INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

Summary of Meeting

February 1, 2, and 3, 2012

Residence Inn Washington, DC/Vermont Avenue, 1199 Vermont Avenue NW, Washington, DC, 20005-3519

	Present:	
	Board Members	Non-Board Members
Wednesday, February 1, 2012 8:40 A.M. – 5:20 P.M. Thursday, February 2, 2012 8:40 A.M. – 4:30 P.M. Friday, February 3, 2012 8:30 A.M. – 1:00 P.M.	Dan Chenok (Chair) Kevin Fu Greg Garcia Brian Gouker Joe Guirreri Toby Levin Ed Roback Phyllis Schneck Gale Stone Peter Weinberger Matthew Thomlinson (participated via telephone)	Donna Dodson Charles Romine Matthew Scholl (DFO) Annie Sokol (DFO) Megan St. Clair (Recorder) See Annex A for record of presenters and visitors

Wednesday February 1, 2012

The meeting was called to order at 8:40 A.M. The Board members provided updates of their recent activities. Annie Sokol, Designated Federal Officer, informed the board that ISPAB Charter is in the final stage of renewal approval at US Department of Commerce. In addition, the letter[1] re. cybersecurity awareness, which was approved by the Board at last October meeting, was presently being reviewed by NIST Legal (Post Meeting Note: the letter was released and uploaded soon after the February meeting.)

Donna Dodson, Chief, Computer Security Division, NIST, stated that the next ISPAB meeting will be held on the NIST Gaithersburg campus. At this meeting she would like to do expanded presentations of work at NIST so as to get feedback on some key areas from the Board and suggestions on where NIST should be involved and developing.

[1] http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/letter_feb2012_future-cybersecurity-awareness-months.pdf

Panel Discussion: Economic Incentives for Medical Device Cybersecurity[2]

Kevin Fu, Associate Professor, Computer Science, UMass Amherst (moderator)
Brian Fitzgerald, Deputy Director, Division of Electrical and Software Engineering, FDA CDRH OSEL
Louis Jacques, Director, Coverage and Analysis Group, Centers for Medicare and Medicaid Services
James Keller, Vice President, Health Technology Evaluation and Safety, ECRI Institute
George Mills, Director, Department of Engineering, The Joint Commission (participated via telephone)
Lt. Col. Erich P. Murrell, Medical Devices, Office of the Air Force Surgeon General

Brian Fitzgerald discussed medical devices, their risks, and most importantly, whether medical devices work, and if new technology achieves the clinical role as well as old technology. The risks appear at a system level. In order to address more strategic planning he will need to incorporate more promotional activities to doctors and hospitals. His presentation also discussed Electronic Information Exchange within large hospitals to small practices.

Kevin Fu mentioned to the panel that the Board had previous discussions on Health Care IT. The newer technology is not addressing more clinical goals. The question is to find the clinical evidence that the outcomes of patient health improve due to better technology.

George Mills of The Joint Commission explained that they survey hospital devices in a 3 year cycle, but in the standards of their survey there is nothing that specifically deals with technology. He provided details of the survey conducted. The hospitals manage all of the patient information electronically, which is instrumental in saving lives.

Lt. Col. Erich Murrell stated that vendors generally believe that DoD and military organizations such as the Air Force are the only ones requiring security and privacy for medical devices, while the country as a whole is lacking in this area. He would like to work with DoD to provide guidance that the vendors will accept. The biggest challenge is trying to get vendors to build appropriate security to the network when the devices are delivered so that no time is needed to do catch up. He would prefer that the vendors start working on the protocol before the devices are sent to FDA for approval.

While there are regulations in place to protect the safety and effectiveness of medical devices, it seems only the larger hospitals and not small practices are in compliance. There is no known baseline in term of market correction for hacked medical devices. There is no regulation for design defect that results in safety violation, and no process for tracking and recording of devices malfunctioning. There are millions of adverse events, but only a handful are willing to report them. This is partly due to fact that the incidents do not really hurt anyone.

Many medical practitioners know the issues and are able to identify occurrence of breaches. Since the economic incentive comes from the customers, it is necessary to have a collaborative plan to put together general rules or guidelines. Lt. Col. Murrell responded about the lack of education and communication to inform people of the importance of maintaining security for medical devices. On the other hand, the vendors must assume certain responsibility in maintaining security for the devices.

