INFORMATION SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

The Hyatt Regency Bethesda
One Bethesda Metro Center
Bethesda, MD

March 16-18, 2004

Tuesday, March 16, 2004

Board Chairman, Franklin S. Reeder, convened the Information Security and Privacy Advisory Board Meeting (ISPAB) at 8:30 a.m. In addition to Chairman Reeder, Board members present were:

Lynn Bruneau
Richard Guida
Morris Hymes
Susan Landau
Rebecca Leng
Steve Lipner
Sallie McDonald
Leslie Reis
John Sabo

The meeting was open to the public. There were five visitors present at the beginning of the meeting.

Chairman Reeder offered congratulations to Board members John Sabo and Bruce Brody on being the recipients of a Federal IRM 100 Award, an annual award recognition presented to them by *Federal Computer Week.*

Session on CRM Activities

Board member, Leslie Reis, presented an overview of the project activity on customer relationship management (CRM), the purpose of the activity and the expected outcome of the session following the presentations. Professor Reis also extended her thanks to Adam Hicks, a John Marshall Law School Research Associate, and Board Secretariat staff, Elaine Frye, for their assistance in organizing this work effort. Mr. Hicks will be assisting Professors Reis with the development of a draft white paper on the CRM topic.

The first participant in the session was Dr. Larry Ponemon, President of the Ponemon Institute. Dr. Ponemon presented a briefing on the recently issued Ponemon Institute 2004 Privacy Trust Survey. **[Ref. #1]** Dr. Ponemon said that they believe that there is a strong positive correlation between the public's perception and extant practice. Good privacy creates good value for organizations because it promotes the trust of the stakeholders such as employees, taxpayers, customers, and organizational partners.

The Privacy Trust Survey focused on people's perceptions concerning the privacy commitment of the U.S. governmental departments, agencies and other federal organizations that are known to collect and use the public's personal information. Privacy trust was defined by two categories:

personal information and privacy commitment. Personal information was considered data about yourself and your family. Privacy commitment was considered obligation of the specified government organization to keep your personal information safe and secure. This included the commitment not to share individual personal information without a just cause or without obtaining proper consent to do so.

Initially, an expert panel created a grand list of 102 U.S. government entities that they identified as collecting and using the public's sensitive personal information. Fifty-three of these organizations did not overlap any of the others. Next, a focus group reduced these 102 to 60 based on the level of privacy concern about the governmental organizations' use of personal information and the belief that the organization collected and used personal information about them or their families. A pilot sample survey of 305 adults using the Web only tested the survey reliability and internal validity of the process. A full sample of 6,313 adults completed a revised survey using confidential channels via the Web, paper and telephone. The results were also broken down by percentage of responses by geographic region and age of respondents.

Dr. Ponemon said that survey results revealed that the government organization with the highest privacy trust score was the U.S. Postal Service, while the Justice Department/Office of the Attorney General scored the lowest. The government organization with the lowest uncertainty level was again the U.S. Postal Service and the Small Business Administration was identified having the highest uncertainty level. Other findings identified by the survey included the public's skepticism about the privacy commitments made by government, especially in the areas of law enforcement and homeland security. Many people expressed concern that the government had lessened privacy protection to enhance its national security agenda that impacts individual freedom and civil liberties.

Mr. Bill Ferguson, Executive Director of Carnegie Mellon's CIO Institute, collaborated with Dr. Ponemon on the Privacy Trust Survey. Mr. Ferguson said that they are aware of the Office of Management and Budget's impact assessments and he and Dr. Ponemon will be looking into the possibility of having a survey compiled that would reflect the impact of these assessments.

