INFORMATION SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

DoubleTree Hotel and Executive Meeting Center
1750 Rockville Pike
Rockville, MD

September 13-15, 2005

Tuesday, September 13, 2005

Board Chairman, Franklin Reeder convened the Information Security and Privacy Advisory Board Meeting (ISPAB) for its third meeting of the year at 8:45 a.m. Other members present during the meeting were:

Bruce Brody
Daniel Chenok
Morris Hymes
Susan Landau
Rebecca Leng
Steve Lipner
Sallie McDonald
Lynn McNulty
Leslie Reis
Howard Schmidt

Chairman Reeder introduced the new member designate Joseph Guirreri of Computer Associates located in Herndon, Virginia. It was also announced that Ms. Pauline Bowen of the National Institute of Standards and Technology's (NIST) Computer Security Division was the new Federal Advisory Committee Act Designated Federal Official replacing Ms. Joan Hash of NIST.

The meeting was held in open public session. There were eight members of the public in attendance during the meeting.

SCADA Briefing

Mr. Keith Stouffer of NIST's Manufacturing Engineering Laboratory updated the Board on NIST's industrial control system security activities. **[Ref. #1]** He reviewed the different performance requirements, reliability requirements, risk management requirements of delivery vs. safety and the different security architectures that are unique in information technology systems vs. industrial control systems (ICS). The goal of the industrial control system security program is to develop standards and test methods to enable the integration of security engineering into the industrial automation life cycle. NIST is working with industry to develop standards and test methods for validation and conformance. As part of the NIST role, Mr. Stouffer lead a Process Control Security Requirements Forum consisting of more than 680 individual members and over 400 organizations from 32 countries, including the United States. NIST maintains a Forum website: http://www.isd.mel.nist.gov/projects/processcontrol. NIST has also developed a 151 page generic system level protection profile for ICS. The Forum has created a SCADA Protection Profile Working Group consisting of ten members who are experienced in Common Criteria, SCADA systems and requirements. Draft NIST Special Publication 800-82, SCADA/ICS Security Guideline provides an overview and presents typical topologies to facilitate the understanding of industrial control systems and identifies typical vulnerabilities, threats and consequences. The

public draft is expected to be complete by September 30, 2005 with the final document completed by January 1, 2006. Mr. Stouffer discussed the ICS Vendor Security Checklist Program and the NIST Industrial Control System Security Testbed effort. Collaboration on this effort is vast: with the Electronics and Electrical Engineering Laboratory and the Information Technology Laboratory at NIST; with the Instrumentation, Systems and Automation Society; with the Department of Homeland Security and the Department of Energy and other government agencies; and testbed collaboration with the National SCADA Testbed (Idaho National Engineering and Environmental Laboratory and Sandia National Laboratory). Mr. Stouffer also represents NIST on the Department of Homeland Security Process Control Systems Forum.

Privacy Act – Legal and Policy Framework Discussion

At their June 2005, the Board discussed the current policy framework of the Privacy Act and its potential need for revision due to the change and additional statutes now in existence since the passage of the original Act. This agenda period was set aside to continue the discussions of this topic and set the ground work for further exploration of this activity. Since the June meeting, Board member Dan Chenok and former Board member John Sabo met with the chairman of the Department of Homeland Security's (DHS) Data Privacy and Integrity Advisory Committee, Paul Rosenzweig, to pursue any interest in collaborating with the ISPAB on this issue. Mr. Sabo, who is now a member of the DHS Data Privacy and Integrity Advisory Committee, provided the Board with an overview of the Committee's activities. The role of the Committee is to advise the Secretary of DHS and the Chief Privacy Officer of DHS on programmatic, policy, operational, administrative, and technological issues within the DHS that affect individual privacy, as well as data integrity and data interoperability and other privacy-related matters. They have organized the Board into four subcommittees: framework/principles; screening; data sharing and usage and emerging applications.