[2] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_med_dev_nist-eco-med-dev-sec-2012l.pdf

Board members suggested the following approaches that can be done:

- Practical baselines for each device, such as requirement to set up a password before first use, and to initiate patches against known threats, which is not a system issue but a per device issue. It is such best practices that can help to secure medical devices.
- What should be the definition of the minimum requirement? What are the measurements?
- Inclusion of certification
- Incorporate education of medical devices security and safety with annual cyber awareness month

The Chair invited Kevin Stine of NIST to share on his work on Health IT. He stated that NIST is working on the broad part of outreach, but as a manager of the Outreach Group, his team is working on Health IT outreach, and he further expanded on the HIPAA Security Rule tool kit, which started out to be a simple application. This application could be tweaked to apply to many medical centers, including hospitals and smaller offices. This could be a topic that the Board to consider for another meeting. Kevin Stine informed the Board that NIST is preparing some publications relating to HIPAA Security Rule for release in a few months.

NIST Updates (Presentation available)[3]

Donna Dodson, Division Chief, Computer Security Division (CSD), NIST

Donna Dodson updated the Board on recent Draft Special Publications and that many are related to security automation work and continuous monitoring. In addition, CSD will soon be releasing the annual report[4] and is close to finishing FIPS 201-2 Personal Identity Verification (PIV). She discussed some important previous and upcoming events including some very important outreach activities including the Secure Hash Algorithm (SHA) Competition.

Donna Dodson discussed the recent reorganization in the Computer Security Division and the search for a group manager. The division is extremely busy with lots of activities concentrating on mobility, cloud computing, identity management such as NSTIC and continuing work relating to FISMA. The division continues to maintain dialogue with senate and working on a green and white paper on Botnets. Dr. Pat Gallagher, Director of NIST, will be speaking at RSA conference at the end of February.

On the administrative side, Donna Dodson is still leading two divisions[5]. Ari Schwartz is detailed to the Secretary of Commerce. Adam Sedgewick from the Hill has joined NIST.

NIST was allocated a budget of $10 million for establishing the National Cybersecurity Center of Excellence[6]. The Center will be funded annually and it is not for R&D. The vision of the Center is to

[3] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_nist_updates.pdf
[4] http://csrc.nist.gov/publications/nistir/ir7816/nistir_7816.pdf
[5] Post meeting note – Donna Dodson is no longer leading two groups but is now the Acting Deputy Director, Cyber Security Center of Excellence as well as the Chief, Computer Security Division, NIST

help community to recognize and use security programs, for people to take advantage of developed technologies instead of inventing new ones, and for using the guidelines and measurements that NIST has developed. NIST wants to optimize this partnership with the State of Maryland and to work closely with the industry and private sector. The goal is to have the center operational within the next five months. Donna Dodson proceeded to discuss the structure of and staffing for the Center, and the benefits of having people from industry and academia, vendors, and research scientists detailed to NIST to help work on the Center. This is a very important and interesting topic, and the Board is to provide input at the next meeting in June and to receive an update from NIST on its development in October meeting.

ACTION: Board to provide input on strategic on cyber security – highlight on considerations, things to be done, and national challenges at the ISPAB meeting in June 2012.

ACTION: NIST to provide updates on the Cyber Security of Center of Excellence in October 2012.

Cloud- Data Location, Data Storage and Data Sovereignty

Earl Crane, Director for Federal Cybersecurity, National Security Staff, The White House
Alma Cole, Custom & Border Protection, US Department of Homeland Security
Kevin Jackson, General Manager, Cloud Services, NJVC, LLC (Presentation available) [7]

Kevin Jackson began his presentation and stated that the value of cloud computing is scalability, the infrastructure is time trusted, and we should continue to leverage technologies to deliver information. It is possible to shut down an IT infrastructure and render it useless. We should address security and manage the risks for cloud computing. While there is a lot of value in cloud computing, not everything can be "cloudable". Included in his presentation are the following discussion topics, but particularly there is a chart provided by IBM that stated that cloud computing is ideal for 'loosely coupled' applications such as business intelligence, data archiving and social media:

