Information Security and Privacy Advisory Board (ISPAB)

Summary of Meeting
November 3, 4, 5, 2010

Dates & Time:	Present:	Absent with apologies:
Wednesday, November 3, 2010 8:45 A.M. – 4:45 P.M. Thursday, November 4, 2010 9:00 A.M. – 4:15 P.M. Friday, November 5, 2010 8:15 A.M. – 10:57 A.M. Location: Washington Marriott Hotel 1221, 22nd Street NW, Washington, DC 20008 Meeting was accessible via webcast <http://csrc-nist.granicus.com/ViewPublisher.php?view_id=2	ISPAB Board Members: Dan Chenok Brian Gouker Joe Guirreri Lynn McNulty Alexander Popowycz Phyllis Schneck Fred Schneider Gale Stone Matthew Thomlinson NIST: Donna Dodson Matthew Scholl Annie Sokol (DFO) Megan St. Clair	ISPAB Board Member: Peter Weinberger

Wednesday, November 3, 2010

Dan Chenok, the chairman of the board called the meeting to order at 8:45 A.M., Wednesday, November 3, 2010. The meeting began with the discussion on replacing the positions vacated by the three members, Ari Schwartz, Jaren Doherty, and Lisa Schlosser, who have left the board since the last meeting. Donna Dodson (NIST), Matt Scholl (NIST) and Dan Chenok (Chairman) had met to discuss about possible new appointees.

The chairman introduced new member, Dr. Phyllis Schneck, McAfee. Following the introduction, each board member talked about individual news and new updates. The Chair reviewed the meeting agenda with the board members, and he also confirmed that the letter relating to NICE that was voted on last meeting was sent to OMB. Donna Dodson, Division Chief, Computer Security Division, NIST, provided the latest news at NIST and updates on a HASH competition in August, and the Annual Security Automation Conference that was held in Baltimore. Pat Gallagher, NIST Director, and Vivek Kundra, the Federal Chief Information Officer (CIO) at the White House, will kick off the Cloud Computing Workshop on Thursday, November 4, 2010, at NIST. She informed the board that Dr. Ron Ross of NIST has been selected to be a NIST Fellow. His work on FISMA has led to the FISMA Team winning a Gold Medal. Finally, Donna Dodson mentioned the latest staff movements - new hires joining NIST, Information Technology Laboratory (ITL), Jon Boyens and Suzanne Lightman.

Research Priorities of Moving Targets, Economic Incentives, Trusted Spaces

Pat Muoio, Science and Technology Lead for Cyber, Office of the Director of National Intelligence (ODNI) / Acquisition Technology & Facilities (AT&F)
(Presentation provided by presenter)

Donna Dodson introduced Dr. Muoio and her work on Federal Cyber Security Research. Dr. Muoio stated that she wants to move away from the R&D Space and toward trustworthiness of digital infrastructure. The

intention is to get coordinated research across the community. A set of research activities including a Science and Security component is also included in the research. She introduced three themes as starting point – 1) Tailored trustworthy spaces that support context specific trust decisions; 2) a moving target to provide resilience through agility, and 3) cyber economics to provide incentives to good security. The presentation includes explanation on each theme, the new paradigms and the challenges related to each theme.

The Moving Targets are like the bad guys in the good guy space, and the research is trying to integrate the good guys to become the moving targets. In the physical realm of Tailored Trustworthy Spaces, we operate in many spaces with many different characteristics. There are technical challenges as a lot of changes are needed especially for certifying the systems. She described different groups under DNI, SCORE, and CSIA, and the main focus of SCORE is to pinpoint what attacks to look for.

Before closing the presentation, she presented a major research initiative, "*Science of Cyber Security*" as the new emphasis area. The idea is to promote science based on understanding of the markets. Pat Muoio agreed with the board that there is relevancy to include Policy Space, and she would like to add some new themes for next year, e.g. wireless as part of the tailored space idea. They are slowly rolling out workshops sometime in January 2011. Fred Schneider suggested that a two-month turnaround by March 2011 would allow more time to engage the academia. Dr. Muoio mentioned that there is consideration to work on an updates for FY12. FY12 statement is presently being prepared under federal development research plan. The estimated time line for releasing the strategy is March 2011. Originally, there was no plan to publish the work with the twelve proposals, but now they intend to release publication with projected plan for the following year every March.

