Information Security and Privacy Advisory Board (ISPAB)

Summary of Meeting

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

September 4 – 5, 2008

September 4, 2008

Started at 8:45 A.M.
Ended at 5:00 P.M.

Present:
Dan Chenok
Brian Gouker
Joseph Guirreri
Rebecca Leng
F. Lynn McNulty
Fred Schneider
Ari Schwartz
Alex Popowycz
Phil Reitinger
Peter Weinberger
Pauline Bowen, DFO

Absent:
Jaren Doherty
Lisa Schlosser
Howard Schmidt

Visitors, presenters, panelists: 15
Donna Dodson
Matt Scholl, NIST, Computer Security Division

The Chair convened the Information Security and Privacy Advisory Board (ISPAB) meeting at 8:45 A.M. He acknowledged and expressed his appreciation to Google and Peter Weinberger for providing refreshments and breakfast. The meeting began with each Board member introducing themselves and relating the highlights of their latest developments. The Chair reported that a draft report from CSIS (Center of Strategic and International Studies) Commission could possibly be ready in a month. Once the draft is ready, the Board will work with James Lewis to set up a presentation before the Board. Ari Schwartz reported that the paper on telecommuting has been released. The Board reviewed each agenda item for the meeting as the Chair provided information relating to the agenda items.

A View from Congress on FISMA
Erik Hopkins, Professional Staff Member
Senate Committee on Homeland Security and Governmental Affairs
Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security

Erik Hopkins works as a Professional Staff Member on the Senate Subcommittee on Federal Financial Management, Government Information, and International Security. He is responsible for overseeing the Federal Government's proper stewardship for taxpayer monies.

Erik Hopkins stated that the FISMA review was completed in April and his presentation described the process that the review was based upon. The presenter discussed the current FISMA "framework;" the review of FISMA success and environment since 2002; the measurement for comparison of information security improvements among agencies in 2002 and 2008, the possible areas for improvement; the problems and possible solutions relating to implementation of FISMA; who should be the partners for success; and a legislative "wish list".

The purpose of this presentation was to receive comments from the Board since FISMA has past its six year mark and an outcome measurement should be in place. The measurement metric should define the system holistically and not from system to system or agency to agency. This measurement perimeter should be set within an attainable middle ground in order to gain reasonable effectiveness. Presently, vulnerabilities exist such as information not being classified properly or clearances not enforced effectively. The presentation identified the partners that could contribute to the solutions to include the educated individual, the responsible business owner, the empowered CISO, the informed agency head, and an educated Executive and Legislative branch. Erik Hopkins provided further clarification on the importance of an empowered CISO to support legislative aspirations. In conclusion, he affirmed that the goal is to make sure that the presented points will be adopted into a bill, and that comments received from the Board will be incorporated.

Privacy Impact (Einstein)
Peter E. Sand, *Director*, Privacy Technology, DHS Privacy Office
Michael J. Castagna, Department of Commerce

Peter Sand has served as the Director of Privacy Technology in the Privacy Office since April 2004. Before joining the Department of Homeland Security, he served as the Chief Privacy and Chief Information Officer for the Pennsylvania Office of the Attorney General, in Harrisburg, Pennsylvania. He had also previously practiced as an attorney and technology consultant with Sand and Saidel, P.C. for state and local government agencies and non-profit and educational organizations.

Michael Castagna, CISSP**,** is the Chief Information Security Officer at the U.S. Department of Commerce. Prior to joining the Department of Commerce, Mr. Castagna was the IT security officer at National Aeronautics and Space Administration (NASA), where he was responsible for supporting the CIO with agency-wide information technology security planning, governance and operations.

After the initial introduction, Michael Castagna began by describing the difficulties of understanding the threats to privacy since 70% of the threats were discovered by a third party. Today's hackers are getting more innovative as they are driven by economic incentives of obtaining data from government sectors and corporations. Einstein is a networking monitoring tool designed to analyze network data from multiple sources. It monitors threats coming from outside the agencies. Einstein monitors all data flowing in and out of agencies and mainly analyzes the headers without capturing the full package. Because the monitoring covers minimum data, the cost and maintenance are relatively low. The information gathered is used to identify potential threats, to build a good indicator from consistent data for decision making, and to provide alerts of potential compromises. The program is not designed to detect fraud. The signal from Einstein is classified from the technical standpoint.