Next, Mr. Sabo presented a conceptual proposal for a joint inquiry and recommendations on 21st century framework for revisions to the Privacy Act of 1974 and related Federal privacy statutes to be undertaken by the ISPAB and the DHS Data Privacy and Integrity Advisory Committee (FACA). It proposed that this effort be undertaken by a subcommittee formed by the members of both committees, or parallel, well-coordinated subcommittees. This effort would be operated under the Federal Advisory Committee Act guidelines and requirements and be supported by both DHS and NIST to the extent deemed appropriate by the respective Designated Federal Officials (DFO) and the Chairs of both committees.

While this proposed idea was well received by the Board, the ISPAB DFO will need to check with NIST Counsel to determine whether participating as coordinated subcommittees or as one joint committee would be feasible. DFO Pauline Bowen will handle this action and report back to the Board.

Board member Howard Schmidt pointed out that there may be other FACA-type Boards who are also looking into Privacy Act-related issues. He stated that Departments such as Justice and Treasury may have established internal task forces or committees, and, it would be useful to learn of the status of their efforts as DHS/ISPAB pursues their efforts. Mr. Schmidt suggested that the Office of Management and Budget's Privacy office would be good source to go to for gathering this information.

Board member Leslie Reis presented the Board with an outline of a framework for revisions to the Privacy Act of 1974 and other Federal privacy statues. The briefing covered a review of ten Fair Information Principles, a synthesis of OECD and Department of Health and Welfare language. She discussed the history of the Privacy Act of 1974 both the language from the Senate version and the House version of the Act; the state of information (or lack thereof) in the late 1960's-early 1970's and that the legislative intent and effectiveness of the Act has been eviscerated over time. Professor Reis identified several possible areas that the Board may want to address in their review:

- Technologies and agency needs have changed
- Minimization principles have been diffused; e.g.., data matching, secondary uses and use of third party data are commonplace and perceived necessary
- Insufficient notice; e.g., the 1977 Privacy Protection Study Commission's Report found publication in the Federal Register to be of "limited impact."
- Choice; e.g., no choice (perceived lack of alternatives for government-to-commercial services)
- Access
- Security/audit
- Enforcement/redress
- Data matching provisions
- Use of third party.

A huge loophole exists today as there is increased use of information collected and maintained by the private sector [collection of cookies is one example].

Following Professor Reis' briefing, the motion was made to form an appropriate subcommittee to partner with DHS, and possibly others, to develop the roadmap for a 21st century framework for revisions to the Privacy Act of 1974 and other Federal policy statutes. Hearing no objections, Chairman Reeder deemed the motion accepted. It was suggested that the Board make Karen Evans, Glenn Schlarman and Eva Kleederman of OMB aware of what the Board is considering. Board member Dan Chenok volunteered to informally speak with Eva Kleederman and relate the Board's activity to her.

Next, the Board established a subcommittee to work on this issue. Members Leslie Reis, Howard Schmidt, Dan Chenok and Frank Reeder volunteered to be members of this subcommittee. The motion was made by Dan Chenok to have Leslie Reis serve as the Chair of the Subcommittee. The motion was seconded by Howard Schmidt and accepted by the Board.

If it is legally acceptable, the Board would prefer the collaboration between the DHS advisory board and the ISPAB to be a joint committee effort.

Board member Morris Hymes offered a definition of three distinctions that could be made:

1. interpretation of the Privacy Act provisions have a direct third party rules; in the context of modern technology;
2. voids in the Privacy Act based on new technology; e.g. cookies;
3. provisions of the Act that no longer have relevance based on modern technology.

Computer Security Division Program Update

Joan Hash, Acting Chief of the NIST Computer Security Division (CSD) gave the Board an update on the activities of the Division. **[Ref. #2]** In reviewing the Division's operating goals for FY2006, Ms. Hash emphasized that the new NIST Director's goal is that each of NIST's Operating Units expand their core competencies program effort. Other goals included continuing to meet the statutory responsibilities given to the CSD, to increase collaboration within the Information Technology Laboratory (ITL); to expand outreach to high impact communities such as health care, financial and academia; and to develop effective portfolio selection criteria consistent with ITL objectives. Ms. Hash reported that the Division is currently assisting the Department of Health and Human Services in their health care initiative.