The board agreed to continue this discussion either informally with NIST or OMB. As this is a work-in-progress, Dr. Muoio preferred an informal dialogue until the document is complete. Dr. Schneider will be the liaison from the board on this topic with ODNI and Pat Muoio.

US Cert – National Vulnerability Database (NVD)

Chris Johnson, NIST, Computer Security Division
(Presentation provided by presenter)

Chris Johnson works at NIST and manages the NVD Team. He explained the functionalities of NVD and the data feed generated on the website is used as a weekly feed. NVD has been hosted at NIST over two years ago, but it is sponsored by DHS. The web page and the data are openly accessible to public. It is the US government repository of IT vulnerability information and it does not conduct any active patching or validation of the predictions. It contains over 44,000 vulnerability entries with data dated as far back as 1999. In 2009, the website received over 40 million hits, and the data holdings are used extensively by government, industry and academia. NVD components include national vulnerability database, National checklist program website, SCAP validation program website, and resources for SCAP. The database is tightly coupled with SCAP.

NVD Common Vulnerability Scoring System Support V2 (CVSS Version 2.0) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. The scoring data provides users the ability to compare what they need to pay attention to and what they need to fix.

Presently, the group is working on outreach to vendors so as to establish channels for comments and feedback. This will give credibility to the data. The NVD data feeds include product dictionary with over 26,000 unique product names, Beta Common Configuration Enumeration (CCE) is mapping to SP 800-53, and Spanish language vulnerability data feeds. Chris Johnson was pleased to add that NVD data feeds are machine-readable, and in July, there were 23,000 downloads and 992 downloads of the NVD CPE Product

dictionary file. They are also working on a combined name convention for CCE and CPE so as to have common identifiers.

In addition, NVD also includes National Checklist Program (NCP), resources for SCAP (Security Content Automation Protocol), and SCAP Validation Program website. The NCP web page contains 162 low-level checklists that are categorized into tiers: Tier I – Prose checklists; Tier II- Non-SCAP automated content; Tier III – Designed to work in a SCAP-validated tool; Tier IV- will work in a SCAP-validated tool. They are working on designing and deploying web services for SCAP products and are looking into Checklist Submission Process.

There are a number of areas that they are working to add to NVD, e.g. 1) creating CCE analysis and scoring capability, 2) to design, build, and implement web services to handle requests for NVD SCAP data products, and 3) to develop and deploy web services and interactive web portal that will streamline and expedite the NCP checklist submission process.

He confirmed that NVD received vetting from other governments, e.g. Japanese and European governments. Japanese has contributed to the database and dictionary. Chris Johnson believes similar database/web sites existed in other countries and companies such as Microsoft compile similar data for their internal use.

CIO Panel on Current Cybersecurity Perspectives

Casey Coleman, CIO, US General Services Administration (GSA)
Vance Hitch, CIO, US Department of Justice
Chris Smith, CIO, Cyber Security & Privacy Information, US Department of Agriculture

Dan Chenok introduced the panel and elaborated on the focus of the discussion. Casey Coleman started the discussion with brief presentation of her background. She is the CIO and leader in policy issues such as cloud computing at GSA. Vance Hitch is the CIO, Department of Justice and is the central authority for technology and cyber security at the agency. He is also the security lead on the CIO Council. Chris Smith is the CIO with the US Department of Agriculture and was CIO of world development. He is a Cyber security leader relating to Einstein.

Casey Coleman suggested that operational security and policy issues would be good start for the discussion. She stated that GSA is one of the first agencies to deal with cloud security and awarding procurement for cloud computing. While there are unresolved issues with cloud computing security, GSA's approach is to learn along the way. Application Security remains their primary concern as Security infrastructure is in a more secure stage. Third parties are responsible for 99% of application vulnerabilities. GSA security requirements are not as stringent as other agencies. She was assuming that GSA will apply FedRAMP process in handling virtual and cloud servers. Both Casey Coleman and Vance Hitch do not have a definite idea of when FedRAMP will be launched. Vance Hitch stated that presently the council is consolidating all the comments by year end with a focus on a possible release by January 2011. A draft policy has been prepared for continuous monitoring, and she would hope that cyber scope and continuous monitoring will eventually converge.

