Information Security and Privacy Advisory Board (ISPAB)
Summary of Meeting

October 26, 27, and 28, 2011

Courtyard Washington Embassy Row, 1600 Rhode Island Avenue, NW, Washington, DC, 20036

	Present:	
	Board Members	Non-Board members
Wednesday, October 26, 2011 8:30 A.M. – 4:45 P.M. Thursday, October 27, 2011 8:40 A.M. – 4:30 P.M. Friday, October 28, 2011 8:30 A.M. – 11:30 P.M.	Dan Chenok (Chair) Kevin Fu Brian Gouker Joe Guirreri Toby Levin Ed Roback Phyllis Schneck Gale Stone Matthew Thomlinson Peter Weinberger	Cita M. Furlani Charles Romine Matthew Scholl (DFO) Annie Sokol (DFO) Megan St. Clair See Annex A for record of presenters and visitors

Wednesday October 26, 2011

The meeting was called to order at 8:30 A.M. The Board members provided updates of their recent activities. Cita Furlani introduced her successor, Charles Romine, who will be the new Director of Information Technology Laboratory, NIST, when she retired. Dan Chenok acknowledged Cita Furlani's support and leadership, and extended welcome to Charles Romine. The Chair also welcomed three new members to the Board, Kevin Fu, Greg Garcia, and Toby Levin. Jason Miller, Federal Radio, had graciously agreed to record the meeting and produced a podcast for the Board. Jason Miller will also be publishing a report of this meeting.

NIST Updates

Matthew Scholl, Deputy Chief, Computer Security Division, NIST

Matt Scholl provided the NIST updates as Donna Dodson, Chief, Computer Security Division, NIST, was on travel and will not be able to participate in the meeting. He discussed updates on the recent international engagements between NIST and other countries in the recent months. He then reported on the successful launch of Computer Security Division (CSD) reorganization. The reorganization will not involve any relocation of personnel to other divisions. Donna Dodson is the division chief of CSD and also the Acting Chief of the Advanced Network Technologies Division (ANTD). The search is ongoing for the suitable candidate for Chief, ANTD. Matt Scholl also provided information on budget trends for FY 2006-2012 as presented by the NIST Director. While appropriation history demonstrated increasing funding since 2006 it will decline in 2012, and there are possible impacts to stakeholders and mission of NIST. It is critical to have a plan to ensure holding strategic production with reduced budget. Ed Roback complemented Cita Furlani for being able to have good control of the situation. The Board requested to have information on CSD's portfolio program so as to provide input to the strategic plan. Matt Scholl agreed to send the

information this week. Matt Scholl next reported on past and future conferences and workshops either organized by NIST or involved NIST's participation. He discussed the list of Special Publications that were released during the past months. The Board stated an interest in organizing a panel on cloud computing relating to the latest publications, SP 800-146, Draft Cloud Computing Synopsis and Recommendations, and SP 800-144, Draft Guidelines on Security and Privacy in Public Cloud Computing. Finally, he reported that there is no announcement of SHA winners.

SP800-53 Appendix on Privacy (Presentation provided)

Ron Ross, NIST Fellow
Roanne Shaddox, Sr. Privacy Specialist, FDIC

Dr. Ross began with stating that they are trying to integrate Privacy and Security into the SP800-53 and that Security and Privacy needs trust in order for it to work. Presently, there is no clear definition of privacy as it is difficult to define the various context of privacy. Furthermore, privacy and security groups did not connect in the past. FISMA defines privacy as part of information security (SP 800-122). He talked about the Threat Space and how it is always getting more sophisticated which causes issues. Some unconventional threats affecting security and privacy are complexity, connectivity, and culture, and that mainstreaming Security and Privacy as being first order requirements. He focused on mutually supporting objectives and digital footprints. Efforts are focused on simplifying the enterprise architecture. There are three tiers (Organization, Mission Business Process, and Information System) for Enterprise Wide Risk Management, and he elaborated on the roles that each tier functioned. He proceeded to explain a new Risk Management Process: Assess, Respond, Monitor. He talked about using Privacy Control Families that are based on the Fair Information Practice Principles (FIPPS). There are eight families:

- Transparency
- Individual Participation and Redress
- Purpose Specification
- Data Minimization and Retention
- Use Specification
- Data Quality and Integrity
- Security
- Accountability and Auditing

Ron Ross explained the steps for implementing these families. The benefits would be simply having the structure and discipline. The goal would be to have better privacy overall as Privacy and Security are tied together more than ever.