Board member Rebecca Leng asked what was the next statutory responsibility that CSD expected to address. Ms. Hash responded that they are in the process of developing a plan for

the development of new standards and expects that one of the standards areas to be addressed will be an update of the risk management standard.

Ms. Hash reported that Dr. Shashi Phoha, ITL's Director, had established an ITL Technology Council. This council reports directly to Dr. Phoha and is composed of Post Doctoral participants (IPAs) assigned to ITL and internal ITL employees. This goal of this group is to look at new emerging areas for ITL initiatives and will formulate project proposals based on collaboration.

Ms. Hash offered to have CSD staff attend future Board meetings to brief them on the efforts of some of the emerging technologies that are being pursued. The Division is getting involved in a NIST nano technology effort and, there is an industry/vendor workshop on C&A activities currently planned. It is expected that the Division's focus on FY06 will be on personal identity verification, C&A work under FISMA, new line management direction, health care and collaboration across NIST. Ms. Hash also addressed the issue of the recent situation involving the Secure Hash Algorithm being threatened. NIST is sponsoring a workshop on October 31-November 1 to discuss this issue.

Chairman Reeder reported that plans are underway for him to have an opportunity to meet with the newly-appointed Director of NIST, Dr. William Jeffery before the December Board meeting. It is also anticipated that Dr. Jeffery will be able to attend the December meeting.

In response to Chairman Reeder's question of what assistance could the Board be to the Division, Ms. Hash indicated that the Division needed to increase their visibility in the scientific arena, making them aware of what the Division does. The Board could serve as a high-level critique vehicle when the Board receives Division briefings. Board feedback could include how is the story coming through, does it have impact and is the story being told effectively. Ms. Hash said that she would share the ITL competency list and the core set of questions that the NIST Director wants addressed. The DFO will see that this material is provided to the Board members.

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

Wednesday, September 14, 2005

The meeting was reconvened by the Chairman at 8:50 a.m.

The motion was made by Board member Lynn McNulty and seconded by Board member Dan Chenok to approve the minutes of the June 2005 ISPAB meeting. The motion was passed unanimously.

Personal Identify Verification Standard Update

Mr. Curt Barker of NIST's Computer Security Division, gave a status report on the Personal Identity Verification Standard (FIPS 201) and HSPD#12. **[Ref. #3]** The Board was especially concerned about the methods by which agencies would be able to purchase the compliance cards needed in the time frame that OMB is requiring and whether or not these agencies would have available funding to purchase these cards.

Mr. Barker reviewed the requirements of the PIV Standard. The standard calls for mandatory and optional PIV card visual data; mandatory and optional PIV card electromagnetic elements; mandatory and optional PIV electronically stored data and card information available for 'free read'. He also reviewed the specifics of NIST Special Publication 800-73, Interfaces for Personal Identity Verification, Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification, and Special Publication 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations. There are two additional documents currently in draft; Special Publication 800-85, PIV Middleware and PIV Card Application

Conformance Test Guidelines and Special Publication 800-87, Codes for the Identification of Federal and Federally-Assisted Organizations. Mr. Barker said that it is a critical observation that access control card cryptographic requirements will need to change to keep up with the pace of evolving security technology.

Mr. Barker identified some issue and questions that still need to be addressed. They included the need for Special Interest Groups in the areas of issuer organization accreditation, acquisition, PIV II implementation/migration, and interoperability and other testing. There is also a need for physical security implementation support of readers, cryptographic integration and others that may arise. There is also the question of whether additional issuer accreditation criteria/procedures are needed and the question of the need for the basis of accrediting individuals for PIV role.

Mr. Barker will continue to brief the Board as this activity continues.