Privacy is perceived differently between inside and outside the agency since the government has a slightly different risk model. DHS assumes that Internet users do not expect privacy in the "To" and "From" addresses of their e-mail or in the "IP addresses of the websites they visit" because their service providers use that information for routing. IP addresses are used as quality data as part of the security analysis. The continued monitoring will help to find a pattern of attack on the federal networks. Presently, the data is not being shared with other agencies. It is possible that other agencies may have set up similar monitoring programs.

Peter Sand – The DHS Privacy Office is responsible for privacy compliance across the Department, which includes assuring that the technologies used by the Department to protect the United States both sustain and do not erode privacy protections relating to the use, collection, and disclosure of personal and Department information. The Privacy Office also has oversight of all privacy policy matters, including compliance with the Privacy Act of 1974, the Freedom of Information Act of 1966 (as amended), and the completion of Privacy Impact Assessments on all

new programs, as required by the E-Government Act of 2002 and Section 222 of the Homeland Security Act. The Privacy Office also evaluates legislative and regulatory proposals involving collection, use, and disclosure of personal and Department information by the Federal Government.

Peter Sand indicated that privacy is the central focus in all work by the DHS. Privacy is the primary issue and premise of DHS's overall mission as well as the system project. The DHS is a relatively new agency and it is trying to build a bureaucracy, provide technology to streamline process, and make privacy a part of people's practices. While this process and part of the standard package is still in an early stage of development, people are incorporating privacy as part of analysis.

Presently, the agency is rolling out Einstein 1, which was deployed in 2004. DHS has made the information relating to Einstein available to the public. The agency is in the later stages of Einstein 2 and the information is available for public viewing on DHS web site. The agency also is developing requirements involving standard administrative steps with nine sections on requirements for collecting information. This is to ensure that people will do the proper analysis especially for risk analysis. The information gathered is not shared and there is strong consideration of who and what to share re the information. The Privacy Impact Assessment (PIA) for Einstein 2 is specifically developed by DHS.

DHS Cyber Security Center Activities Brief
Rod Beckstrom, DHS

Mr. Rod Beckström is the Director of the National Cybersecurity Center in the United States Department of Homeland Security. He was appointed to his current position on March 7, 2008, and reports to Secretary Michael Chertoff. In his capacity as Director of the Center, he facilitates information sharing and collaboration among Federal Government organizations responsible for various aspects of cybersecurity. He leads the effort to fuse information across multiple Federal Government domains in order to represent the composite state of U.S. cyber networks and systems.

The National Cyber Security Center (NCSC) operates separately from DHS but reports directly to Homeland Security Secretary Michael Chertoff. The department is leading efforts to protect federal networks and enhance capabilities that defend and reduce cyber-associated risks. The NCSC works with the interagency to implement cyber security strategies in a cohesive way, consistent with privacy laws. It is dedicated to cyber security and not operational or does it shares information. Rod Beckström serves the department by coordinating cyber security efforts and improving situational awareness and information sharing across the federal government.

After the initial introduction, Rod Beckström asked the Board members to present their questions on his presentation. The questions focused mainly on procedures, approaches, structures, analysis, resolution, objectives within the government, the plan influence other agencies, and handling future threats.

Mr. Beckström emphasized that the presentation was to provide a general view. He began the presentation entitled "Cyber History, Future & Questions" with an illustration of Lincoln and his usage of the telegraph to elaborate the connection between communication and cyber security. He further explained that George Washington modified his warfare strategy by countering insider threats and hackers (traitors). But to protect our systems today, it is necessary to first set the values and rules, and to decide the functions that we need to maximize. He defined his formula for success –the total cost of security should equate with our cost of security and the expected cost of loss of security.

He proposed that better protocols will lower the loss function. We have invested in various protocols (IPV6, BGP, DNS, SMS/IP, POTS, etc.) but when IP, internet and other components fail, we consequently lose text messaging, telephone connections, internet, and SCADA.