This document is to provide a structure and controls but the agencies should be responsible for privacy policies. Comments were received for SP 800-53 Rev.3. Privacy will be incorporated in SP 800-53 Rev.4 due out December 2011, with plan to finalizing SP 800-53 Rev.4 Appendix J on or after March 2012. The Board would like to review the document and also to invite both presenters to return with the updates.

Roanne Shaddox continued the discussion to cover privacy controls. She and the Federal CIO Council Privacy Committee are very excited to work with NIST. It took time to review the FIPPs, categorize the controls and then draft Appendix J. The collaboration produced a White Paper on the element of a privacy program and simultaneously leveraged those parallel activities. The Privacy

Committee was in the process of developing privacy controls and turned to Ron Ross and Erika McCallister for feedback, and to align privacy with security functions and to integrate controls in key information security functions. FICAM has defined key privacy controls while SP 800-53 Appendix J provides even more guidance. They have yet to do the mapping between these documents. Roanne and Ron will continue to look to the Board for feedback.

Consumer Privacy

Ari Schwartz, Senior Internet Policy Advisor, NIST

The Board invited Ari Schwartz so as to discuss how best to provide input and help in this area. Ari Schwartz began his presentation on the White Paper that was released a few days ago but was slightly edited from a bill drafted a year ago. Ari Schwartz suggested that the Board could reach out to the Chief of Staff for the Commerce Secretary. Ari was only recently detailed to the Secretary of Department of Commerce. His tasks include helping the Secretary of Commerce, who was sworn in the past week, with policy program; with specific focus on three areas, being a commerce level representative; approving policy oriented interactions between secretaries and three technology agencies; and Internet policy taskforce (commercial policy for the internet).

Ari Schwartz reported on the released notice of inquiry (NOI) on a number of Green Papers. The Green Paper on Privacy provides the discussion of the Fair Information Practice Principles; also the traditional US view on privacy. They are working on promoting the idea. The goal is a broad principle based Framework. Presently, there is an effort to address mobile marketing. They are working on moving it into the government space, which should translate well.

Certainly, they are interested in reviewing the privacy paper from NIST SP 800-53 as it is a natural fit with the Green Paper's Privacy Impact Assessment Model. The Green Paper was written by the Department of Commerce (DOC). A belated White Paper is being drafted by the NSTIC. The White Paper is projected for released sometime this fall. A public meeting is planned and hosted by DOC when the White Paper is released.

He stated that they had put out a Green Paper on Cyber Security as well, which is similar to the Privacy Green Paper. In a year they should have new policies or practices. The main thing is to have proof of concepts and successful multi-stakeholders. Interaction from the Board is always helpful, but there is nothing specific at the moment.

Updates from Howard Schmidt

Howard Schmidt, Cyber Security Coordinator and Special Assistant to the President

Mr. Schmidt's discussion was to emphasize that what they are doing is relevant to government systems, DHS's role, and Cyber Security Month. In addition, there are the three priorities in government systems: What is going on; What is coming in and out of Government Networks; and the focus on PIV cards. One could be compliant with FISMA according to FISMA and could still be insecure. But using continuous monitoring could fill the gap. He raised the issue of handling risks. They have been evaluating sub-units of Government Agencies, and DHS has been involved in applying a CIO effort and a CISO effort. Mr. Schmidt also said they are looking at government-wide security controls, in which GSA is key with their MTIPS program (Managed Trusted Internet Protocol Services). He confirmed that Einstein II is progressing.

For Identity Management, they are working on both a national and international level. The state version of FICAM is SICAM. The implementation of HSPD12 must be executed fully for both physical and logical access. In Mr. Schmidt's words, "HSPD-12, we have to do it, we have to use it too." People need to start moving away from password login. Open Identity solutions for open government would make the end user experience a lot easier; Mr. Schmidt referenced the Memo[1] from Steven VanRoekel on accepting externally-issued identity credentials that will make life easier for end users and allow the use of online identity credentials. They are exploring developing a global process. In order to monitor progress and step up coordination across all agencies, information will be provided for people to check milestones and also to monitor and to assess progress. Pilots are planned to assess effectiveness.

He touched on Awareness and Prevention, and reported that the NICE program has been institutionalized. Education will make people become more aware of the process. He also talked about the issue of everything being classified, which makes it difficult for small businesses to be involved. There is a lack of recognition on what the Private Sector is doing.