Dialogue with NIST's ITL Director

Dr. Shashi Phoha joined the Board to discuss the NIST Director's support of the Laboratory and the Computer Security Division in particular. Dr. Phoha wants ITL's focus to be on is ITL meeting today's challenges, how is ITL preparing the nation for the next generation of information technology (IT) and how is ITL addressing the IT problems. Information technology today is business and needs driven and cuts across disciplines. As a results of the way the industrial revolution reorganized the world, government and academia are not set up to handle cross occurring issues. Dr. Phoha explained the purpose of establishing the ITL Technology Council. She sees this as a vehicle to assist the Laboratory in identifying some core IT projects. Dr. Phoha also told the Board members that the position of Chief of the Computer Security Division is open and, and she asked the Board to publicize it to people that they know to help identify the appropriate person for the job. Dr. Phoha sees the Division Chief position as a unique opportunity to influence the national direction of computer security. The Division will have a major role in the national health information network agenda focusing on security and privacy issue. The Board will hear from Dr. Phoha again at their December board meeting.

NIAP Report Briefing

Board Member Morris Hymes briefed the Board on the latest information about the National Information Assurance Partnership (NIAP) effort, a joint project between the NIST and the National Security Agency (NSA). The Department of Defense and the Department of Homeland Security have launched a contract with the Institute for Defense Analysis in support of one the President's National Strategy Plans' recommendations that the Federal government conduct a comprehensive review of the NIAP program. It is anticipated that the report's expected alternative/recommendations will have implication for NIST because of funding issues and have implications for the IG community as well as the expanded federal sector. Mr. Hymes said that the NIAP program is a subset of a larger entity. It is part of a neutral recognition agreement with other nations. Mr. Hymes reviewed how the NIAP process works to validate laboratories. He described NIST's role and NSA's role. The NIST/NSA partnership has been strained. Because of funding constraints at NIST some feel that NIST has not been able to participate in the manner that they would like to. Protection profiles at the lower level have not been created thus creating a void at the lower level of evaluation. That is not the case in the NSA environment because they have had the necessary funding to produce adequate protection profiles. Software assurance does not currently plan into the NIAP program issues. However, there is evidence of software assurance being seen at the higher level of evaluation. There are currently ten Common Criteria Testing Labs in existence and an additional five new candidates going through the clearance process. Since 2000, 285 products have been evaluated in the laboratories. Ninety-five products have been successfully completed and 154 are in the process of being evaluated. As the program continues to grow the resources need to be in place. Mr. Hymes stated that the federal

government is not being reimbursed by the vendors for this certification. They are subsidizing this effort.

NIAP is a program currently mandated only for the national security establishment. The question arising from the National Strategy is would a version of this program be something that should be mandated to non-national security establishments.

Mr. Hymes reported that the fundamental issues that can be addressed include the length of time of the process, the funding issue, the right model, etc. From a policy perspective, the drivers come from the NSTISSP-11.

The final IDA study should be issued to OMB within the next several weeks.

The Board could question whether or not this process contributes to the security of government systems. If so, what is the cost, both fiscally and technologically? Board member Susan Landau suggested that the Board prepare a letter to OMB stating their concerns and asking for consideration of a broader industry review of the report prior to the development of specific government policy.

Chairman Reeder suggested that the Board handle this issue in two parts: (1) wait until the report is issued and ask Morris Hymes to share with the Board those portions that he deems appropriate for sharing; and (2) based on information obtained, decide if there is anything that the Board believes it could address.

