Information Security and Privacy Advisory Board (ISPAB)

Final Summary of Meeting

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

December 6 - 7, 2007

December 6, 2007

Board Acting Chairman, Lynn McNulty, convened the Information Security and Privacy Advisory Board (ISPAB) for its last meeting of the year at 8:35 A.M.

In addition to Acting Chairman McNulty, members present during this meeting were:

Brian Gouker,
Joseph Guirreri,
Susan Landau,
Rebecca Leng,
Leslie Reis,
Phil Reitinger,
Fred Schneider,
Howard Schmidt
Dan Chenok (Chairman) joined the meeting after lunch.

The entire meeting was open to the public. Over the 2 days of the meeting, there were 23 members of the public in attendance.

Acting Chairman, McNulty asked each Board member to introduce themselves and to give a brief report on their recent and current activities. Alex Popowycz participated in the 2-day meeting via teleconferencing.

NIST Computer Security Division Update
Donna Dodson, NIST Computer Security Division, Deputy Division Chief

Ms. Dodson presented an organizational update to the board of managerial changes. She provided an overview of three division activities including the update of Federal Information Processing Standard 140 Security Requirements for Cryptographic Modules, the Secure Hash Algorithm competition, and the secure web services project. She ended her presentation with an updated list of NIST publications in development.

Senior Management's Role in FISMA Review
Rebecca Leng, DoT, AIG for Financial and IT Audits
Wanda Scott, DoD, AIG for Readiness and Operational Support
Gwen McGowan, GSA/OIG Audit Director

Rebecca Leng opened the discussion with an introduction of the panel members. She explained the process of how the various agencies respond to FISMA reviews and how senior management has to weigh many different important considerations during the process. She said that the reports submitted to CIOs included factual data and independent opinions from IGs. She pointed out that senior management conducts information audits throughout the year with or without FISMA for internal organization purposes, and conducts FISMA reports for OMB when they are due.

Wanda Scott provided an overview of the Department of Defense (DOD) organizational chart to help the board members understand the multiple levels of reporting for the operating units within DoD. She stated that she works closely with the DoD FISMA board to carry out the FISMA process within DoD. She stated that at DoD, each single function/component has different reporting, multiple missions, and different divisions have different policies.

Gwen McGowan stated that the Inspector General considered risk management as an integral part of GSA's FISMA reviews. She indicated that there is a 12-person IT team that is responsible for maintaining reliable audit work and planning and supporting IT issues at GSA.

The panel of IGs would like to receive more guidance from the federal government on IT security, federal sectors for value added requirements, and report requirements from OMB. They also would like to get better guidance from senior management when collaborating with each IG.

Use and Implementation of Federal IT Security Products as a Baseline
Patrick Howard, HUD CISO
Brenda Abrams, GSA IG Auditor

Patrick Howard stressed in his presentation titled, *Use of Best Practice IT Security Products*, that general IT security program must have a strategic plan, organizational structure/staff, policies, and procedures to be able to achieve FISMA compliance. He stated that HUD achieved an "A+" on FY06 FISMA since establishing procedures using NIST guidance. He said that although FISMA plays a pivotal role in IT security, HUD added its own IT Security documentation requirements. He stated that HUD educates and communicates its requirements to all systems owners and conducts training to further create awareness of IT Security. He added that HUD makes its system user friendly with checklists for verification and guidelines.

Brenda Abrams further emphasized the importance of procedures. She has created a template of checklists that can be used by federal agencies and provided instructions for completing the checklists. She said that training was also available to educate people on completing the checklists. She explained that this is a system created in-house for HUD as part of its process to be compliant with their requirements. Brenda Abrams requested that the Board hold support discussions with NIST and OMB on the recommendations to realize the following benefits in 2008:

- A reduction in the amount of time that the agencies use in "reinventing the wheel."
- Use of products immediately by agencies
- Results that can be realized in 2008

Chairman Dan Chenok joined the meeting after lunch. He briefly introduced the panel for the next session, and the board members introduced themselves to the panel.