FISMA Reporting is still in need of improvement. FISMA has over 120 questions. The White House wants to maintain as the top priority as budget is reduced. Mr. Schmidt commended Cita Furlani for putting ITL's agenda together and being able to keep all moving parts together. The Board did not have any questions, but Mr. Schmidt would like the Board to think about a workplan for the next year.

The Future of Cyberdefense[2] - An Information- Centric View

Tony Sager, Chief Operating Officer, Information Assurance Directorate, National Security Agency

Tony Sager has been at the National Security Agency for 31 years where he started as a COMSEC intern doing cryptography. Nowadays, he makes public speeches about security. He described the lessons he learned over the years: 1) finding an answer is not where it should be as it is often found somewhere else: the information that we receive is usually not in the form needed for you to solve the problem. 2) The bad things that happened to you today probably happened to someone somewhere yesterday and could happen to someone tomorrow. 3) After you have cleaned up what has happened, there are probably many signs in the environment that you missed.

He stated that Cyber Defense is really an Information Management problem and the goal is to think of it as information and not as an action problem. Where there is a known problem, there is also a known solution. Mass Information Sharing is overrated, and can be addressed by a learning system with global visibility. NSA has restructured around information, making information accessible. Tony Sager described DHS Security Automation Handbook that he is working on other agencies. He discussed managing trust and how it is becoming a negotiated condition all the time.

[1] http://www.cio.gov/Documents/OMBReqforAcceptingExternally_IssuedIdCred10-6-2011.pdf

[2] Overhack.wordpress.com/2011/10/11/tony-sager-the-future-of-cyberdefense/

Cyber Awareness Month – Updates and Report (Presentation provided)

Bill Newhouse, Cybersecurity Advisor, NIST

Bill Newhouse joined NIST in March of 2010. CNCI was a major focus when he came to NIST. He joined the Computer Security Division at NIST in January 2011 and started working on the National Initiative for Cyber security Education (NICE). When ISPAB was first introduced to NICE, the work was still in the infancy. NICE has since advanced to a 'toddler' position. Receiving more funding has aided NICE's progress. He talked about the four components of NICE. The draft NICE Strategic Plan received over 490 comments when the comment period ended October 3rd. A new booklet was produced for the 2nd annual NICE workshop, September 2011. The Workforce Framework was released with a curriculum and comment period to close end 2011. The workshop was video webcasted, all webinars will be up on the website, and a NICE Participant Supplement Report made available.

They had just established MOU with the Department of Education, NIST and the newly formed National Cybersecurity Education Council. Bill Newhouse explained the Planned Activities/ Goals, some of which are to raise awareness among the American public about the risks of online activities, broaden the pool of skilled workers capable of supporting a cyber secure nation and develop and maintain an unrivaled globally competitive Cyber Security Workforce. He stated that DoD is not going to implement its own framework but follow NICE framework.

DHS led the Cybersecurity Awareness Month, and some of the main events of Cybersecurity Awareness Month were the following shared responsibility; *Stop. Think Connect* Campaign; Formal Education and Workforce Development; Cybercrime and Law Enforcement; and Online Security for Small and Medium sized businesses. The *Stop. Think. Connect* campaign is focused more on teenagers and parents.

Bill Newhouse felt there should be more advertising of many of these events, and there should be more ways to bring awareness in the years to come. But he is not sure how best to get the message out more widely. There are needs to gather data to identify gaps and to conduct studies. The ISPAB gave some suggestions, including Brian Gouker's suggestion of getting on Channel 1, which is a wide known Television channel for High Schools. Another suggestion was to get a young celebrity to promote cyber security.

The meeting recessed at 4:45 P.M., Wednesday, October 26, 2011.

Thursday October 26, 2011

The meeting resumed at 9:18 A.M.

FCC and Technology (Presentation provided)

Robert Naylor, Chief Information Officer, Office of the Managing Director, Federal Communications Commission

In his presentation, Robert Naylor provided a definition of cyber security, the Cyber Security State of the Union and the U.S. President's priority with cyber security. He described the information technology approach and explained cyber security. He stated that we are trying to help others but we need help ourselves, and we need systems that are more proactive than waiting for human responses. It is important to keep up-to-date in cyber security. FCC's cyber security vision includes a list of target goals/milestones. With increasing security, there is an increasing cost. There are a lot of different threat vectors, and he provided a list of 2011 major attacks and breaches in the news which were committed by mostly anonymous hackers. He identified the hackers and some known major hacking organizations. FCC is still at risk as the defenses are not yet matured. Two risks that FCC faced are internal threats and external threats.