Vance Hitch has been working with the Federal CIO Council security committee for past five years. He has observed that large agencies have different components and complex environments. Vance Hitch/DOJ worked closely with Department of Homeland Security to be one of the first implementers of Einstein I. They have been slower in implementing Einstein II; the agency is ready to implement it once legal complications with the text are resolved. He proceeded to share the recent reorganization that he orchestrated so as to focus on cyber security, compliance, and vigilance on other extreme possibilities. As part of the reorganization for The Justice Security Operations Center, he implemented monitoring tools, data at rest, preparedness of possible PII incidents, and alternative for dealing with social media.

On the subject of FISMA, overall, he has been a supporter of FISMA but he would like to find ways to automate compliance reporting. After a year or two of following FISMA, the audits and follow-up questions are becoming a burden to him and his division in term of time and costs. It is his opinion that the federal government has outgrown FISMA and it should be changed.

Chris Smith described how the Department of Agriculture handled the security responsibilities that it performs in the government structure. He remembered when he first stepped into the position the department was facing a serious threat embedded in criminal activity, and the infrastructure was being attacked. They countered with a very aggressive restructure and he is happy with the progress. The program is showing signs of maturity. A year ago, they embarked on a mission on cyber security and are looking at configurations and patching updates. They had also started work on cloud computing – external cloud and internal cloud. They implemented remote access abilities, and considered using the PIV card at the end user for logon as an option. They would like to make the decision early next year, and in the meantime, users can still be logging on with passwords. It will not mandatory yet, but would like to have that resolved in the spring time. USDA is working closely with DOJ on implementing Einstein. Chris Smith thinks FISMA is fantastic but it is not as useful as it is intended. Monitoring is good but there is a consideration of costs, and he would rather be in a proactive position. He has sixty staff but he does not know if any of them have completed the cyber corps program.

In closing, Vance Hitch told the board that he would like to have funding allocated for research and development. Presently, they are doing things the hard way – waiting and reacting to an event. He felt that there is too much emphasis on cyber security, and spending is unsustainable and is imbalanced on risk management. Funding could be redirected from FISMA for cyber security or maintained vigilance to damage control which will reduce overhead and provide funding for R&D. Cyber security approaches are not coordinated among various departments and efforts are too fragmented, with each department implementing multiple solutions. In order to tackle a common focus on cyber security successfully, departments need to agree on a set of centralized efforts/solutions. He often referred to NSA for advices and directions. Vance Hitch also stressed the importance of collaborating with ISIMC (Information Security and Identity Management Committee). Casey Coleman emphasized the difficulties with direct hire and the importance to recruit outside talent.

Building a Cybersecurity Workforce for Industry and Government-Focus on SCADA Systems and Security and Reverse Engineering

Dr. Sujeet Shenoi, University of Tulsa
(Presenter withheld presentation for distribution)

Donna Dodson had known Dr. Shenoi and spoke highly of the cyber corps program. Dr. Shenoi's goal is to create well trained cyber security workforce in the US – real world approach and not the laboratory lessons taught in the universities. He elaborated on the set of additional programs and recommended unique courses only offered at Tulsa University. The programs have attracted many students from the Secret Service, DOD, DHS, FBI, IRS, NSF, ICE, and NSA. The course work includes hardware and software reverse engineering, forensics, cracking, keygenning, and working with various technology such as cell phone and cell phone chips, remote control, video game memory chips, etc.. The programs also open up opportunities to do research projects with various agencies such as information assurance, CIP, network exploitation intelligence, reverse engineering, pipeline situation awareness, SCADA network topology, device integrity, SCADA risk assessment, penetration testing, credit card skimmer, cell phone hacking, password cracking of mobile devices, and other security related projects.