Social Networking and Security Briefing
Hart Rossman, Chief Security Technologist, SAIC
Sandy Smith, Manager of Technical Development, Forum One Communications, Inc.
Janice Nall, CDC

Sandy Smith stressed that good practices are needed to adapt to the current technological climate. It is critical for all web application developers and policy clients for both government and non-government to bring about network security; security is a process and not a product or certification. Many attackers pose as social callers on these social sites to get to the users. In many instances, attackers broke into the network randomly and innocently but simply to use the site. There are many web sites that set up to imitate a popular site so as to trick people to divulge their information. Sandy Smith described a number of preventive measures, namely, to limit the harm, change work habits (login every time), raise the level of security, educate developers to sanitize their websites, and increase the level of values.

Hart Rossman stated that high traffic to a social network is driven by economics. In his presentation, he listed the following eight core patterns that need to be addressed:

- •Harnessing Collective Intelligence
- •Data Is the Next "Intel Inside®"
- •Innovation in Assembly
- •Rich User Experiences
- •Software Above the Level of a Single Device
- •Perpetual Beta
- •Leveraging the Long Tail
- •Lightweight Models and Cost-Effective Scalability

Janice Nall explained how CDC uses social media to increase the impact of CDC's science. CDC's goal is to make CDC content, tools, and services available when, where, and how users want them in order to improve the health and safety of people around the world. CDC had researched user data briefs on various platforms and created CDC 2.0 eHealth Efforts, which was used for crisis communication, conducting research and collecting secondary data for disease management. CDC is presently working with three social networks and encountered a number of challenges including security risks and sexual content. Many federal agencies, including CDC, use MySpace to reach their constituents. It would be reasonable for the government to provide guidelines for users of social network sites.

Information Security and Privacy Advisory Board – Past and Future
Susan Landau, Sun Micro Systems

In her final presentation on the board, Susan Landau provided a historical background on the creation of ISPAB, beginning with the Brooks Act and Computer Security Act, and defining the role of Computer System Security and Privacy Advisory Board (CSSPAB) that is today's ISPAB. Susan Landau described CSSPAB's historical involvement in the rise and fall of the clipper chip and noted similar concerns with today's cyber initiative. She stated the cyber initiative will allow NSA to monitor internet-based networks supporting critical infrastructure (electric power grid, subways, nuclear power plants) to prevent unauthorized cyber intrusion/attacks. Susan stated the board should be involved with such programs since it directly impacts the NIST Computer Security Division mission.

ISPAB Discussion & Panel On Einstein Program and related initiatives
Moderator: Lynn McNulty, Board Member, Mischel Kwon, Chief of Security, DOJ, Andy Purdy, Former Acting Director, U.S. Department of Homeland Security, National Cyber Security Division / US-CERT; President, DRA Enterprises, Inc.

Lynn McNulty introduced the distinguished guest panelists. Andy Purdy explained to the board that Einstein is a pilot, not fully funded. This is a program to monitor and gather data on internet systems among agencies, with centralized gathering capabilities of any possible intrusions. The program is designed to address the challenge of identifying cyber attacks on federal agencies and revealing federal systems that have been corrupted by cyber attackers. It is under the care of the National Cyber Security Division of the US Department of Homeland Security, National Security Agency, Office of Management and Budget, CERT/CC at Carnegie Mellon University, and several cabinet-level agencies.

The Einstein program enables full-time monitoring and analysis of network traffic received and sent by federal agencies, resulting in identification of patterns that may be signs of persistent presence of unauthorized software and users on federal networks. Its expansion into the Trusted Internet Connection (TIC) program extends these benefits to all federal agencies. Fourteen federal agencies already have deployed Einstein sensors at their network gateways to capture information about network traffic, and feed it to analysis programs run by CERT/CC at Carnegie Mellon University in Pittsburgh on behalf of the US Department of Homeland Security.

The Panel recommended that the Board examine this issue further, for example:

- what is the investment in Einstein and what are the outcomes?
- Is the initiative successful at mitigating risk?
- How does Einstein contribute to a defense in-depth strategy?

Public Participation
There was no request for public participation.

The meeting was recessed at 4:40 P.M.