Mr. Naylor described the ongoing activities that the FCC CIO and CISO have been doing since April 2011. He talked about the multiple visits to different agencies including Department of State (DOS), Department of Homeland Security (DHS), the National Security Agency (NSA), and the FCC. There were some field office visits to Gettysburg and Atlanta as well. The FCC has also published some directives including the FCC Directive 1479.4, Cyber Security Program.

Mr. Naylor talked about the FCC cyber security vision: FCC to be the Center of Excellence for Federal cyber security. They are looking at working with other agencies on this. FCC will incorporate and create best practices for continuous monitoring and executive dashboards. He described NSA and DHS Blue Team. DHS would have a certain role as will NSA. One of the main things he wants to focus on is periodically practicing real life breach and data integrity scenarios. He also touched on FISMA's role. In Conclusion, the cost reputational damage and congressional oversight after a major FCC breach will be much more expensive. Before an annual training program is planned, they need to figure out a way to help people understand the importance of the training.

The Board stated that they would like to hear from him again on what steps they are taking.

OMB Discussion
Carol Bales, OMB
Lisa A. Schlosser, Deputy CIO Federal Government, OMB

Carol Bales had participated in discussions with this Board while Lisa Schlosser had participated as presenter and as a former member of this Board. Lisa Schlosser started her position as Deputy CIO for OMB about three months ago. She talked about Steven VanRoekel's agenda and the expectations. Mr. VanRoekel was previously from FCC and responsible for putting up the broadband map. He was one of the first 1000 employees at Microsoft, and left Microsoft about four years ago. He is a combination of a 'business guy' and a 'techie'. There are three areas that he is focusing on: 1) How to be smart and to find areas to cut costs and find savings; 2) How to enhance productivity in government such as mobile tool security, mobility, and capability; and 3) to look at

the government from the outside such as messaging, domain, and to work on the websites. One initiative is the dot gov reform. Apart from these focused areas, architecture is a big issue. There is a need to get rid of duplicative networks and refocus on more shared IT. There are many resource systems across government agencies costing ~$2.4billion.

Lisa Schlosser stated that Steven VanRoekel has cyber security on his agenda. In addition, the release of Memorandum M-10-28, that "*outlines and clarifies the respective responsibilities and activities of the Office of Management and Budget (OMB), the Cybersecurity Coordinator, and DHS, in particular with respect to the Federal Government's implementation of the Federal Information Security Management Act of 2002 (FISMA; 44 U.S.C. §§ 3541-3549).*" This memorandum was released within the first three weeks after Steven VanRoekel took office, and it defines that "*effective immediately, DHS will exercise primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within FISMA under 44 U.S.C. §3543.*" Howard Schmidt's office will focus on Continuous Monitoring, Einstein, TIC, and HSPD12. The memo relating to FedRAMP will be cleared for release very soon or possibly within the next couple of weeks. It will set the process for other areas for longer term and scale up for cyber security.

Carol Bales has been the Identity Management Lead for the past five years. She has worked on the Open Identity initiative, and she provided a list of the key activities for HSPD-12. She also worked with the CIO Council on the PIV-Interoperability guidance for non-federal users in July 2010. On February 3rd, Memorandum M 11-11 was issued, which details logical access usage for agencies. It is not a mandate, but follows up on investment for implementation of PIV cards. It is also a measurement of how complete is the solution for using PIV card for logical access. Carol Bales provided the status of PIV card issuance. They have been following up with agencies on issuance of PIV cards, and to date, over 5 million cards have been issued. There were many questions from agencies, including whether it is mandatory or optional to use the cards. They are looking at all the different IT investments through their research with CyberScope.

A discussion followed on the October 6, 2011, OMB memorandum: Requirements for Accepting Externally Issued Identity Credentials. They are meeting with agencies to discuss trust framework and policies. While agencies were very supportive, there were some concerns about accepting externally issued credentials at a higher level. The Board would like to have a discussion at the next meeting on topics relating to derived credentials, PIV, FICAM, and NSTIC. A number of questions were raised, e.g. should US data be stored outside of the US; does the USG want to store anything outside of the US; the issue of supply chain and the use of foreign help desk.