Dr. Shenoi stated that this is a unique program and it is only the university in the US that works with FBI and Center of Intelligence Agency. The program is funded through a trust fund, and therefore, it is difficult to replicate and franchise to other schools. Each year, he sends four students to the SecretService so as to gain real life experience and experiment with new things. Secret Service has set up four laboratories in the US,

including one at University of Tulsa. Dr. Shenoi presented examples of attacks/hacking/penetration, and described how the analysis was completed on each case.

Dr. Shenoi explained his mission to create a well trained cyber security work force. He plans to offer the workforce training program to large student population through 2-year institutions. The program will include workforce training, an intense hands on component, and rapidly changing tools and techniques to meet customer demands from private industry, government agencies, law enforcement. The core curriculum will be information assurance principles, secure elective commerce, network security, enterprise security, and computer security. The program has funding from NSF for establishing in 40 institutions, and eight states. He has designed a mobile laboratory for easy curriculum dissemination to each program location. There are three things he is concentrating on: Curriculum development, Instructor Training and Workforce Development. His plan for next 4 years is to target large populated areas such as top fifty metro areas possibly among eight cities and/or eleven mid-size cities.

The meeting recessed at 4:46 P.M., November 3, 2010.

Thursday, November 4, 2010

The Chairman of the board called the meeting to order at 8:45 A.M. Gale Stone joined us via telephone.

Usability and Security

Mary Frances Theofanos, NIST
Ellen Cram Kowalczyk, Security Group Program Manager, Microsoft
(Presentation provided by presenters)

Matt Tomlinson, Microsoft, introduced the panel and explained the purpose of the discussion. The topic stemmed a discussion on usability at the last ISPAB Meeting in August 2010. There are multiple problems when approaching usability – people cannot always do the right thing and be compliance. We cannot simply have policies and expect people to be compliance. As users behavior change quickly, it is not practical to lock out users if they forgot passwords and/or misplaced their tokens. Mary Theofanos stated the definition of Usable Security: The extent to which a product can be used. She said the key is to keep the customer satisfied and taking into account that the user is often the most important part of a security solution.

On the subject of passwords, there are many different rules. People are required to use passwords but are allowed to record them anywhere. While many of us understand and expect people should understand the important of safe-guarding their cards and/or tokens, it is difficult for people to internalize the impacts of securing data, system, cards and/or tokens. Mary Theofanos maintained that enforcing these procedures put too much pressure on any users. Many organizations do not consider users as the most important part of a security solution. In addition, Ellen Kowalczyk added that some organizations do not completely understand or care about usable security, and therefore, they were reluctant to spend the money on single sign-on. They discussed the relationship between behavioral factors and the extent of what people will do to get around security when they are focused on completing their tasks. But until the users understand the cost, they will choose the easy way and may not follow the requirements and do the right thing. Mary Theofanos stated that they are working on how to show the consequences to the users. While training that includes an actual crash due to weak password usage is a good option, it is also costly. Ultimately, we need to transfer cost to users. They are looking into providing actual reporting of incidents as part of changing people's behaviors. The goal is to gather good usability data for NIST policy makers. Parts of the survey will focus on data to balance security, policies, stabilities, and guidelines.

Mary Theofanos recently conducted a pilot test for card and PIN use with the PIV from usability perspective. The users are allowed to access two applications with the PIV card, and therefore, users at NIST did not see any advantages to using their card to access their computers. Beside training and educating people, Ellen Kowalczyk stressed the values of using collected data to understand users' behavior and then provide appropriate guidance to help people to understand at least the minimum basics. They would like to make it easy for the user to do the right thing and hard to do the wrong thing, and easy to fix the wrong things when it happens.

Mary Theofanos and Ellen Kowalczyk discussed their current work at NIST and Microsoft respectively, and the challenges that they faced on usable security. Before concluding the presentation, they listed a number of research needs as well as security solutions and policies research. When wrapping up, the presenters described the next steps in securing funding to research in usable security and that usability will be embraced as the security solutions and security policies. The last sentence on the presentation is "*We can't meet the cyber security challenge without usable solution*."

Fred Schneider suggested a pilot research on using a device, such as cell phone, to authenticate access with identity management. This could be used as a model reference. Donna Dodson stated that Howard Schmidt, Cyber Security Coordinator of the Obama Administration, has shown some interests in this approach.

