Information Security and Privacy Advisory Board (ISPAB)

Summary of Meeting

George Washington University
Cafritz Conference Center
800 21st Street, Room 405
Washington DC

September 6 - 7, 2007

September 6, 2007

The Board members attending in person were Dan Chenok (Chairperson), Brian Gouker, Joseph Guirreri, Susan Landau, Lynn McNulty, Alexander Popowycz, Rebecca Leng, Howard Schmidt, Fred Schneider, Jaren Doherty, and Pauline Bowen as the Designated Federal Official.

Dan Chenok began the meeting and asked each Board member to introduce themselves and to give a brief report on their recent and current activities. Dan Chenok explained that Lisa Schlosser was away serving as a reserve, while Leslie Reis was unable to attend as she was working with DHS on the Privacy Technology study. Philip Reitinger was only able to join the meeting on the telephone briefly in the morning. Both Alex Popowycz and Brian Gouker will not be able to return on Friday, but Brian Gouker will provide information on other forthcoming workshops and presentations on telecommuting. Alex discussed his recent work on cross-Federation compatibility in identity management, as well as first responder credentialing; Dan noted that these issues would be taken up in the December meeting.

Howard Schmidt raised the issue of risk and vulnerability in Peer to Peer Networks. A discussion ensued as to whether the security issue was the P2P technology medium itself, or the way that individuals used the data on that medium. It was pointed out that telecommuting from machines where other household members have access to P2P networks posed a new kind of risk. This led Rebecca Leng to mention that risks from home computing involved security vulnerabilities and potentially privacy information breaches, noting that Fox News had recently reported the downloading of privacy offer personal information.

NIST attendees included Cita M. Furlani, Director, Information Technology Laboratory (ITL); Curt Barker, Division Chief, Computer Security Division (CSD); and Ron Boisvert, Division Chief, Mathematical & Computational Sciences (MCSD). Meeting minutes were taken by Annie Sokol, NIST.

Dan Chenok thanked both Curt Barker and Cita Furlani for joining the meeting, especially for staying on an extended time with the Board. Dan Chenok elaborated on each agenda item, and announced that the Board will spend some time in the afternoon on planning of future meetings. He reported on his recent presentation to IG communities at a meeting in Norfolk, thanks in part to Rebecca Leng. Rebecca reported that the IGs were impressed with Dan's presentation and they gained further understanding of the working of the Advisory Board.

NIST Metrics Project Briefing
Dr. Ron Boisvert, NIST Mathematical & Computational Sciences Division, Division Chief

Dr. Ron Boisvert began his presentation with a description of the functions and works of Mathematical & Computational Sciences Division (MCSD) including NIST FY07 Cyber Security Initiative. This presentation was a follow-up to the presentation made by Dr. James Turner, NIST Deputy Director, at the last quarterly Board meeting, where he stated that NIST activities need to be premised on a balancing of security, cost, and usability – higher security that drives risk down is less efficient, considering trade-offs is important. Ron Boisvert defined the foundation of measurement and goals as:

- Understanding relationships among structure, protocols, and performance;
- Characterizing robustness, fragility; and

- Identifying key (computable) measures

Dr. Boisvert stated that there were fundamental limits to MCSD's ability to design reliable information systems, and it is a difficult question to characterize the absolute security of a system that could be resilient against threats/vulnerabilities known and unknown.

The Board asked whether a better measure may be to assess relative security, rather than absolute security, and Dr. Boisvert agreed. Relative security could account for human interaction and usability issues – the question for research is how best to measure it. The Board also discussed the fact that it was important to measure reliability/availability rather than just confidentiality

Computer Security Division (CSD) Briefing (Part I)
Wm Curt Barker, NIST Computer Security Division, Division Chief

The presentation began with an overview of NIST Special Publication 800-55 Rev.1 as part of the introduction to Information Security Measurement, its structure, scope, and approach to measuring and analyzing security. The types of measurement (implementation, effectiveness, and impact) were discussed and a measures template was provided. Several Board members pointed out that a sound measurement approach would be to combine types of measures.

Curt Barker noted that making measures more granular allowed for more harmonization across public and national security-sensitive networks.

Creating Value from Vulnerability
Tony Sager, Chief of the National Security Agency's Vulnerability Analysis and Operations Group

Brian Gouker introduced the speaker and also provided the background and brief bio. During his 24 years with NSA, Tony Sager has served in a variety of technical and management positions, spanning computer security, cryptography, software analysis, and network security. His Center produces the NSA Security Recommendation Guides to Windows 2000, the first of several security products they have released to the public. Tony is also actively involved with a number of community-wide public activities in network security. He has degrees in Mathematics and Computer Science, and dabbles as a PC hobbyist.