He explained the economics of privacy as being purely external.. When examining privacy, values are not transferred to the market because there is a need to internalize the economics of privacy. It is necessary to allow trade-offs among security, privacy, and convenience. It is desirable to want information to be free, but at the same time to allow information sharing and to be simultaneously secure and private. There is the other arguments that privacy will provide better security. The perimeters of privacy include minimizing data, anonymity, leveraging private sector, cloud computing, definition and measurement, incentive structures, auditing, Red teams, and Privacy and Cyber security. However, it is difficult to analyze data with anonymity and to require accountability with privacy. Mr. Beckström proposed that it would benefit society to establish the framework as described in "*Aspen – Nextgen Privacy?*" and to create a standard and a market based on this ideal:

> *The multi-stakeholder process outcome will be an open source standard, supported by a policy and legal framework, for authentication and credentialing of individuals without requiring exposing personal identifying information. At the same time, the framework will support the availability to law enforcement of relevant personal/identifying information upon presentation of a suitable warrant.*

NIST Computer Security Division (CSD) Briefing

Donna Dodson, NIST Deputy Cyber Security Advisor and Computer Security Division, Deputy Division Chief

Donna Dodson began her presentation by acknowledging the two new Board members. She also noted that Cita M. Furlani, Director, ITL, and Jim St. Pierre, Deputy Director are on assignment are unavailable to attend. The presentation represents a regular update of NIST Information Technology Laboratory/ Computer Security Division's (ITL/CSD) mission and concentrates on the technical aspect. She distributed organizational charts, described the inter-relationship of the program, and explained how the new programs are anticipated to address the emerging strategic priorities. The presentation moved from division structure and IT Security Mechanisms to include an update on FISMA legislation. Apart from development of FISMA Phase 2, Ms. Dodson explained how the legislature impacts CSD work on FISMA development and how to improve mechanisms to protect the integrity, confidentiality, and authenticity of Federal agency information by developing security mechanisms, standards, testing methods, and support infrastructure requirements and methods. Following the detailed description of each of the four groups under CSD, Ms. Dodson also listed highlights of each group. In conclusion, the presentation also included a list of workshops supported or sponsored by CSD in 2008/2009.

Cyber Initiative and relationship to Civilian Agency Security

Melissa Hathaway, Office of Director of National Intelligence (ODNI)

Melissa E. Hathaway is a Senior Advisor for the Director of National Intelligence (DNI) and Cyber Coordination Executive. She chairs the National Cyber Study Group (NCSG), a senior-level interagency body that was instrumental in developing the Comprehensive Cybersecurity Initiative (CNCI) aimed at substantially improving the ability of the United States to secure and defend its critical cyber national infrastructure. In January of this year, Ms. Hathaway was appointed Director of the Joint Interagency Cyber Joint Task Force (JIACTF) and is responsible to coordinate and monitor the implementation of the Broad portfolio of activities and programs that comprise the CNCI.

Ms. Hathaway proceeded to relate that the United States is confronted with unknown and known vulnerabilities, adversary capabilities, target exploitation, and weak situational awareness. There are numerous elements that contribute to crisis – the government and private sector networks and information are being exploited at unprecedented scale. By looking at multiple dimensions and, remote access, we need to address penetrations to our networks. The most persistent and weakest penetrations have occurred at supply points, which could impact and lower the price point of product lines. There are different categories of malicious activities and levels of sophistication that are increasingly severe and better organized. Terrorist groups, including Hamas, have shown much interest in penetrating our systems. The major targets include information and data, resulting in a multitude of illegal cyber activities, including credit card fraud and extortion. The motives of these activities range widely from curiosity and prestige to industrial espionage and subversion of our national security interests by hostile nation states. Above all, the cyber security strategies and various perspectives are overwhelmed, and compounded with the lack of understanding of the risks, have compromised the entire organization. It is survivability as national security aspect. The presenter pointed to two reference documents – 1) the Presidential Decision Directive/NSC-63 on Critical Infrastructure Protection which provides the foundation and cohesive strategies, and 2) NSPD-54/HSPD-23 and the Comprehensive National Cyber Security Initiative, which includes 12 projects, interagency and government-wide to form a defense. The strategies have key initiatives and foreign policy perspectives that include:

1) front line defense – to formalize network enterprise to a manageable size (DHS)
2) An interfacing connection to a manageable internet connection
3) A detection system before getting to your computer
4) A global liaison with FBI, NSA, Defense, national cyber security organizations, private telecommunications, military, and government entities

There are a number of challenges for consideration –

1) how to collate information and inform national leaders
2) how to define network to defend threats
3) how to create and reinvigorate the workforce and build life cycle practice
4) how to build security of spy network and the level of trust
5) how to save future environment 5-10 years from now
6) how to identify priorities and pressing science and research development on cyber security

When everything is brought together and priorities are set, individuals, selected institutions, 87 universities, and NSF will be approached to begin work on R & D on cyber security. The funding will be provided through IR, and competitions and awards will be initiated to drive innovations.