Mary Theofanos agreed that it will be beneficial for the Chair to inform OMB that the board had received a briefing on this topic. She also agreed that it would help very much to bring more awareness on this topic.

Domain Name System Security Extensions (DNSSEC)

Scott Rose, NIST, Advanced Network Technologies Division
(Presentation provided by presenter)

Update on DNSSEC
Scott Rose began his presentation with an explanation of DNSSEC and a brief historical background of DNSSEC development at NIST. NIST has been involved in DNSSEC development and deployment since 2000. There are four phases in the DNSSEC Incremental Deployment Plan as follows:

- Phase1: 2005-2010 Technology Development/Guidance.
- Phase2: 2010-2012 Deploy Signed DNS Infrastructure
- Phase3: 2012-2014 Deploy Validating Resolver Infrastructure.
- Phase4: 2014-> Exploit Trusted Naming Infrastructure.

They have completed Phase 1 and began Phase 2. Scott Rose proceeded to explain the components relating to the present state of deployment and the lessons learned. For Root Zone DNSSEC Deployment, US government maintains a "hands-off" approach and only approves change requests to the root and does not play any roles in key generation or signing. ISP's and universities are turning on validation, and Comcast has moved testbed to production servers. Windows 7 has DNSSEC as a managed policy setting. In closing, Scott Rose listed next steps in .gov are to finish Phase 2 and transition to Phase 3. When achieving Phase 4, the expectation is for using the DNS as a trusted infrastructure.

US Government Configuration Baseline (USGCB)

Steve Quinn, NIST
Suzanne Lightman, NIST

The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. The USGCB is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security. "The USGCB is a further clarification of the Federal Desktop Core Configuration (FDCC); specifically, the USGCB initiative falls within FDCC and comprises the configuration settings component of FDCC." – CIO Council memo dated September 15, 2010[1].

Since his work on FDCC, Stephen Quinn has been actively working with CIO council on many issues. He asked Suzanne Lightman to elaborate on the policies baseline because of her work with OMB and on policies. Steve Quinn discussed his work on FDCC, Policy, Policy continuity, administration changes, and the complicated process as FDCC evolved.

There are a number of lessons learned from the process. Firstly, it is difficult to measure effectiveness if there is no process in place to record the status prior to measurement. Secondly, if it is intended to do testing tools for a core configuration, it is necessary to ensure that these occurrences are on a predictable cycle. Thirdly, things need to be ready simultaneously. It happened that the testing tools that agencies that needed to use were not available. The new applications being used at the time were Vista and Windows XP, and therefore, they are only now testing Windows 7 and Internet Explorer 8.

He discussed how Technology Paradigm shift is not a sustainable process. The technology shift was when a company produces a product and they also create a thick security guide on how to manage it. The guide

[1] USGCB - http://usgcb.nist.gov/

needs to be formatted so any tool vendor could understand and implement on its system. SCAP validated tool is able to interpret the content and run it on the system to make sure it is compliant. This changes things in relation to producing baselines. NIST will now be participating in updates and updating patches which will be costly. Industry is beginning to assume some of these responsibilities. Steve Quinn also discussed the checklist program presented in Special Publication 800-73 Revision 1.

NSTIC and Privacy Issues

Naomi Lefkovitz, Federal Trade Commission
(Presentation provided by presenter)

Naomi Lefkovitz has worked in Privacy and Identity Protection at Federal Trade Commission for over nine years ago. Her first task was on identity theft program. Naomi Lefkovitz presented the overview of NSTIC (National Strategy for Trusted Identities in Cyberspace) and the focus on privacy and identity. The vision of NSTIC calls for the creation of an online environment[2]. The coordination of existing programs for the government and private industries influences the success of NSTIC. NSTIC offers benefits to individual, private sector, and the government. There are four guiding principles: Security, Privacy, Interoperability, and Easy-to-use. This strategy identifies four types of participants: individual, identity provider, attribute provider, and relying party. She iterated that the intent of the strategy is to carryover the benefits from the offline world and the baseline focus is not intended to take away anonymity from anyone. In closing, Naomi Lefkovitz briefed the board a series of next steps which include providing a clear strategy for President's signature, conduct review of implementation plan, establish national program office, complete and release of the implementation plan, and execute implementation activities.