She then talked about the FICAM roadmap from a privacy perspective, there is a lot of information in the FICAM roadmap, which provided good protection on the privacy level. She explained FICAM performance metrics and a few of the key end state targets of HSPD-12. NIST is in the process of completing the revision of FIPS 201 where mobile devices will be addressed. The main end goal is that users will only need to have their pin cards and their 6-digit pin. She said they would be releasing Part B to the FICAM Roadmap that will include more guidance but not so many requirements.

Upcoming activities and next steps: The NIST updated FIPS 201-2 will be coming out soon in 2012, but it will depend on the mobile issue. She talked about users running into issues when trying to

use the PIV card with older systems. Mobile devices are the biggest inhibitor to using the PIV card, and not every system will be enabled to use the PIV card.

National Vulnerability Database (NVD) International (Presentation provided)

John Banghart, Security Automation Program Manager, Computer Security Division, NIST

John Banghart began his presentation on domestic vulnerabilities, international vulnerabilities, and securing systems. In general, many nations do not have an inventory of their systems. The researchers in China have put out a proposal for an international alliance, in which they proposed the idea of shared understanding and expanding to more than a single repository. There was much vulnerability with many different names. Now, there is still much vulnerability, but with fewer names, and fewer names lead to quicker fixes.

John Banghart next explained how the National Vulnerability Database (NVD) works. The NVD assigns names to the vulnerabilities and then shares the research after identifying the vulnerabilities. MITRE searches for information to make sure it is a legitimate vulnerability. A CVE (Common Vulnerabilities and Exposures) number will then be assigned. The information will be forwarded to NIST's NVD Map Score before publishing the vulnerability. NIST has four analysts to handle implementation. In response to Peter Weinberger's question regarding the present users of the database, John Banghart stated that the Security Tool vendors use this information. There are a lot of values to enable reference to common known vulnerabilities in their reports. Many companies, including US CERT, are using this database as a baseline to understanding their systems. Matt Thomlinson stated that Microsoft works differently – after they get the numbers, they assign them themselves because they want to research what was known and unknown. Microsoft conducts the research before sending it to MITRE.

Presently, NVD/NCP has published over 48,000 vulnerabilities; and adding approximately 16 each day. Patching is still an issue and has not been solved. As they evaluate the proposal from China, many people are nervous. NIST had taken time to review the 7/8-page proposal thoroughly. The primary concern is that the vulnerability database is English centric (it is US funded and based in the US), and CVE is not open or well defined. Also, insufficient ID's are available per year, and currently, it is 9,999. John Banghart presented a possible structure that would need an international governance body to propose naming authorities and repositories.

In conclusion, John Banghart stressed the importance of this window of opportunity whereby if it is done properly, we could improve Global Internet Security. It would set a precedent and create structure for expansion into new information domains and information sharing. Standards can help with the understanding of vulnerabilities. We all will benefit, but we will need to take action and a coalition of ability is necessary.

NSTIC Update

Jeremy Grant, Senior Executive Advisor, NIST

Jeremy Grant talked about NSTIC's focus on governance, whereby FICAM is only one element of NSTIC. NSTIC will provide stronger technology for ID management. NSTIC released a NOI in summer, and with the extended closing date they received 57 responses. They are slowly building the initial team. In term of budget for NSTIC, presently there was no clear defined funding. The team has started planning on initiation by leveraging existing groups, start up pilot programs, and when funding is finalized they will be able to process approval for pilot programs. The team has been spending time with other agencies and working with them to develop pilots. Most pilots would not be focused on the Government but more on industry. Jeremy Grant believes that NSTIC cannot be a government-run entity and it needs the private sector to lead the process. A steering group needs to be formulated for this role.

A white paper is in the works with possible release around Thanksgiving. The White Paper would address the initial groups, structure, and balance of groups. The decision is whether to compile a new group and not adhere with any existing groups or FACA. They had researched setting up a grant so as to work separately. There will be a short-term contract with transition to non-government. It will be private sector led with about 8 stakeholders with a set of credentials, rules, and roles. The NSTIC Team will guide and steer the group without imposing any standards. In term of initiation and structure, it is modeled after the successful organization of smart grid. It includes plenary and counsel and 22 stakeholder working groups. The real power lies in the plenary to ensure development in an orderly manner. There will be one vote for every organization. The identified stakeholders are participants of the working groups. The groups are to focus on the four guiding principles[3]. This will include setting up a dot com or dot org and not a dot gov. Almost thirty pages of requirements and bylaws had been drafted. Dan Chenok suggested that NSTIC should have a 3-page summary for initial discussion, and to present the 30-page for deeper involvement. The NOI was established to gain a rapport of support. The finished document will be submitted to inter-agency review.