Role of the Chief Privacy Officer – Next Steps

Board member Leslie Reis discussed the Board's on-going effort of addressing the role of the Chief Privacy Officer (CPO). There is a huge variety of understanding and interpretation of the role of the CPO from agency to agency as well as a huge interpretation of the same position within the private sector. Questions exist as to what might be the appropriate criteria or skill sets that a government CPO should possess and where should the CPO position lie in the agency infrastructure. Whether the CPO should be a compliance or policy leader is another question that needs to be addressed. At the June ISPAB meeting session by private sector and government CPO types, the Board learned that their skills sets encompassed a variety of things; e.g., cross function skills and knowledge; the need for knowledge of technology or easy access to staff with such knowledge; a certain amount of chutzpah and the ability to be multidisciplined. Diplomacy was another skill set identified as being useful. The Board has to make the decision of whether or not draft a recommendation calling for repealing, reducing or eliminating the role of the federal CPO.

ISPAB Work Plan Discussion

The members reviewed the ISPAB task work plan for 2004 and revised it according to those tasks already completed and adding those new task areas that they deemed appropriate. Each member ranked the respective task items in order of what they felt were significant and needing the Board's attention over the coming months. Those members giving any task an "A" ranking are responsible for preparing an outline/work plan covering the proposed mission of the effort and a suggested set of action items to be taken. Each outline should be provided to the Board members for further consideration. These outlines will be presented and discussed as part of the agenda for future Board meetings. Board member Susan Landau proposed that the Board weigh in on the recent developments affecting the PIV standards implementation effort and the recent Secure Hash Algorithm issue. The motion was made and seconded to develop a letter to be sent to the Director of OMB conveying the Board's concerns. Those members voting in favor were Susan Landau, Franklin Reeder, Howard Schmidt, Dan Chenok, Lynn McNulty and Steve Lipner. Those members abstaining were Sallie McDonald, Rebecca Leng, Bruce Brody and Morris Hymes.

Information Systems Security (ISS) Line of Business (LOB)

Mr. John Sindelar of the General Services Administration briefed the Board on the government's line of business initiative. **[Ref. #4]** He reviewed the vision and goals of federal information systems security. The issues are in the areas of security training, FISMA reporting, situational awareness and incident response and security solutions. To close the information systems security gaps it is recommended that common solutions such as consistent and comprehensive implementation of proven security products, services and training be undertaken. The initiative also calls for the establishment of three Centers of Excellence for each of the four areas; phase-in of required and optional use of the common solutions in tiers over a three year period; maintenance of agency flexibility to tailor required solutions; and establishment of common metrics for effective performance evaluation. Mr. Sindelar explained the anticipated outcomes of each of the solutions to the four areas. He also discussed the criteria for the Center of Excellence Due Diligence Checklist.

The Board is very interested in doing whatever it can to help and influence this effort. Mr. Sindelar would welcome the Board's assistance as smaller subcommittees are established as this project progresses. Mr. Sindelar will be invited back to discuss the pilot projects effort at one of its future meetings.

Public Participation

There were no requests to speak from the public attendees.

Board Discussion Period

The Board reviewed the draft letter to the Director of OMB to convey the Board's concerns regarding the NIAP program. Board member Steve Lipner and Chairman Franklin Reeder will make the edits as suggested by the Board and have the final letter prepared. The motion was made by Board member Susan Landau and seconded by Board member Howard Schmidt that the letter be accepted and forwarded as appropriate. All members voted in favor of the motion.

As Board member Susan Landau will be unable to attend the December 2005 Board meeting, Chairman Reeder expressed the thanks and gratitude of the Board for her contributions to the Board's activities during her term. Her current term will officially end in January 2006.

The Chairman recessed the meeting at 5:10 p.m.

Thursday, September 15, 2005

The first meeting of the Federal Privacy Policy Review Committee was held this morning. Chair Leslie Reis discussed the steps the subcommittee would undertake. They are:

1. Establish method to structure the problem.
2. Identify what the problem was that the Board is trying to solve.
3. Find alternative ways to address the identified shortfalls.
4. Develop a roadmap based on these discoveries.
5. Send forward any suggested recommendations or alternatives identified.

There being no further business, the meeting was adjourned at 11:50 a.m.

Ref. 1 - Devereaux Presentation
Ref. 2. – Stouffer Presentation

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting.

Franklin S. Reeder
Chairman