bar Association. The questions presented to the Court were (1) did the Supreme Court of Lincoln err in upholding the State Bar of Lincoln's denial of Mr. White's application for admission to the Bar where the denial restrained Mr. White's First Amendment rights to free association and free speech; and (2) did the Supreme Court of Lincoln err in finding that the Fourteenth Amendment was not violated when the State of Lincoln denied Blanco White's application for admission to the Bar. Acting as Judges on the bench were Professor David Sorkin and Adjunct Professor David Laudy. The exercise concluded with the Board members having an opportunity to interact with the participants with follow-up privacy question.

Megan E. Gray of Baker and Hostetler LLP was the next speaker. **[Ref. #7]** Ms. Gray presented three snapshots of citizens and their government in the online era; online court records, computer-accessible government databases and the rise of identity theft. On the subject of on-line court records, Ms. Gray stated that she believed that anonymous access to on-line court records should be required. She believes it to be a fundamental right. Ms. Gray stated that journalism studies show that current public information is, in fact, restricted, for example, giving your name, showing identification and identifying why the information is being requested. Risks associated with ubiquitous on-line access are misattribution and data integrity. Ms. Gray reported that there is a Judicial Conference that is considering some on-line access proposals. They include proposals that would make whatever a court has available online; that a subset of court records would be available online, that there could be full access but only in the Courthouse, and that there be no online access granted. Ms. Gray reported that some courts are taking criminal records out of their databases. Since courts move slowly, Ms. Gray believes that it is important to put the framework in place now.

On the topic of computer-accessible government databases, Ms. Gray reported that various laws regulate the government's collection and use of personal data. None of these laws is entirely effective. The government has to obey a patchwork of laws, regulations, and policies that aim to protect citizens' privacy. Ms. Gray reviewed several of the current privacy laws that are currently in place to improve the security and privacy of sensitive information in federal computer systems. Computer-accessible government databases foster a better-informed public. However, federal agencies are not very good at controlling database access. Ms. Gray cited a September 2000 General Accounting Office report that stated 97% of federal web sites failed to adhere to four basic privacy principles recommended by the Federal Trade Commission (FTC). These principles were notice, choice, access and security.

The last topic Ms. Gray discussed was identity theft. Ms. Gray stated that the more that computerized databases are networked, the easier it will be for ID theft to occur. The FTC's recently installed hotline has logged an average of 2,000 calls per week reporting crimes of identify theft. While there are laws against identity theft, to stop identity theft there must be continual improvement of electronic-security measures and educations of people to protect their sensitive information.

The next speaker in Session 3 was Helen Foster, an attorney from the Bureau of Consumer Protection of the Federal Trade Commission (FTC). The FTC has jurisdiction over deceptive acts and practices, by authority of the Identity Theft and Assumption Deterrence Act of 1998. Identity theft relates to obtaining or transferring any single or multiple element of identification that a person acquires without lawful authority with the intent to commit or abet a crime. Ms. Foster's presentation outlined the components of the identity theft program at the FTC, described the information that they collect and how that information is used and shared. Other FTC initiatives in ID theft were also discussed. **[Ref. #8]**

Following the session, Board Member Rick Weingarten led a discussion with the members to review the presentations that were given the first two days of the meeting and to determine what actions the members may want to take as a result of the information that they had received.

The meeting was recessed at 5:00 p.m.

Thursday, June 21, 2001

Chairman Reeder reconvened the meeting at 8:30 a.m. Mr. Reeder acknowledged that this was the last Board meeting for Professor George Trubow. The Board expressed their gratitude to Professor Trubow for being instrumental in arranging for the meeting to be held at the John Marshall Law School. He was also lauded for his many contributions to the Board during his tenure as a member.

The minutes of the March 2001 meeting of the Board were unanimously approved.

After recapping the privacy presentations, the Board discussed actions/activities that they could consider pursuing.