The Board agreed to continue to be actively involved with NSTIC and would like to invite Jeremy Grant to the next meeting for updates on implementation and funding.

Board discussion

Dan Chenok reported to the Board that the letter requesting the Under Secretary of Commerce for Standards and Technology to review a paper presented by Dr. Fred Schneider[4] was approved and submitted. He explained to Board members that the letter needed first to be reviewed and cleared by NIST legal counsel. There were a couple of changes to June meeting minutes. Dan Chenok, Chair, motioned to approve minutes, Matt Thomlinson seconded the motion.

[3] National Strategy for Trusted Identities in Cyberspace
www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

[4] http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/Nov2011-letter-to-PGallagher.pdf

The Board discussed dates for upcoming meetings in 2012. The dates agreed by the Board for meetings in 2012 are:

February 1 through 3
May 30, May 31, and June 1
October 3 through 5

The following is the Board discussion on presentations from Day 1 and Day 2, and potential agenda items for next meeting:

- FISMA, SP 800-53 Privacy, the Board would like to invite Ron Ross to return for an update on the final appendix on privacy.
- Discussion with Ari Schwartz – It would be beneficial to follow-up on the Akaka privacy Bill, former Senator Evan Bayh, and/or DOC Chief of Staff, Bruce Andrews.
- The discussion with Howard Schmidt: SEC is a model for the government to have an impact without a set of requirements. Dan Chenok suggested to follow-up with Howard Schmidt or Ari Schwartz on engaging Cam Kerry for the next meeting.
- Future of Cyberdefense, Tony Sager: Brian Gouker will look into inviting a speaker from NSA for a discussion on policy and operations for cyber sharing.
- Cyber Awareness Month, Bill Newhouse: There is insufficient involvement from private sector to help NICE to breakout from the traditional communication model. While NICE has good materials and activities, it is not able to communicate the message more widely to reach the larger audience. Matt Thomlinson to draft letter/email to Pat Gallagher, NIST Director, for Board's review on Friday.
- FCC and Technology, Robert Naylor: The Board is interested in having a discussion on DHS Red Team the process rules of engagement, how to the team is being used, and success metric. If DHS and NSA were willing to discuss the subject, we could put together panel that include Robert Naylor. Would this have to be a closed session? Depends on what the Board would like to hear from them.
- NVD, John Banghart: There were a lot of activities. It is unclear about the process or how is it useful for government to hold on to the database. Opening the database and allowing others to access it will enable others to contribute to it. There is no disadvantage for allowing other countries to build/add to the database.
- NSTIC, Jeremy Grant – to maintain the engagement

Suggested Topics for the next meeting:

- DHS cyber strategy update
- A panel discussion on NCIC
- Kevin Fu suggested organizing a panel discussion relating to medical devices, standards and guidance.
- From discussion with Jeremy Grant, to include discussion on Derived Credentials – possible speaker: Bill MacGregor, NIST.
- Data protection directive, data storage, data sovereignty, supply chain
- Management and Software assurance – possibly invite common criteria people
- Invite Steven VanRoekel

Peter Weinberger commented that there have been many activities and good intention on cyber security but with little outcome. People are seriously concerned and want to see effective actions from the government.

The meeting recessed at 4:30 P.M., Thursday October 27, 2011.

Friday, October 28, 2011

The meeting resumed at 8:02 A.M. There was no public participation.

Panel Discussion on prospects for content of cyber legislation

Adam Golodner, Director, Global Security & Technology Policy, Cisco Systems, Inc.
Jim Kohlenberger, Director, JK Strategies
Greg Nojeim, Senior Counsel and Director of CDT's Project on Freedom, Security and Technology

Dan Chenok stated that the Board had a number of congressional panels but thought it would be advantageous to hear from experts. Jim Kohlenberger stated three questions; what should be in legislation, what shouldn't be in legislation and what they expect to be resolved in legislation.