December 7, 2007

Chairman Chenok reconvened the meeting at 8:05 A.M. In addition to Chairman Chenok, members present during the meeting were:
Jaren Doherty,
Brian Gouker,
Joseph Guirreri,
Susan Landau,
Rebecca Leng,
Lynn McNulty,
Leslie Reis,
Philip Reitinger,
Fred Schneider,
Howard Schmidt,
Alex Popowycz (on conference call),
Donna Dodson, NIST's Computer Security Division was also present at the meeting.

Board Discussion/Review of Day One of Meeting

Dan Chenok proposed to move the CSIS Commission Briefing to the later part of the morning. All the Board members agreed.

Brian Gouker provided paraphrased bullet points of NSA telecommuting policies and procedures to the board members 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 the September 6 & 7, 2007 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)

Dan Chenok asked for a motion that the draft Summary of the Meeting from September 6-7, 2007 be approved. Lynn McNulty proposed the motion that Meeting Summary be approved and accepted, and the motion was seconded by Board members.

Dan Chenok thanked Donna Dodson for attending the meeting and Donna in return extended her appreciation to the board members for their dedication. She also expressed her appreciation to Susan Landau and Leslie Reis for their involvement on the board. NIST will be sending certificates of appreciation directly to them. Rebecca Leng also added praise for Susan Landau and Leslie Reis. Leslie Reis and Susan Landau both responded with their summation of their time working with the board.

- Dan Chenok suggested a further discussion from Donna Dodson's presentation specifically on FIPS 140-2, FIPS 140-3 and HASH. Dan Chenok suggested that a white paper be drafted on this subject for the June meeting.

- Philip Reitinger suggested a briefing on secure information alliance to promote reference architecture to protect and share information. He is not involved in the policies but he could organize a panel to present a policies perspective.
- Telecommuting was another topic of interest for a future board meeting
- Additional information on the Einstein program is of interest to the board. Dan Chenok provided description on the OMB's memo. There is very little information available on this program even though it is widely applied to all agencies. Alex Popowycz wondered how the program is being coordinated among all the agencies, which are spread out over the country. Lynn McNulty suggested that it maybe worthwhile to request OMB to put together FAQ on Einstein. Rebecca Leng requested OMB to share the long term view and policies on Einstein. Dan Chenok had some information regarding Einstein and he will present them to the board at the next meeting. Philip Reitinger suggested reviewing the White House Administration's budget for provision on this program. Dan Chenok suggested forming a subcommittee for discussion on Einstein between now through February 1, 2008. The subcommittee will consist of Dan Chenok, Alex Popowycz, Joe Guirreri, Lynn McNulty and Fred Schneider. Lynn McNulty will Chair the subcommittee.

Identity Management Briefing
Morris Hymes, Director Department of Defense Public Key Infrastructure (PKI) Program Management Office

Morris Hymes stated that the use of the Internet has exploded over the past twenty years and that trust is the most critical element in the use of communication systems. DoD's Public Key Infrastructure (PKI) is part of the larger DoD construct of Identity Management. PKI contributes to Identity Management by generating digital credentials that are: 1) unique, 2) un-forgeable, and 3) trusted for use in virtual network transactions. The process involves establishing identity and establishing a process that uses one form of identity to verify and validate each individual's credential. The process entails 1) verifying documentation, 2) binding identity information with credential, 3) associating credential with individual, 4) discovering/presentation of credential, 5) validating credential. The Board suggested that there should be an infrastructure to allow a machine to be able to remotely authenticate the identity of a person.

Morris Hymes posted the following requests to the board:

- Encourage the development of guidelines for authoritative sources and protection of biometric information
- Promote government structure that addresses certification and accreditation challenges across organizational boundaries
- Consider whether there is a need to create common standards for sharing / accessing identity information (law enforcement versus operational use.)
- Discuss decision support systems that assist with authorization services and address privacy issues associated with aggregating identity information.

Center for Strategic & International Studies (CSIS) Commission Briefing
Dan Chenok, SRA and Board Chairman

Dan Chenok provided a letter and a list of the CSIS board members which is available on the CSIS website. Dan Chenok briefed the board on the meeting that he attended. Susan Landau noted that the board does not include representation from technologists and technical researchers. They should be included to help develop policies. The ISPAB could invite members of CSIS working group to speak to the board. Dan Chenok will discuss the issues raised by ISPAB board members to the CSIS and report back to the board.