- Address pending legislation and make recommendations (including dissenting opinions);
- Establish a position on need for a governance model of a privacy "entity" or agency. Adopt a "tiered" strategy recognizing the best approach may be incremental. Consider proposing a Privacy Officer Board as a first step. Address the CIO Council role in enabling a formal privacy officer communication policy coordination mechanism.
- Address issue of "differential access" to information as a way to limit the potential excesses and threats that are caused by digital, networked databases and access.
- Draw attention to national databases and linkages issues in light of the Privacy Act of 1974 and other legislation.
- Consider proposing there be research projects on the mapping of data sharing/databases in federal/state and local government and linkages to the privacy sector;
- Address Notice and Consent issues.
- Address private-public sector converging technology and policy models. Technology developments such as ISTPA Privacy Framework, XNS, P3P, underscore the importance of working with private sector to make use of new technology and tools in government environment where appropriate.
- Ask the Office of Management and Budget to identify Privacy Officers in federal agencies, including organizational level, authorities and responsibilities.
- Address Identity Theft issues. The Federal Trade Commission's legal definition of ID theft is so broad that the FTC is unable to get a good grasp on the issue. The Board would like to see more data on remedies offered and assistance given to the victims.

A follow-up discussion on this two-day privacy session will take place at the September Board meeting. A report of the event will also be assembled and made available on the Board web site.

Board Discussion on Work Plans for Baseline Standards

Board Member Steve Lipner presented a proposed outline for conducting a baseline security controls event during the September Board meeting. The focus of the event will be on learning from federal agencies what baseline security controls they have in place. From the input the Board hears presented, they hope to possibly identify a list of recommended baseline controls and document their findings in a brief report that could be forwarded to federal agencies and publicized on the Board web site. Mr. Lipner will work with Dr. Fran Nielsen to develop an appropriate outline and agenda for this event to be held in September.

Critical Infrastructure Assurance Office (CIAO) Update

Mr. Robert Miller, Deputy Director of the CIAO, presented an update on the activities of the CIAO. The CIAO was created in 1998 as a result of the then PPD #63 and was set up as a planning secretariat with additional functions. Over the past two years two new program areas have evolved. The first program area is public-private partnerships and the second program area is an internal effort, Project Matrix. Mr. Miller said that their outreach goals are to change the discussion of critical infrastructure protection (CIP) beyond discussion of firewalls and technological solutions. The CIAO is stressing that technology protection is a management issue. The Project Matrix effort focuses on the civil side of government to help agencies develop a process of identifying vulnerabilities and prioritizing investments. Mr. Miller reported that the Securities and Exchange Commission and the Departments of Commerce, Energy, Health and Human Services and Treasury have already been reviewed.

Mr. Miller reported that the new Administration is fully engaged in the CIP effort. The CIAO is expected to continue reside at the Department of Commerce. As a result of the Administration's national security views, Mr. Miller said that it is expected that there will be a tighter coupling of critical infrastructure protection, information assurance and counter terrorism. Resources may be slightly increased in this area, but not greatly enlarged. In the area of transnational issues, Mr. Miller noted that it remained uncertain whether the United States would seek ratification of the Council of Europe Cybercrime Treaty.

Version 2.0 of the National Plan is moving forward. Mr. Miller said that the Partnership for Critical Infrastructure Security (PCIS) is taking a major role in developing the next version. This version is expected to be available by the end of 2001. It will cover some broader issues as well as the transnational issues.

Congress recently established an Institute for Security. The Institute is being hosted at Dartmouth and headed by Michael Vatis. The National Institute of Standard and Technology also received Congressional approval to establish a $5M grants program and CERT-like effort [C-SEAT]. Mr. Miller said that he thought that the CSEAT effort will be very useful and fill in a lot of voids. The National Infrastructure Protection Center (NIPC) effort is part of the landscape and will be for the foreseeable future.

Mr. Miller spoke about the PCIS and recommended that the Board develop a relationship with this group.