Internal Revenue Services (IRS) CRM Activities

The next to speak was Ms. Mary Ronan of the Office of the Privacy Advocate at the IRS. The IRS has a varied and wide amount of interaction with their customers. They include over 138 million tax filers, their dependents, the CPAs, attorneys, enrolled agents, tax return preparers, and volunteers who prepare taxes for free. There are also more than 100,000 employees and contractors working within the IRS. The Privacy Advocate Office role is to balance the collection of the minimum amount of personal information and make sure that the information collected is correct. There are several legal statues in place that mandate how the IRS deals with taxpayers. Another narrow definition of real customers is the people such as the practitioners, those who do taxes or financial accounting, perform analyses or give advice for a fee. The IRS's Office of National Public Liaison is primarily responsible for the practitioner community. They conduct tax forums several times a year. The IRS also goes on the road and briefs on what's new at the IRS. Privacy has been on the agenda of these forums over the last three years. They have a strong advocacy for encouraging electronic filing across the country. Their goal is to have 80% of all returns filed electronically. The IRS has also produced an entire series of email messages, newsletters, etc. for the practitioner covering what has changed in the IRS over the last year.

Ms. Ronan said that the IRS privacy statement is that they will collect only that information that they need and that the IRS's job is constantly being defined and the public is not always aware of this. With regard to the use of contractors at the IRS, Ms. Ronan stated that the IRS does background checks on all contractors, requires systems to have audit trails and the Inspectors General of Treasury review the audit trails via a safeguard unit that performs onsite inspections.

Ms. Ronan addressed several IRS CRM initiatives that had been eliminated such as customer service people wanting the permission to tape the phone conversations of the callers without informing the customer. This was denied principally because of the government's wiretapping statutes. The IRS is also looking at the renewal/revision of Section 7216 of the IRS Code that deals with practitioners. The transmittal of tax information to and from the IRS from filers living abroad is another issue under review.

Mr. Reeder thanked Ms. Ronan for her briefing to the Board.

U.S. Postal Service (USPS) CRM Activities

Ms. Zoe Strickland, Chief Privacy Officer, Mr. Ken Ceglowski, Manager, Customer Relations Management and Ms. Emily Andrews, Privacy Programs Specialist of the U.S. Postal Service presented the next briefing. **[Ref. #2]** Ms. Strickland stated that the Postal Service sees CRM as treating different customers by knowing what needs they have and how to meet those needs. Customer service enhancement is one of the major initiatives of the USPS as the use of the Internet moves toward taking business away from the USPS. In 2002, a business case was developed for customer ID solutions integrating corporate solutions. Ms. Strickland said that the current customer data management capabilities at the USPS present significant business challenges for both the organization and its external customers. The customer ID (CID) that they developed is a repository of customer identification data that is used to match and cross-reference customers across multiple USPS business systems. The CID service identifies customers across multiple systems, cleanses, standardizes and matches customer records, creates a unique identification of a customer, and is the corporate-wide solution for customer identification. A customer is identified as any business entity or individual person at an address who utilizes a paid service of the USPS. The CID is consistent with USPS architecture, privacy and security, hardware and software. A key goal of the CID integration approach is to minimize the imposition on existing business systems. The benefits of CID will be realized through further integration with other key initiatives such as customer gateway and sales initiatives and privacy.

Ms. Strickland clarified their project activity stating that CRM typically applies to the voluntary databases as opposed to individual mail distribution. The benefits to the users were identified as data accuracy, service such as convenience and ease of use and access across channels, and customer choice to opt in or opt out. Ms. Strickland noted that USPS follows the OMB guidance on Privacy Act compliance.

Ms. Emily Andrews, Privacy Programs Specialist, addressed the Fair Information Practices that must be followed throughout all of the channels the USPS works with, i.e., online, phone, mail, and retail areas. Practical implementation issues that they deal with include limited budget, numerous customer forms, numerous collection systems of various age/size, non-integrated use and sharing of customer information and lack of knowledge about privacy inquiries across channels.

Mr. Ken Ceglowski, USPS Customer Relations Manager, spoke on the topic of the customer gateway and why it is necessary. The USPS has an opportunity to drive down costs while making it easier for customers to do business with them. The four key characteristics of the customer gateway are design and navigation, customer experience, single point-of-access and customization and personalization. These characteristics translate into benefits to both customer and the USPS. Accomplishments to date include the launching of the gateway in June 2003, enabling of customer service (iBSN) in August 2003, enabling of consolidated mail tracking and reporting in September 2003, start of single sign-on solution and initiation of definition of personalization requirements. Next steps include new real-time automated on-line registration process, enabling of single sign-on, development and building of enterprise capabilities and implementation of customization and personalization.