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

Leslie Reis presented a draft white paper.. The concept of this paper is to raise alerts and awareness. The challenges she faced included huge differences between practices and applications. She requested the board to suggest an applicable approach and to provide comments so that she will be able to continue finishing the paper. The comments provided as follows:

- Trends that implicate privacy practice and why it is problematic today.
- Needs to include social Networking
- Cultural norms

Dan Chenok will work with Susan Landau and Howard Schmidt to provide the input.

Essential Body of Knowledge – A competency and Functional Framework for IT Security Workforce Development
Brenda Oldfield, Director for Education, Training & Workforce Development, National Cyber Security Division, DHS

Brenda provided a briefing on the DHS program: A competency and Functional Framework for IT Security Workforce Development. The program is based on three objectives:

- Ensure that we have the most qualified and appropriately trained IT security workforce possible.
- Establish a national baseline representing the essential knowledge and skills that IT security practitioners should posses to perform.
- Advance the IT security landscape by promoting uniform competency guidelines.

The presentation also included a discussion of the DHS methodology, functional perspectives, framework, framework components, Regulatory and Standards Compliance, and competency areas. DHS had already incorporated ISO standards to this framework and is working with DoD to incorporate their requirements. The document is available on the web site for review and comments http://www.us-cert.gov/ITSecurityEBK/EBK2007.pdf

After the presentation, the board had concerns with the appropriateness of the framework and the, lack of any special certification for individuals. The board would like to write to OMB regarding its concerns and further funding on this framework. Susan Landau proposed a motion to write a letter to OMB, and the board members seconded the motion. The motion was passed with two members abstaining.

DHS National Communication System Update
Sallie McDonald, Director and Deputy Manager of the National Communications System, DHS
NGN Task Force report
NSTAC Next Generation Networks
Report<http://www.ncs.gov/nstac/reports/2006/NSTAC%20Next%20Generation%20Networks%20Task%20Force%20Report.pdf>

There were several briefings on emergency response presented to the board that subsequently led to request to get an update on National Communication System (NCS.) Sallie McDonald briefed the board on its functions, mission, and structure. NCS worked closely with the vast majority of the communications industry as many communications infrastructure are owned by corporations. Because access to the public communications network is often degraded in times of crisis, the NCS has developed programs to ensure priority access for critical users. While priority service programs are beneficial when the network is degraded, the NCS has also designed programs in anticipation of an inoperable public network. These programs are Telecommunications Service Priority (TPS), ESF Emergency support function, and Shared resources high frequency radio program. Since inception, NCS has developed programs and services to address the unique communications challenges. The success of NCS is based upon the understanding of the relationship of agencies with each other. Current priorities are 1) keeping the continuity communications for federal departments and agencies; 2) emergency support function #2, i.e. access,

fuel and security for industry, 3) priority telecommunications services in the next generation network, and 4) telecommunications and electric power interdependence. NCS ensures that there is a viable plan in place for emergency preparedness.

Work Plan Discussion

1) Susan Landau - Technical standards should be initiated by NIST
2) Rebecca Leng recommended that OMB should evaluate FISMA grading so as to help IG communities, however, it may be too late in the cycle to write to OMB. The Board recommended that NIST write to OMB requesting OMB to publish the guidelines earlier.
3) Howard Schmidt suggested inviting the Secretary of DOC, Secretaries of various departments or the Director of NIST to visit with the board periodically so as to have a dialogue with the board. Dan Chenok will verify with Cita Furlani and James Turner and then inform Howard Schmidt to initiate the invitations.
4) Dates set for ISPAB meeting in 2008 – quarterly, first Thursday and Friday of the month
   March 6 & 7 (Fred Schneider is unable to attend)
   June 5 & 6 (Phil Reitinger is unable to attend)
   September 4 & 5
   December 4 & 5

The Chairman adjourned the meeting at 4:16 P.M.

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting.

Daniel Chenok
ISPAB Board Chairman