The meeting recessed at 4:25 P.M., November 4, 2010.

[2] http://www.whitehouse.gov/blog/2010/06/25/national-strategy-trusted-identities-cyberspace

Friday November 5, 2010

The Chair called the meeting to order at 9:35 A.M.

Direction of the Cyber Security Agenda

Suzanne Lightman, NIST

Suzanne Lightman has recently joined NIST after working for sometime with Howard's office at the National Security Staff. Prior to that position, she was with OMB. Suzanne Lightman was to share with the board of the directions that OMB and White House are planning, and also on issues related to national security

Suzanne Lightman first described PDs and their status – revised or current. She said that Howard Schmidt's office is working very hard on the NSTIC within the government and also on the national front. NSTIC is more about resilience for public use than the government. CNCI had a series of twelve initiatives that were processed through Howard's office. Presently, the issue of supply chain is under serious discussion, which is an initiative under CNCI. Howard Schmidt's office is working hard on how best to approach this issue and how you make the internet more resilient. She also touched on National Cyber Incident Response Plan (*NCIRP*) and Cyber Storm 3. Every agency has different authorities, and authorities are scattered among various agencies. There are concerns about communication with authorities to respond to incidents and critical events. Plans are being initiated to update the procedures. Howard Schmidt is seeking interagency feedback on Cyber Storm III.

With regards to NSTIC, DHS has come to realize that it needed to set up a center to cover the necessary work and as an entry point for the industry. Since classified information is highly regulated and it is difficult to share/pass them to various agencies, it is necessary to consider the private industry on how to gather information and allow accessibilities to the public.

Suzanne Lightman described the current public status of Einstein II and how a detection system is being brought up. Both NSTIC and Einstein III involve areas of Communication and Information Infrastructure. OSTP is responsible for examining the government side extensively while NSS is to cover other areas. There had been extensive discussion re. Einstein III with international, interagency committees, cyber crime communities, secret service, and USDOJ. This is to ensure everything is inline with policies, laws and environments. There is an enormous distrust among parties. With so many different committees representing every sector, it is necessary to establish communication channels between private companies and government agencies. The needs for setting up an information correlation center for NSTIC so as to formulate policies and decision making responses to cyber security incidents.

This led to the discussion of cyber security spending. Presently, government agencies are allocated specific and do not have actual cyber security budget. Many agencies mainly include many cyber security activities/spending in project budget. Therefore, it will highly difficult to find out what agencies actually spend on cyber security. Howard Schmidt's office did compile a list of priorities that require funding for discussion with OMB. They are also looking into creating a job series for cyber security.

Congressional Update regarding Cyber security

Update on Current Legislative Proposals
Davis Hake, Legislative Assistant for Congressman James R. Langevin
Jacob Olcott, Counsel for the Senate Commerce Committee

Jacob Olcott has moved to Senate Commerce working on Committee staff, he came from House of Homeland Security Committee after 4.5 years. While Davis Hake joined the congress after Jacob Olcott, he realized that cyber security is a big problem. He acknowledged that Howard Schmidt has done a great job, and it is good to have White House to lead this initiative. The US House Cybersecurity Caucus introduced a bill that will

establish strong, centralized oversight to protect the nation's critical information infrastructure and esign a comprehensive policy for operating in cyberspace (The Executive Cyberspace Authorities Act of 2010)[3]. Congressman Jim Langevin worked with Representative Diane Watson on a bill that makes important updates to the Federal Information Security Management Act (FISMA) and establishes a National Office for Cyberspace in the Executive Office of the President[4]. Davis Hake also mentioned that Congressman Langevin introduced the Homeland Security Network Defense and Accountability Act[5], which passed the House on July 30, 2008. In addition, there are movements on the electrical grid, and commitment to protecting vulnerabilities in our critical infrastructure sectors, from water systems and chemical facilities to financial systems and hospitals. Presently, they have yet to address SCADA systems. In the area of Defense Authorization, they are exploring budget and cost burden in federal contracts with the congressional budget office.