This presentation was suggested during the last board meeting to learn about the best practices, processes, standards, software and technical scope at NSA.

The speaker explained the vision and mission of NSA Vulnerability Analysts & Operating Group. There are four major areas of focus:

1) Conduct operations to find vulnerabilities in
   - All stages of the life cycle of technology
   - The operational environment
   - Content (networking, signals, space…)
2) Analyze vulnerabilities
   - In emerging technologies
   - In core concepts
3) Translate vulnerability knowledge
   - Into guidance and countermeasures
   - To understand root causes
4) Lead the community
   - In the development of security guidance, training, education and standards development

Tony Sager elaborated at length about the influence of information assurance on each stakeholder - Practitioners, Buyers, Users, Suppliers, and Authorities.

Tony also discussed the SCAP program, though which NSA works with NIST and DISA on vulnerability assessment and security measurement.

When the meeting adjourned for lunch at 12:30 P.M., Joe Guirreri left the meeting. Leslie Reis joined the meeting via telephone in the afternoon.

NIST Computer Research Division (CSD) Briefing (Part II)
Wm Curt Barker, NIST Computer Security Division, Division Chief

Curt Barker stated that CSD focuses on integrity of information and processes, and availability of information and services in order to build trust and confidence in information technology (IT) systems. He then provided an update on CSD's major FY07 activities where the key initiatives include:

- Secure Hash
- Security Metrics
- Security Content and Other C&A Automation Initiatives
- Federal Desktop Security Configuration Activities:
- Security Product Assessment Requirements and Methods (Murugiah Souppaya, NIST CSD, works with several vendors)

On FDCC, Curt discussed the collection of activities including the NIST Checklist, FDCC image, virtual machine for testing, SCAP, and National Vulnerability Database. The question was raised about whether agencies should be able to purchase only products that conformed with the FDCC; Curt indicated that NIST was assessing a lab accreditation process, possibly linking with the DHS software assurance activities. Jaren Doherty indicated that HHS and other agencies would request exceptions per the OMB policy, and Curt responded that exceptions would be collected and posted.

Some current challenges CSD faces are cryptographic algorithms (long range), access control (in relation to which Alex Popowycz discussed the IAEG and indicated he would send information about the group to NIST), harmonization of Federal standards and guidelines with IC/NSS requirements (in response to a question about whether this was a policy shift, Curt said no and that the goal was to codify what is already common), defense against electronic identity fraud (about which NIST is consulting with the financial services industry), and balancing standards mission against implementation support requirements.

Curt also mentioned that ISO has adopted the PIV as a standard, and changes to that would be reflected in FIPS 201 later this year.`

The Board discussed the need to do more work on the user interface/human intervention element of cybersecurity, recommending that NIST research delve more deeply into human factors. The Board also discussed whether the number of bodies doing metrics oversight could be consolidated in the future. Curt said he would reflect on both issues and discuss them further with the Board in future meetings.

General Work Plan Discussion

Real ID and COOP Letters
Dan Chenok explained the comments from Curt Barker regarding the letters on Real ID and COOP. Curt indicated that NIST preferred the letters to be addressed to Karen Evans (OMB E-Gov Administrator) with cc. to Director OMB. The Board acknowledged Curt Barker's issue regarding the sensitivity of these letters and believe that the issue is not the content matter of these letters, but the questions lie in the roles of this Board. The Board had worked on the letters since the last meeting and had now reviewed and cleared the letters to be sent to OMB. The Board members agreed that they have the authority to speak to the Director of OMB.

Cita Furlani repeated her preference, given clearance timing and logistics, to send the letters to Karen Evans with a copy to the OMB Director (who is now confirmed as Jim Nussle). This was in line with the agreement made in the meeting and Dan Chenok accepted this alternate course of action.
Pauline Bowen is now working on the clearance process for these letters within NIST.

Pauline Bowen reminded the Board that there were other letters addressed to OMB in previous years, but that the Real ID and COOP letters that were prepared for this fiscal year, are the only letters to be recognized as part of the Board's work in FY07.

Fred Schneider noted that there were several items listed in Rob Boisvert's presentation that were too vague to be actionable. Dan Chenok noted that NIST produced documents with guidance and recommendations, but not as a White Paper, which would be much more useful, from his perspective.

The Board spoke very favorably about NIST's deeper involvement in discussions around key issues, and spoke about a process for moving forward with such sessions. This process could include:

a. Going over the broad NIST agenda semi-annually, selecting items with Curt Barker for detailed review at the next Board meeting.
b. Reviewing the list of NIST guidance documents and selecting key ones for Board review.

Dan Chenok agreed to discuss these ideas with NIST.

Susan Landau raised the idea of the Board engaging in more projects that result in white papers, rather than letters. The Board agreed to discuss potential ideas for such projects in the December work plan session.