It was acknowledged that it is difficult to identify threats and espionage that are occurring daily. While the private sector is designing the technology, it is critical to use lessons learned to initiate a dialogue with the private sector. The government needs to extend its resources and create a partnership with the private sector.

The strategy must be holistic, with increasing capital and authority for law enforcement. The presenter stated that her office has made much progress during the past 18 months resulting in collaboration among agencies and executive branch and increased policies, interaction and understanding. There is still a need to bridge the gap between national and non-national security systems, and to address the future gap of cyber security. The government needs to rethink technical sharing, risk management, and functions, and to simultaneously consider how systems are built, operated, connected, and what and when to retire. The government has been reluctant to disclose the problems and threats to the public because of liability issues. There are a number of directions to be taken by the government: 1) to extend resources;2) to set up higher standards for national security; 3) to treat global IT industries as critical to security defense; and 4) to set up

action and accountability for long term investment and security measures. Presently, there are a lot of plans and initiatives, but no definitive actions from the government.

Meeting adjourned 4:51 P.M.

September 5, 2008

Started at 8:23 A.M.
Ended at 4:50 P.M.

Present:

Brian Gouker
Joseph Guirreri
Rebecca Leng
F. Lynn McNulty
Alex Popowycz
Philip Reitinger
Fred Schneider
Ari Schwartz
Peter Weinberger
Pauline Bowen DFO

Absent:

Jaren Doherty
Lisa Schlosser
Howard Schmidt

Visitors, presenters, panelists: 8
Donna Dodson, Matt Scholl, NIST's Computer Security Division

Dan Chenok opened the meeting at 8:23 A.M. with a recap of yesterday's discussion. The Board reviewed the draft Summary for June 4-6, 2008. Peter Weinberger proposed the motion that the Meeting Summary be approved and accepted, and the motion was passed with all in favor. Subsequently, the Board discussed the meeting dates for 2009 and it was agreed to hold the following three meetings in 2009.

1) April 1, 2, 3
2) July 29, 30, 31
3) December 2, 3, 4

Each meeting will begin on Wednesday with the first two days as full day agenda and concluding with a half day on the last and third day: The venue will be confirmed later.

Board Discussion
Dan Chenok, Board Chairman

- Einstein: The Board agreed to continue discussion on Einstein during the next meeting. There was a general disagreement on the premise that there is no privacy impact on scanning IP addresses. It was not a good precedent that PIA has been classified after release. Ari Schwartz discussed the possible points for drafting a letter to clarify the privacy impact to the PIA. The letter is intended to advise NIST and OMB of the required law and responsibilities to the public of relating classified information to unclassified system. Ari Schwartz requested for a motion to prepare the letter (Cyber Security Initiatives) to OMB and NIST. Lynn McNulty proposed the motion, which was seconded by Peter Weinberger. The motion was passed. Joe Guirreri had serious reservations with the letter. He asked that the letter be thoroughly coordinated in detail before being released.

- Rod Beckström – It was unclear to the Board how Rod Beckström proposes to implement his plan, including the relationships and responsibilities involved. It was agreed that the Board should attempt to provide feedback to Rod Beckström. It was suggested that the Board could invite Greg Garcia, Admiral Brown, or a career representative for further discussion on organization and how security and privacy are organized. The goal would be to provide advice on the structure. The Board will wait for the release of the commission paper before proceeding further..

- Melissa Hathaway – The Board did not have sufficient knowledgeable data to raise any questions..

- Potential Agenda Topics for December 2008 Meeting:
  1) The creation of a panel to discuss FIPS since FIPS has broad perimeters for interpretation which are difficult to enforce. There is a need to develop guidelines for consistent metrics and measurements for FIPS and defining the foundation and basis for

setting these measures and metrics. The process for approving FIPS is both lengthy and difficult to achieve a timely response. NIST Special Publications (SPs) do not require the same lengthy process, even though part of process is to display for public review (industry, agencies, public) to gather neutral responses and comments.