Jacob Olcott did not think this year will be year for comprehensive cyber security legislation. He is working under the leadership of Senator Reid. He further emphasized the seriousness of the issue especially when an incident occurs. Senator Reid wanted to have bills merged by August 1st. There are on-going conversations with Homeland Security people and Senator Reid's people and many other committees. They are waiting for feedback from the administration. Senator Reid had written to the president requesting for help on defining the scope. Jacob Olcott was expecting to get a response very shortly.

Jacob Olcott elaborated on issues relating to the bills: On initial review of the two bills: commerce and HLS bills, it would seem that they are two different approaches. After taking a closer look, it will reveal many similarities, e.g. R&D is an agreement, workforce issues, standards issues, presidential authorities. He maintained that there is no kill switch. Senator Rockefeller's approach of introducing the bill is a mean to start a public dialog on Critical Infrastructure.

On looking toward next year, he predicted a number of fundamental issues that must be addressed:

- Smart Grid – particularly security, privacy and how to expand the flow of information across borders. They will be major issues for the government and for NIST especially as we move toward telecommuting.
- Security of the Global supply chain – particularly trust. It is a very specific concern in the intelligence community.
- Cloud Computing
- Standards
- Internet governance
- Health IT security

Jacob Olcott welcome the board to talk to them about any issues or concerns.

Board Discussion During the 3-day meeting

Board members

Board Discussion, November 4, 2010
The Board approved the August Meeting Minutes with no comments. A motion was proposed by Lynn McNulty and seconded by Matt Thomlinson.

The board and NIST will continue to work on filling the open board member positions. The Chair asked the board to recommend candidates for consideration.

[3] http://housecybersecuritycaucus.langevin.house.gov/news/press-releases/2010/05/bill-creates-national-cyberspace-office-centralizes-cyber-protection.shtml
[4] http://langevin.house.gov/news/press-releases/2010/05/prcyber052810.shtml
[5] http://langevin.house.gov/legislation/issue/cybersecurity.shtml

Review of presentations during the day:

- Pat Muiuo's talk: the board was encouraged to provide feedback to Pat Muoio. Fred Schneider is scheduled to talk to Pat Muoio on Monday, November 8, 2010, and the board members should send any comments and/or questions to Fred Schneider by Monday.

- Chris Johnson's discussion on NVD: It was agreed that it is good to have correlation but be wary of possible exploitation. The board expressed concerns of the openly accessibility of analysis of vulnerabilities at one location with no monitoring or tracking of activities. Matt Tomlinson would like to see real world data. Dan Chenok would like to get more information/feedback from NVD through Donna Dodson. Lynn McNulty agreed to be the lead to gather the emails.

- CIO Panel: Joe Guirreri thought the CIOs need additional guidance from OMB guidance as it seemed that they did not know what they are supposed to do with their CNA programs. Lynn Nulty thought it would be helpful for OMB take a look at Special Publication 800-30, Risk Management Guide for Information Technology Systems. It might be worthwhile to push for an update of the document as the present version was last updated in 2002.

  On the subject of Direct Hire Authority, the board sympathized with the panelists. The board would like to work Ernest McDuffie from the NIST NICE team on moderating a panel on direct hire. Alex Popowycz thought the coordination should be tighter and maybe to conduct some cross agency activities.

- Shujeet Shenoi's presentation on Cyber Security Workforce: Fred Schneider is curious to see how well the program is received in the government. The program does not really teach students to be good researchers or giving the students the foundation to continuing educating themselves and to be able to deal with changes for a long time. The program is too narrowly focused and lacks balance between hand-on and theory. Phyllis Schneck noted that he is providing information to three different groups: the Secret Service, technical people, and general. Donna Dodson stated that 90% of his students work for the secret service, and the remainder work for NSA and NIST. Lynn McNulty was very intrigued by what Dr. Shenoi was doing at the community college level. SCADA systems research, Lynn McNulty believed that there are benefits to broaden the scope.