Mr. Reeder thanked the group for their presentation. Ms. Strickland commented that she would like to see if there are ways that they (USPS) could work mutually with the Board on CRM efforts within the USPS.

Overview of ACCENTURE CRM Project

Mr. Richard Hauf, CRM Core Team Member with ACCENTURE presented an overview of their recent study on CRM in Government. CRM is a capability that allows government to dramatically improve its relationship with its customers through re-organizing services around customer intentions. CRM constitutes a more comprehensive, methodical approach to providing services that would have traditionally been pursued in separate, ad hoc ways.

Mr. Hauf said that recent government services have identified a significant uptake of CRM concepts and principles, as well as a convergence of CRM and e-government initiatives. Key findings include government thinking of the people they serve as their customers. Government is embracing the fundamental principles of CRM, i.e., CRM underpins e-government, e-government decisions that are driven by considerations of values. While agencies have embraced the fundamental principles of CRM, they are struggling to put the building blocks of customer insights, customer offerings, customer interactions, organization performance and networks, solidly in place. CRM underpins all successful e-government. It allows the relationship between government and customer to be reinvented; the term 'customer' is gaining currency while superior service becomes more important. This is not 'service at any cost.' Investment up front will lead to savings over time.

When asked to define CRM as a concept, Mr. Hauf responded that CRM is the process and content and the information required to deliver customer service.

Health Care Community CRM Activities

Mr. Rich Guida, Board Member and Director of Information Security with Johnson & Johnson presented the health care community perspective on CRM activities. In examining the environment of CRM in the health care community, Mr. Guida pointed out that there is an extremely diverse customer base. The rules on selling, buying, pricing and privacy differ from country to country and state to state. Competitive pressures apply especially where customers purchase from multiple suppliers. When dealing with doctors and hospitals, patient privacy requirements apply. Likewise when you are dealing with clinical research where anonymity on clinical trial data is sought. An overarching principle is that the impairment of the relationship with a customer is not a good thing. For example, Eli Lilly exposed hundreds of users of the drug Prozac over the Internet. Competitive pressure thus helps ensure that the data holder acts responsibly. Information that is typical managed as CRM covers the areas of specialization, buying records/habits, product interest and scope. The data is not managed on line over the Internet. Even if the information is on the Intranet, it's access is typically very strictly controlled. The data is used to tailor customer interactions, predict sale, and look for new market opportunities. Groups such as the call center personnel, sales force personnel, government and other internal users will have knowledge of the information collected. The degree of knowing the customer is set in part by what the customer can tolerate or what the customer prefers. Tolerance is sometimes imputed rather than overtly expressed. If you really know your customer, you know what is acceptable; for new customers it can be challenging. Outsourcing is commonplace and is increasing. Overall, it is not viewed as a serious risk. Mr. Guida's final point addressed the use of radio frequency ID (RFID) tags. While RFIDs may be relevant to CRM over time, that is currently not the case since the practice is not widespread.

The meeting was recessed for the day at 4:55 p.m.

Wednesday, March 17, 2004

The Chairman reconvened the meeting at 8:30 a.m. Board member Susan Landau opened the meeting with an overview of the session on the NIST Computer Security Division (CSD) funding effort. Other participants in this session included Christopher Hankin, Director of Federal Affairs for Sun Microsystems, Steven Adler, Marketing Manager for Privacy and Compliance with IBM Tivoli Security and Privacy and Richard Guida, Director of Information Security with Johnson & Johnson. Dr. Landau presented a brief history of the Division and the mandates given to it by the Computer Security Act of 1987. She praised NIST for their success efforts in the Data Encryption Algorithm/Advanced Encryption Standard activity. Dr. Landau especially applauded how NIST works with outside industries. It was also noted that the Division has been invaluable in the PKI and role based access areas. Mr. Reeder shared the view that funding for the computer security research program at NIST has been inadequate and NIST should do a better job of marketing their good work. Dr. Landau called on the panelist to offer their views.