2) CPO – A possible panel to discuss the following: definition of the role, privacy knowledge, and related security aspect; the differentiation, if any, between CPO and CIO; definition of the privacy aspect; A consensus on the best practice that the industry uses to address privacy; and possible technical qualifications of the CPO

3) CSIS paper – To extend an invitation to Jim Lewis to brief the Board. The Board needs to decide to review and comment on the CSIS's draft paper. It is necessary to define NIST's involvement in CSIS. The Board plans to recommend to the Commission to consider the NIST presentation and to allow both NIST and CSIS to respond independently.

4) To decide on whether the Board is to prepare a statement or white paper regarding FISMA review.

5) Donna Dodson to invite Elaine Newton for discussion on identity management

6) To discuss Authentication

7) To discuss Privacy

8) To discuss Cloud computing

9) Briefing on NIST SP 800-53

10) To invite a representative from DHS to discuss technical questions on US surge and Einstein

11) To invite representatives from DHS and/or DOT re. transportation, regulatory approach on SCADA (panel) energy, e.g. Mike Castagna, DoC

Board Work Plan Discussion: Cloud Computing Conference Planning
Paul B. Kurtz, OMB

Paul Kurtz stated that he represents Karen Evans' view and the interest in the issues on public advocates He provided a draft outline of the forum tentatively scheduled for December 2008. With consideration of today's migration and the speed of migration, it is necessary for the government to keep up with the world, and to examine certification and accreditation processes. While Cloud computing is not part of the government, many government organizations are using it. The forum in planning is to gain government understanding through discussions, to raise awareness, and to explore the numerous aspects surrounding Cloud computing, e.g. models; trends; security applications, architecture and models; security challenges; relevance of current standards; and privacy. The forum is to be an educational program for the government and the incoming Administration. The forum will be an event hosted by this Board.. It was suggested to include speakers from major organizations such as Google, Microsoft, Intel, NIST, government agencies, think tank organizations, and individual experts.

NIST is presently conducting testing on a small environment to meet FDCC requirements (SP800.53 Recommended Security Controls for Federal Information Systems) – the security aspect with Cloud. The other issues to consider are how to handle cloud together with virtualization and how virtualization impact cryptography modules, etc.

Lynn McNulty, Alex Popowycz, NIST (Matt Scholl and Donna Dodson) and the Chair will assist in planning of the forum. It was agreed to hold bi-weekly meetings or teleconferencing for planning of the forum.

Privacy Technology Report
Dan Chenok, Board Chairman

The Chair reported that as the paper had not been released, therefore there was nothing to be presented for discussion or review at this time.

Board Discussion: Board discussion on transition letter for the old and new Administration
NIST Director and OMB Director

Lynn McNulty briefed the Board on every department that has a team responsible for transition. At the national level, OMB normally maintains the present cyber security initiatives to the next Administration. At the departmental agency level, CIOs produce a white paper on cyber security program and the accompanying issues to be decided by the next department secretary. The FISMA report is considered insufficient and inappropriate to be applicable as there are problems and issues that need to be reviewed and decided. Any specific reports should be handled by someone at OMB and not by this Board. There will be functional transition teams with particular attention to cyber security. The Board should present itself to the new Administration to make the most positive impact. Information security and privacy is considered critical challenges for many agencies. The Chair agreed to draft a two-page document highlighting the board's functions and roles, major security issues, sharpening cost cutting on security, and providing a view from the civilian's perspective of the government. The document will explain to the new Administration the key issues concerning the Board and the possible consequences. Dan Chenok will build on the comments provided in the outline and will distribute the draft to Board members. Lynn McNulty proposed the motion. All agreed thereby approving the motion.

Industry Security Officers Best Practices Panel
Glen Marshall, (MED US) HITSP (Healthcare Information Technology Standards Panel) Security, Privacy, and Infrastructure, Domain Technical Committee
Glen Marshall, Standards and Regulations manager, was elected as co-chairperson for the HITSP Security and Privacy Technical Committee. This committee is responsible for the selection of standards to protect patient privacy and healthcare information and system security in the U.S.

Deven Bhatt, Chief Security Officer at Airline Reporting Corporation
Deven Bhatt is responsible for physical as well as information security at ARC. He specializes in compliance, specifically PCI (Payment Card Industry), security architecture/management, audit and privacy. He has been instrumental in developing an internal security standard which harmonizes PCI, and other standards like ISO 27001, BITS. ARC became the first company in the airline industry to achieve PCI compliance in 2005.