Adam Golodner said that everything is quite global. He has spent the last three weeks in Malaysia, India, and China. Every country is struggling with many of the same issues. They have not found that place of equilibrium among nations to create the global norms that we are looking for. The problem from a technical perspective is everything included in the internet is under tension. Any attempt to do things differently around the world could tear things apart. The business model is based on international standards and on world trade regulations. The domestic standards, particularly supply chain, should not discriminate against certain countries. The concept of having robust industries within countries is desirable. Putting more money into research and development will increase indigenous innovation. The answer is to find a better way for information sharing, which the House is focusing on. For global law enforcement, the focus should be on physical cyber control, and highly sensitive areas.

Jim Kohlenberger said that cyber security is a key enabler. There are several things that are difficult for the Hill to implement – 1) speed of change, 2) interdependencies, and 3) complexities. The third piece is the international global nature of the issue. It is very difficult to come up with US centric solutions.

There are five key challenges, for example:

- Difference in regulatory philosophies.
- Difference between committees of jurisdiction.
- Difference between operator and appropriator
- Difference between military hawks and deficit hawks
- Difference between chambers

There are also five things Congress could do; 1) lock up the bad guys; 2) tough new criminal codes; 3) increase resources; 4) innovate and boost ability to come up with great new systems; and 5) education – we need every cyber security geek. The cyber security bill needs to focus on cyber security workforce, and education awareness is the hardest thing. It is important to ensure privacy and civil liberties. They are also focusing on improving information sharing and FISMA changes.

The things that congress should not do:

1) Use the acquisition process in a way to slow down the ability to bring latest technologies into the government. This would increase the cost of IT for the government.
2) Breadth of critical infrastructure (HSPD 7)
3) Legislate specific security measure
4) Design supply chain method - Whatever we do, international agencies are going to do 10X more.
5) Lastly, there should be a 'no kill switch'. The key is we need to be patching in this area.

Greg Nojeim began with a question, "What should be the role of government in securing private networks?" The President made a pledge and the Congress needs to bring it to fruition. The concern is if an information sharing machine is created, it would be too robust. They would like to see in cyber security is information sharing but within bounds. We could assign DHS as an information sharing hub and regulated it. The White House proposal was too broad and not close to incremental approach to be helpful. The focus should be on information sharing as a lot of other issues are complicated and sharing information could be the solution.

The Center for Democracy & Technology (CDT) has a new proposal[5]. The other part of the government's role in secure private networks is the kill-switch proposal[6]. He also touched on the Lieberman-Collins bill. The law should make provision for private sector to share information and at the same time, to protect the companies. While the President has the power to enforce a cyber security emergency, if the government takes control of the internet, the information would be brought over the Critical Infrastructure system which is a huge risk of unintended consequences. This could discourage fast action because of the information. Greg Nojeim believes there will be a Senate bill that will incorporate pieces from the House and Senate. A mechanism needs to be developed and an extension of legislation to provide clarity and safeguard the network security. There is a narrow window for the Senate to move anything, but if the Senate moves forward, the House will follow.

FedRAMP Update (Presentation provided)

Dave McClure, Associate Administrator, Citizen Services and Innovative Technologies, US GSA

Dave McClure stated that the issue with FedRAMP is trust – lack of agreement and sharing of information. FedRAMP should be based upon the foundation of FISMA. After agencies figure out the baseline controls for each individual environment, they subject each vendor through many similar processes. It is necessary to put into place a trusted environment by leveraging the baseline, consistency, and sharing information. He has been working on FedRAMP for almost two years. FedRAMP was supposed to be launched last fall but the team received many comments that required the team to step back and resolve the comments. The FedRAMP Service Scope has a good solid baseline of controls and agencies are not required to adopt them. The government would save millions if agencies would adopt them.

---

[5] www.cdt.org/blogs/joshua-gruenspecht/white-house-cybersecurity-proposal-pt-i-emergency-powers-regulation-call-sw

[6] Cybersecurity legislative proposal www.whitehouse.gov/blog/2011/05/12/administration-unveils-its-cybersecurity-legislative-proposal

FedRAMP is not being required of agencies. Firstly, it is being tested so as to ensure it runs efficiently and well, and subsequently, it may become mandatory. The set of controls were vetted last year. When an agency is doing its own assessments with its own staff, the agency is expected to meet the same criteria. The assessor accreditation is a huge difference for FedRAMP which includes cloud assessment and certification. In order to bring some consistency to the assessment process, it may be necessary to turn to a private accreditation board. Presently, NIST and GSA are evaluating criteria to form the private board. Lisa Carnahan, NIST and Gordon Gillerman, NIST, have helped to set the process. They are in the process of creating a joint authorization board for the assessment and authorization. They will review the work and the testing. DOD, DHS, and GSA will be part of the joint board.