The Board discussed several issues for potential consideration at the December meeting:

- Identity management – presentation by Morris Hymes, newly appointed as head of the ID Assurance Directorate at DOD (Dan to contact Morris)
- Sallie McDonald on the National Communications System (Dan to contact Sallie)
- Systems Assurance Activities that bridge national security and civilian IT, including product testing (Lynn M to work with ITAA; possibly invite Joe Jarzombek back)
- Web services/SOA security – briefing on the NIST guidance
- Privacy technology; review the ISPAB draft white paper (Leslie), should we advise CPOs on what they need to be doing re technology (Susan)
- Are senior managers continuing to pay attention to strong security – has the NIST executive guide enhanced understanding? Is the metrics program too fragmented and distant from senior management (Rebecca)?
- Social networking and security (possibly with the CDC CISO, Tom Madden – Jaren to inquire)
- Cisco, EMC, Microsoft Alight offer comprehensive technology architecture for helping protect and share sensitive government information – SISA Alliance unites industry leaders to produce a breakthrough in sensitive information exchange for government and private sector.

September 7, 2007

The Board members attending in person were Dan Chenok, Joseph Guirreri, Susan Landau, Rebecca Leng, Fred Schneider, and Pauline Bowen as the Designated Federal Official. Alexander Popowycz and Leslie Reis joined the meeting on the telephone periodically throughout the day.

Dan Chenok asked for a motion that the draft Summary of the Meeting from June 7-8, 2007 be approved. Lynn McNulty proposed the Meeting Summary be approved and accepted, which was seconded by Board members. Dan Chenok had discussed with NIST extending the terms for both Rebecca Leng and Howard Schmidt, which were due to expire sometime this year. Two other members, Susan Landau and Leslie Reis will be leaving the Board when their terms end early 2008.

Telecommuting Security Issues Panel
Tom Eilers, Blue Ridge Networks
Chris Shenefiel, CISCO Systems
Richard W. Swartz, Chief Information Officer of the Bureau of the Census

Dan Chenok introduced the panelists and followed with a brief introduction from each Board member.

1) Chris Shenefiel is manager of business development for Cisco Systems, Inc.'s Internet Communications Software Group (ICSG). In this role, Shenefiel is responsible for identifying new markets and partnerships that match emerging market opportunities to strengthen Cisco's position in the Unified Communications market; and to support Cisco's efforts to deliver software which improves the effectiveness of business communication by enhancing and unifying media-independent customer interactions across voice and data networks. Chris Shenefiel believed that telework is viable and should be used regularly, but he also suggested the following:
   - Independent operating system to ensure security
   - Encryption needs to be from operating system to operating system
   - Strict monitoring control but should not use operating system to manage security
   - Emergency response activities should be structured across geographical locations
   - Rely on technology, e.g. Virtual desktop to monitor and to secure endpoints
2) Tom Eilers is the Media contact at Blue Ridge Networks, which is a respected and leading provider of unparalleled security solutions for government and private industry. Tom Eilers insisted that it is a good practice to authenticate everything and trust nothing. It was necessary to validate all PCs, all applications used on every desktop, and from every connection.
3) Rick Swartz, CIO of the Census Bureau, stated that FISMA was overly concentrated on policies, and therefore, it lacked consistency in IT. He explained the following structure at the Census:
   - No PII information allowed on offsite workstation.
   - Digitalized signature required for logging on.
   - Strict enforcement of US CODE (Sensitive) Title 13 & 26 data on every laptop.
   - Very restricted telework policies.
   - Secure ID cards required in time of emergencies when staff has to work at home.

The panel members reiterated the importance of some level of baseline policies, validation of end points, and the essentials of authentication as a form of firewall. They also noted that every agency had different telework policies and various levels of sensitive information. The State Department only allows staff to log on at work and all work must be completed within the embassies. The main focus should not be simply to protect systems and hardware, but more importantly, to protect the data. In closing, the panel had the following suggestions:

1) Establish appropriate telework policies
2) Develop a general foundation across government agencies, and allow variation up by agencies.
3) Conduct audits and develop more consistent policies on use of PII in telework.

Brian Gouker provided paraphrased bullet points of NSA telecommuting policies and procedures to the board members during the December 6 & 7, 2007 Meeting for review and comments. A brief discussion on telecommuting and computer access followed and a motion was made and passed to add the bullet points to the minutes of this meeting.