The Chair introduced the speakers and explained that this panel was to provide the different perspectives between government and private sectors. Glen Marshall explained that he is using a presentation which was pre-approved for a web seminar. The objectives presented were:

- The core concepts related to security, privacy and infrastructure (SPI)
- The HITSP constructs developed to address SPI needs
- The core standards involved in the implementation of the HITSP SPI constructs
- Examples of how the SPI constructs are being implemented in the marketplace

To address health privacy and security, HITSP needs to deal with risks model base, privacy policy, permissive regime for life-saving purposes. This approach is dependent on auditing, and on privacy to be preserved by and expected from employers and medical practitioners. It is a relationship that exists between the patients and medical practitioners. Privacy is going to change as the focus is first to prevent harm to patients. Privacy is defined as an individual's

rights to determine whether, when, and to whom personal or organizational information is released. Security of health information is a defined set of administrative, physical and technical actions used or taken to protect the confidentiality, availability and integrity of health information. Health Information exchange is based on four criteria – persistence, stewardship, potential for authentication and inclusive of integrity and completeness. Integrity control is considered the most important. In order to ensure patients are getting the proper medical care, various controls are included in SPI Constructs. There are various provisions for basic consent, e.g. – options to disallow information for research and publication. Security begins with litigating risks. The presenter provided a web link for further review - http://www.himss.org/content/files/HITSP_Technical_Comittee_Orientation_2008.pdf

Deven Bhatt explained that Airlines Reporting Corporation's (ARC) core business is financial services. ARC provides the travel industry with financial services, data products and services, ticket distribution, and settlements in the United States, Puerto Rico and the U.S. Virgin Islands. It compiles and gathers historical transactions on travel agencies and airlines that need to be stored securely. The CSO is responsible for information and physical security, privacy, budget, development of new security program and team. He also conducts risks analysis in line with company's continued business plan, and maintains continuous compliance and monitoring regardless when the audit is performed. He considers raising people's awareness as the most important attribute to security and privacy compliance. In protecting confidential data, it is a challenge to identify where all data is and who are the users. Therefore, it is essential to enforce encryption on everything – laptops/desktops, email, database, mainframe, backup tapes, and CDs. Telecommuters must strictly adhere to all procedures whether on or off site in order to be allowed to work offsite. ARC has set up structures for monitoring and auditing access, and conduct regular testing on the systems. In pressing for full compliance, ARC provides a consolidated set of policies that are easy to read and follow. Most importantly, the comprehensive policies simplifies audits and compliance becomes a life practice.

Public Participation
There were no requests for public participation.

ISSLOB/TIC Update
Michael Smith, DHS

Michael Smith is the Program Manager at the Department of Homeland Security, overseeing ISSLOB/TIC program - The Federal Government's information systems security program. He provided an update on the latest developments. A status report has been publicly posted. The evaluation completed in April showed that two agencies demonstrated capabilities for full service, while another fifteen agencies were categorized as one/single purpose self serve. The number of TIC connections is not known. The objective of evaluation was to reduce the number of access points to less than 100. The mandatory and reference source is the OMB "Trusted Internet Connections" initiative which was intended to reduce the government's 4,300 access points to 50 or fewer by June 2008. They are working with 18 agencies on defining and refining function interpretation. The TIC would standardize individual external network connections so agencies can provide the connections for themselves or use the services of TIC Access Providers. There are over 100 agencies seeking service that will need to piggy back to other agencies while ensuring all needs are being met.

While focusing on reducing access points for reducing vulnerability, the question exists as to whether there are contingency plans when one of the two access points fails, and whether there are enough access points for each agency. Presently, TIC is developing plans to perform metrics and monitoring on access points, but it is still questionable if the accreditation boundary can be trusted. The other issue involves outsourced hosted service –allowing agencies data to reside on a server outside the agency connects to multiple internet. The system will have to be certified and must go through government entry point.

NIST is reaching out to the other agencies to set up Security awareness training. Agencies providing services must be SP 800-37 compliant. The closing proposal is due in the next few weeks and includes network mapping to ensure vendors have time to upgrade. ISSLOB has adequate funding for all four programs and also for any agencies which do not have an executive plan.

The Chairman adjourned the meeting at 4:28 P.M.

Pauline Bowen
Board Designated Federal Official

CERTIFIED as a true and accurate summary of the meeting
Daniel Chenok
ISPAB Board Chairman