The other big change is continuous monitoring. They have been working for over the past nine months to set up fifteen monitoring controls. Dave McClure addressed three cloud barriers: FedRAMP is a program that is comprised of several pieces including a light weight PMO and Joint Authorization Board (JAB). The JAB is a prerequisite to getting things through the FedRAMP. A memo is presently under review by OMB to be released soon to the public. Ed Roback, voiced his concerns on getting things through on a deadline. Furthermore, he questioned if there will be a fee for the accreditation. Dave McClure confirmed that initially there will be no fee but that may change when it moves to the private sector. He mentioned that a certain amount of classification in C&A documents, which is a big debate since there is a lot of sensitive material.

Federal identity management and authentication are important part of cloud computing. Cloud computing was previously considered to be locationless. FedRAMP deals with data location, both legal and contractual which needs to consider laws and treaties. They expect this process to become more transparent as they would like to make incidents public knowledge. The Board will continue to follow up closely on this topic.

Board discussion

Based on discussion and notes taken yesterday, Dan Chenok circulated a draft letter on NICE. The Board discussed various points for inclusion in the letter: 1) not narrowly focused on cyber security awareness month; 2) the importance of reaching small business; 3) address cyber security awareness month in relation to NICE; 4) it should be a letter and not an email; and 5) the letter should be addressed to Dr. Gallagher with a copy to DHS, Howard Schmidt, the Secretary of Department of Commerce, and DNI. Dan Chenok proposed a motion to draft the letter, Greg Garcia seconded the motion, and all were in favor.

Phyllis Schneck raised the topic of cyber criminals and what should be done. It was noted that a number of bills, but how can we positively influence legislation to get good work done. It is unlikely for the Board to define a game plan before February meeting. It was agreed to form a task group to work on the plan. Joe Guirreri, Matt Thomlinson and Phyllis Schneck agreed to be part of the task group.

Tasks and Suggested topics for February Meeting:

- A panel from Hill staffers to have a dialogue / discussion (suggested panelists include Tommy Ross, Denise Zheng, Matt Grotti, Peter King, Bruce Brody)

- Dstribute FedRAMP memo to the Board

- On reviewing Matt Scholl's presentation on NIST Update, the Board would like to have a presentation on CSD future research programs

- Panel on FedRAMP

- Panel for DHS/Private Sector / IC on data feedback to the network – coordinate panel with Phyllis Schneck

The meeting adjourned at 11:35 A.M., Friday, October 28, 2011.

Annex A

LAST	FIRST	AFFILIATION	ROLE
Bales	Carol A	OMB	Presenter
Banghart	John	NIST	Presenter
Camm	Larry	Schweitzer Engineering Labs	Visitor
Clay Jones	Alicia	BAH	Visitor
Cuff	Elizabeth	SRA International	Visitor
Curran	John	Telecom Reports	Press/Visitor
Cutshall	Charles R	DHS	Visitor
Engleman	Eric	Bloomberg News	Press
Golodner	Adam	CISCO	Presenter
Grant	Jeremy	NIST	Presenter
Hernandez	Jessica	Treasury Cybersecurity	Visitor
Kerben	Jason	DOS	Visitor
Kohlenberger	Jim	JK Strategies	Presenter
Lightman	Suzanne	NIST	Visitor
McClure	Dave	GSA	Presenter
McGann	Chuck	US Postal Service	Visitor
McNulty	Lynn	McNulty & Associates	Visitor
Miller	Jason	Federal News Radio	Media/Press
Navy	Robert	NSS - Cyber Directorate	Visitor
Naylor	Robert	FCC	Presenter
Newhouse	Bill	NIST	Presenter
Nojeim	Greg	CDT	Presenter
Ressmiller	Scott	PWL	Visitor
Ross	Ron	NIST	Presenter
Sager	Tony	NSA	Presenter
Schlosser	Lisa A	OMB	Presenter
Schmidt	Howard	WH	Presenter
Scholl	Matt	NIST	Presenter
Shaddox	Roanne	FDIC	Presenter