- Discussion on Usability element: the board believed there is need to take this issue seriously, and a letter should be drafted to OMB. A draft letter was prepared and reviewed the board on November 5, 2010, which was approved by the board. A motion was proposed by Lynn McNulty and seconded by Matt Tomlinson.

- Naomi Lefkovitz's presentation on NSTIC: It was unclear as to where the authority is placed and no clear implementation plan was provided.

Board Discussion, November 5, 2010

The board discussed the advantages/disadvantages of continuing Webcast of the meeting. During the 3-day meeting, approximately 30 visitors viewed the web cast with the first day of meeting receiving the highest number of visitors. Various options/approaches were suggested, e.g. web casting part of the meeting with a focus on certain agenda items/subjects. Donna Dodson, NIST, stated that NIST is open to transparency. While there are many positive aspects of web casting, the board needs to be act cautiously. It was decided to include webcasting at the next meeting but take one step at a time in experimenting with more interaction, e.g. use the web for interactive discussion and perhaps include an online panel. Matt Scholl reported of technical difficulties with allowing public to submit comments.

Action Items and possible agenda items for next meeting:

- We need to invite Howard Schmidt to our next meeting
- NIST update (Donna Dodson)
- FEDRAMP – a year end update from Dave McClure
- DHS Updates (Phil Reitinger)
- Access to classified information to improve cybersecurity (DHS)
- Review of OMB appendix 3 burden vs. benefit
- Direct Hiring, training vs. education, retention - Ernest McDuffie, NIST (NICE)
- Addressing issues with Sujeet
- IG panel (to be arranged by Gale Stone)
- Panel involving how to properly declassify information regarding Cyber Security
- DOD, DHS, DOJ Sharing information – Briefing on this
- NSTIC – Briefing and implementation plan
- Revisiting TIC and Cloud conflicts- DHS memo on how Cloud works with TIC
- HSPD12 and PIV being used in the government
- Overlapping networks- private clouds, public clouds and hybrid
- Security of Network Medical devices from August 2010 meeting
- NCICC and Cyber Storm 3 lessons learned.

The next ISPAB meeting is scheduled on March 2, 3, 4, 2011. The location is yet to be confirmed.

The board did not receive any requests/questions relating to this meeting from public.

The ISPAB November 2010 Meeting adjourned at 12:30 P.M., November 5, 2010.

Presenters	Visitors
Research Priorities of Moving Targets, Economic Incentives, Trusted Spaces Pat Muoio, ODNI ***US Cert – National Vulnerability Database*** Chris Johnson, NIST ***CIO Panel on Current Perspectives on Cybersecurity*** Casey Coleman, GSA Vance Hitch, US Department of Justice Chris Smith, USDA ***Building a Cybersecurity Workforce for Industry and Government-Focus on SCADA Systems and Security and Reverse Engineering*** Sujeet Shenoi, The Center for Information Security ***Usability and Security*** Ellen Cram Kowalczyk, Principle Security Strategist, Microsoft, Trusted User eXpereince (TUX) Mary Francis Theofanos, NIST ***Domain Name System Security (DNSSec)*** Doug Montgomery, NIST Scott Rose, NIST ***US Government Configuration Baseline*** Stephen Quinn, NIST Suzanne Lightman, NIST ***National Strategy for Trusted Identity in Cyberspace and Privacy*** Naomi Lefkovitz, Federal Trade Commission ***Discussion with the National Security Staff*** Suzanne Lightman, NIST ***Update on Current Legislative Proposals*** Davis Hake, Congressional Staff Jacob Olcott, Legislative Assistant	Angela Prentice WINS, Greenbelt, MD Jason Kerben DOS, Arlington, VA M. Rie University of Tulsa, Tulsa, OK Jocelyn Farah Ex-USAF, University of Tulsa (McLean, VA) J. Clifton Excalibur Associates Alexandria, VA Paul Suh Jonathan Butts Air Force Institute of Technology Shawnetta Davis Dakota Consulting Silver Spring, MD20910 Keren Cummins nCircle San Francisco CA 94105 Approximate e-Visitors through webcast link: Varies throughout the 3-day meeting between 3 and 30