Brian Gouker provided the following paraphrased bullet points in regards to NSA's telecommuting policies and procedures:

- A specific, written agreement with a bound time frame (one year.)
- Work role and responsibilities defined
- Government equipment only
- Home is considered "Alternate Duty Station"
  - Workman's Comp applies
- Management can revoke agreement at any time
- Unclassified work only
- Conservative Operational Procedures
  - No downloading
  - Regular virus scanning
  - No WEB surfing (except as permitted by the specific duty description)

Privacy Briefing
Maya Bernstein, J.D., Privacy Advocate, Secretary, Policy advisor, U.S. Department of Health & Human Services

Maya Bernstein has special expertise in information policy and electronic commerce, including data protection, privacy compliance and electronic signature law. She raised the following concerns on privacy:

1) Reduce volume of PII
2) Review PII, FISMA, ID theft
3) It is difficult to reduce the overall use of social security numbers as many businesses deal with the government using SSN. Medicare and the military use SSN as an identification number, and their systems are old and difficult to change.
4) Encryption, remote access
5) Ensuring awareness of privacy
6) Breach response requiring one hour to report - matching act is limited to matching certain needs to applicable functions within the administrative purposes, use of commercial databases
7) NIST Guidance on technical requirements – pull guidance together on technical implementation.
8) OMB is no longer covering staff level group, and there is less emphasis on privacy in federal government
9) Many entities are not covered by privacy law. Many medical companies are gathering patients' information as part of the treatment to generate Internet sites used by patients and medical practitioners to manage their illnesses, simultaneously, the information is compromised for marketing purposes.
10) Employers are using employees' information, particularly health records.
11) Mental health information is turned over to law enforcement.
12) Information is gathered for emergency preparedness, but there is no one way of knowing what information is gathered, where it is going and who should have access. It is necessary to have a technological tool to sort and direct information to responsible people.
13) The issues of Civil Rights, Patriot Act and Privacy.
14) New technologies are creating gaps in the policy framework governing privacy.

Privacy Technology Project White Paper
Leslie Reis, The John Marshall Law School
Dan Chenok

Leslie and her colleagues were back working on the paper, and they are working on producing an outline before the next meeting.

General Work Plan Review

Curt Barker had provided a list of specific issues to the Board for recommendation and suggestions. The list included issues of interest for the NIST Computer Security Division, and areas for future research that the Board would recommend NIST undertake. The Board concurred on the three research items as follows:

1) Usability and security: research on how best to present security choices to users so that they can make informed and implementable choices about security options and settings that are easy for users.
2) Upgrade NIST's SCADA systems research program, with a goal that research would point to enhanced NIST guidance on SCADA safeguards.
3) Trustworthy computing and cybersecurity: Add research on the confidentiality and availability to the existing program that is more focused on reliability; develop a greater picture of trust for enterprise networks that include servers, workstations, databases, firewalls, etc.

It was noted that NIST is active in releasing publications. Dan Chenok asked the Board if it is their interest to be involved in the process of review, approval and notation of these publications. Susan Landau believed that the documents consist mostly of technical details and that it would be better for the Board to request a brief presentation of selective upcoming publications.

Action items

1) Dan Chenok and Pauline Bowen are to review NIST publications and identify which publication(s) that the Board would like to be briefed on every six months. The Board could also review the list included in Curt Barker's presentation. The author(s) and/or Curt Barker will then give a presentation of the main points and focus of the publication.
2) Dan Chenok is to discuss agenda topics with Curt Barker prior to next meeting.
3) Dan Chenok to discuss process with Curt Barker and Cita Furlani for continuing to have in-depth discussions on key topics with NIST.
4) Board members requested that future meetings should be scheduled on Thursday and Friday of the first week of each quarter.
5) Consider topics for white papers that would be six to nine month-long projects
6) Potential speakers for the next board meeting in December 2007 (to be prioritized based on the Board strategic focus areas, and to be scheduled based on availability):
   - Identity management – presentation by Morris Hymes, newly appointed as head of the ID Assurance Directorate at DOD (Dan to contact Morris)
   - Sallie McDonald on the National Communications System (Dan to contact Sallie)
   - Systems Assurance Activities that bridge national security and civilian IT, including product testing (Lynn M to work with ITAA; possibly invite Joe Jarzombek back)
   - Web services/SOA security – briefing on the NIST guidance
   - Privacy technology; review the ISPAB draft white paper (Leslie), should we advise CPOs on what they need to be doing re technology (Susan)-
   - Are senior managers continuing to pay attention to strong security – has the NIST executive guide enhanced understanding? Is the metrics program too fragmented and distant from senior management (Rebecca)?-
   - Social networking and security (possibly with the CDC CISO, Tom Madden – Jaren to inquire)
   - Cisco, EMC, Microsoft Alight offer comprehensive technology architecture for helping protect and share sensitive government information – SISA Alliance unites industry leaders to produce a breakthrough in sensitive information exchange for government and private sector.

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting.

Daniel Chenok
ISPAB Board Chairman