First to speak was Mr. Hankin. He acknowledged that SUN lobbied to make certain that the Division did not get moved into the Department of Homeland Security, recognizing that the outcome for monetary funding for the Division may be put at risk. Mr. Hankin noted that the FY04 NIST budget problem was a problem across the entire NIST program and not just the Division program. He referred to a March hearing that was held by the House Science Committee at which time forty lobbyists rallied to demonstrate their concern for the NIST budget shortfalls and raise the issue to the Presidential level. Mr. Hankin stated that there was no NIST champion currently in Congress, and more specifically, there was no champion for the Division's program. SUN has done their own survey in-house of the value of the Division's work to SUN. The survey data will be shared with the Board. It is important to SUN that there be a government-to-government entity when dealing with US interest. Interoperability testing is one area that NIST does best. Other positive output from the Division have most certainly been observed in the cryptography area and the smart card and biometrics areas. Mr. Hankin believes that NIST/CSD needs to do a better job at promoting themselves, especially to get the notice of Congressional appropriations committees.

The next panelist to speak was Rich Guida. Specific areas of research that are important to the health care community are the cryptography and security standards. These standards are invaluable to the computer security protection of patient personal information [HIPPA] and electronic signature [FDA] areas. For example, good cryptography is essential in clinical trials and results in saving patient lives because the data can be processed more efficiently and drugs can hit the market sooner. Getting the word out as to how valuable and recognized NIST standards are is occurring more frequently as many former government employees begin second careers and bring their trust marks with them into the industry arena.

Steve Adler was the last panelist to speak. Mr. Adler also referred to the branding challenge of NIST not selling themselves too well. He noted that the SPAM workshop that was held in February was an excellent example of raising the seriousness of the SPAM problems. The workshop added a great deal of value to the issue that industry could not lay out. He encouraged NIST to play the catalyst for other issues and provide the leadership to bring everyone to the table and look at the ways to arrive at resolutions to these issues. It was also noted that NIST mission statement speaks to both computer security and privacy. However, nothing appears on the CSD website that refers to any effort that the Division is doing in the privacy arena. Mr. Adler said that he is seeing many privacy and security regulations in the personal data protection area and that information technology standards are lacking in the area of protection of privacy of personal data.

Following Mr. Adler's briefing, the Board members shared their views with the panelists. Board member Rebecca Leng noted that integrity of the data is missing in the government. The E-government Act has a new requirement that privacy impact assessments (PIA) be done when it involves the collection of personal data. The definition of a PIA is different across industry and government. The question is what should the benchmark be and who in government would develop such a benchmark.

Board member Morris Hymes reminded the Board that there is a strong partnership between NSA and NIST in the PKI, biometrics and NIAP areas. NSA is able to bring the intelligence piece of the business into play.

Because of the legitimate missions of critical protection of homeland security, there is the need to create a structure that can be one voice that is not drowned out by the whole, commented Chairman Reeder. The Board should ask themselves these salient questions: is there a problem, what is the nature of the problem and what can the Board do to provide a path to bringing the issue to the attention of those who could do something about the issue.

Board member Steve Lipner stated that more resources and consistent resources are part of the solution to the problem, while not the entire solution. He believes that there is a lack of understanding and a need for well-guided efforts because there are different demands and requirements by the civilian agencies.

NIST continues to do its foundation/engineering work, said Board member John Sabo. The people making the funding decisions are not that computer security educated. NIST needs to link what it is doing in its foundation work to the outside world. Private sector information centers already exist and none of them have adopted any common security standards. The private and public sides are spending a great deal of money on this issue.

Board member Susan Landau said that the private sector that is using NIST standards the most is the pharmaceutical and banking industries. She expects that this movement to NIST standards will spread into other area of the public sector.

Board member Rebecca Leng commented that the environment has changed in light of the FISMA and CSD should focus more on the management of computer security issues as opposed to technical issues. She noted that more than one-half of government agencies reported computer security as a material weakness. Leng suggested that NIST help federal agencies with this problem by assisting them with information on how to properly implement the standards that are already available to them.