Update on Federal Bridge CA and the Federal PKI

Ms. Judith Spencer, Chair of the Federal PKI Steering Committee, briefed the Board on the current status of the Federal Public Key Infrastructure (FPKI). **[Ref. #9]** Ms. Spencer reported that the FPKI Policy Authority approved final documentation on June 18, 2001, for certificate policy; certification practices statements and compliance analysis. The Federal Bridge Certificate Authority (FBCA) is open and ready for business and is located at the GSA/FTS Willowoods facility. The FBCA is being operated by Mitretek Systems. The next steps the Steering Committee plans to undertake include working with federal agencies to achieve interoperability (for example, initial cross-certifications with NASA, USD/NFC and FDIC), bringing additional products into the Bridge membrane by working with RSA, Cylink and Spyrus, pursuing interoperability with State PKI's and pursuing interoperability with Canada.

Ms. Spencer also briefed the Board on the access certificates for electronic services (ACES). ACES has already being implemented at the Environmental Protection Agency, the Federal Emergency Management Agency, the National Institute of Standards and Technology and the Social Security Administration.

The leaders today in the Federal PKI effort are the Department of Defense, the Federal Aviation Administration, the U.S. Patent and Trademark Office, the U.S. Department of Agriculture National Finance Center and the National Aeronautic and Space Administration.

In addition to establishing federal agency cross-certification with FBCA, other current initiatives include State interoperability and international interoperability. They also anticipate issuing electronic records management guidance by September 2002.

Update on OMB Computer Security Activities

Ms. Kamela White of the Office of Information and Regulatory Affairs in the Office of Management and Budget briefed the Board, via a teleconference, on OMB activities in the computer security area. Ms. White announced that Mr. Mark Foreman, formerly with UNISYS, will oversee privacy issues and he will be responsible for e-government funds, the CIO Council and other agency councils that are similar to that.

As a result of the passage of the Government Information Security Reform Act (GISRA), OMB issued guidance on implementation of the Act. This guidance included instructions on the new reporting requirements of annual agency program reviews. There are 13 topics that agencies must comply with. These annual reports are due to OMB in September. The Act also requires that the Inspectors General of each agency perform an independent evaluation of the agency programs. Ms. White indicated that executive summaries of the agency plans will be made available as part of a report that OMB plans to issue.

Ms. White reported that the Lieberman legislation (S. 803 – E-Government Act of 2001) was moving. However, OMB had not released their opinion on that issue at this time. If and when the Administration's position is made known, Ms. White will inform the Board.

A hearing was held on June 21, 2001, on the Government Paperwork Elimination Act (GPEA) to discuss where agencies were in the process of automating as required by GPEA's 2002 deadline. In his testimony, the OMB Director named those agencies that were not on schedule.

Ms. White informed the Board that there was a new draft executive order in the works that would cover the issue of coordinating security within the federal government. The Board will be kept informed as this matter progresses.

Public Participation

There were no requests from the public to speak at this time.

Discussion of Board Agenda for September 2001 Meeting

In addition to the two-day event on baseline security controls the Board plans to discuss the following topics:

- Updates on the June privacy event
- Work plan discussions on GPEA and governance
- Tools and strategies for the Board
- Discussion of holding quarterly Board meetings; options of virtual meetings, subcommittee meetings, etc.
- Identify theft topic to be schedule for December meeting timeframe

There being no further business, the meeting was adjourned at 2:40 p.m.

Ref. 1 - Andrew Shen presentation
Ref. 2 – Darrell Blevins presentation
Ref. 3 – Lee Zeichner presentation
Ref. 4 – Judith Droitcour
Ref. 5 – Drummond Reed
Ref. 6 – Peter Reid
Ref. 7 – Megan Gray
Ref. 8 – Helen Foster
Ref. 9 - Judith Spencer

Fran Nielsen
Board Secretary

CERTIFIED as a true and accurate
summary of the meeting.

Franklin S. Reeder
Chairman