Board member Morris Hymes commented that NIST is particularly under funded in the NIAP area. He said the Board should put that issue on the table. He also suggested that the Department of Homeland Security create its own Memorandum of Understanding with the Computer Security Division, that the Board seek out OMB help's to follow up with compliance of those standards already implemented. He also pointed out the seriousness of technology rollover and the length of time it takes to develop FIPS to cover the latest technological issues.

Mr. Adler suggested that perhaps the mission statement of the Division might be too broad or too narrow. The demonstration of the value issue is missing. It should show how to implement the technical specifications, what the architecture is, what the management guidelines are, implementation scenarios, use cases for public and private sector and once deployed, what the values look like.

The Board agreed that they would develop a draft report and transmittal letter on the issue. Board member Susan Landau discussed a draft outline for the proposed report. A draft will be prepared and forwarded to the members for discussion and action at the June meeting.

The next item of business was the adoption of the minutes of the December 2003 Board meeting.

Briefing on DOD/DHS Review of the NIAP Program

Dr. Greg Larsen of the Institute for Defense Analysis briefed the Board on the program review they performed on NIAP. **[Ref. #3]** The National Strategy to Secure Cyberspace called for a comprehensive review of NIAP. The general approach was to develop the facts, information, arguments, and recommendations concerning what NIAP must be, what NIAP is, what NIAP could be and what NIAP should be. The report had four major tasks: to characterize the National intent, NIAP implementation, and stakeholder expectations, conduct fact-finding, and develop issues. Other objectives were to assess impacts of selected issues and generate alternatives and options to address these issues; analyze selected issues/options and, to provide recommendations. Dr. Larsen reviewed the sample questions asked during the review and the status of the activities performed. Dr. Larsen requested that the Board members consider participating in this activity as interviewees and welcomed identification of any other people with knowledge of the NIAP program as potential interviewees.

Board Discussion

Ed Roback, Chief of the Computer Security Division updated the Board on the March 16, 2004 hearing held by Congressman Adam Putnam on the agencies computer security report cards by. The DOC representative testified about other activities that it could do if NIST received additional funding. They also testified has to how the Division had reprioritized to meet the new FISMA requirements given to it. Two specific areas raised as important to Congressman Putnam were the issue of governance within the agencies and more accurate and more complete inventories of IT assets by agencies.

Mr. Roback also shared the following observations and updates with the Board. The NSA/NIST technical working group activity has enjoyed excellent crypto relations over the past five years. On the matter of extending or broadening this activity to include others outside of the government,

Mr. Roback noted that there might be some difficulty in complying with the Federal Advisory Committee Act to accomplish this. In the area of international negotiations, NIST is constantly asked to participate but funding shortages hinder such participation. With the Advanced Encryption Standard in place, the Data Encryption Standard (DES) will be withdrawn. The DES will continue as a federally approved algorithm but not as a Federal Information Processing Standard (FIPS). The Triple DES will be preserved. FIPS waivers are no longer allowed under FISMA.

The meeting was recessed for the day at 5:00 p.m.

<u>Thursday, March 18, 2004</u>

The chairman reconvened the meeting at 8:35 a.m.

Board Discussion Period

The Board reviewed the activities of the previous two days of the meeting. They also discussed the agenda topics for the June 2004 meeting.

Chairman Reeder encouraged the members to come prepared with their recommendations for the work plan discussion to be held at the next meeting. Three criteria of what they should consider are: first, is this an important question that someone wants an answer to, i.e., is there a client; second, is the Board, by authority and composition, in a position to offer some constructive advice or value on the issue at hand; and third, is there critical mass on the Board of members willing to pursue the topic.

As there was no further business, the meeting was adjourned at 11:51 a.m.

Ref. 1 Ponemon presentation

Ref. 2 USPS presentation

Ref. 3 Larsen presentation

Joan Hash
Board Designated Federal Official

CERTIFIED as a true and accurate
summary of the meeting.

Franklin S. Reeder
Chairman