- Information Assurance Risk Factors by Domain and Bandwidth vs. Trust
- Browser-based application
- Ubiquitous data access
- Global compatibility
- Reduced capital requirements
- Frictionless environment (Viral applications)
- International market place of ideas

When Kevin Jackson raised the example of scientific collaboration, e.g. NASA and Japan NII, he stressed the importance of not creating rules and policies that would prevent collaboration. It should be the government's intention to have international connection and accessibility. Many countries like Korea are acquiring data centers globally as cloud starts at multiple locations. If the needed consensus is taking too long, it could impact interoperability and portability. He further illustrated market collaboration and formation such as EuroCloud. There are also other challenges such as legal Issues, interoperability, portability, and increased in "Digital Divide". The one thing

[6] http://www.nist.gov/itl/csd/nccoe-022112.cfm
[7] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_cloud_jackson_k.pdf

that Kevin Jackson considered the Board should do is to provide more visibility and information on FedRAMP.

Alma Cole talked about the big difference in transport and housing data. Where data will be stored is always an issue because of concern for privacy. We could outsource data storage but should not outsource management of data. FedRAMP emphasizes a number of controls, which include avoiding storing sensitive data in the cloud. There are always risks but there are a few good practices – authenticate users, monitor who and how data is accessed, monitor the storage log, SLAs, and controls to lock down the systems.

Earl Crane agreed that data locality is critical but there is the issue of governance. There are so many different answers on sovereignty when considering governance of locality. Therefore, the approach of visibility - knowing what happens to your data, and what and who is sharing data, systems, etc. While FedRAMP addresses many of these challenges, there is work needed to improve program managers and decision makers. This concept of visibility is now exists in large enterprise IT management, which subsequently leads to continuous monitoring, which may take some years to gather sufficient information.

We need to establish the right level of information for continuous monitoring in the cloud environment. Security Content Automation Protocol (SCAP, NIST) is one way to monitor the information coming back to us. We still need to rely on our experience to know what to look for. Cloud computing is in automated IT environment, it is important to leverage automation to enable government. But we need to be actively involved in governance as laws and policies are set. Earl Crane and Alma Cole requested the Board to address the issue of continuous monitoring in the cloud environment.

Security in the next generation mobility

Lily Chen, Mathematician, NIST (Presentation available) [8]
Murugiah Souppaya, Computer Scientist, NIST
Tom Karygiannis, Computer Scientist, NIST
Andrew Regenscheid, Computer Scientist, NIST (Presentation available) [9]

Matt Scholl introduced the panelists and their works. Murugiah Souppaya talked about the two issues that they are focusing on for this year's project plan, cloud and mobility. NIST SP 800-124[10], Guidelines on Cell Phone and PDA Security provides the guidelines for mobile devices was published early 2012. Murugiah Souppaya is working on a early draft of "Guidelines for Managing and Securing Mobile Devices in the Enterprise." This is a recommendation for agencies to set up a general policy for mobile device. He would appreciate comments from the Board.

Andy Regenshied's presentation, "Roots of Trust in Mobile Devices," is to explain Roots of Trust in relation to hardware and software components that need not only be secured by design and not just roots of trust but trusted roots of trust. The presentation also described the release of NIST SP 800-

[8] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_mobility_lchen.pdf
[9] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_mobility-roots-of-trust_regenscheid.pdf
[10] http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

147[11], Basic Input/Output System (BIOS) Protection Guidelines (April 2011), and SP 800-155[12], Draft BIOS Integrity Measurement Guidelines (December 2011). The information is being applied to not only to PCs, but also to mobile devices.

Tom Karygiannis is working with DARPA and using smart phones in a tactical environment such as the military. The work includes the use of encrypted file system especially the potential of losing the phone while in the field, and downloading safe Apps to a mobile device. On the subjects of Privacy and Linkability - For government databases, we typically think we can protect one's privacy by simply not disclosing the contents of a particular field in a database (name, ssn, dob, for example). As the amount of data available about individuals increases (social media, free web-services), the opportunity to determine one's identity by combining different sources of data makes it much more difficult to protect PII. As we focus on protecting data collected by government agencies and improving technical controls, at the same time the amount of information available in private databases is increasing dramatically. This makes it possible to more easily link information to an individual and overall more difficult to maintain privacy.

Lily Chen is working on mobility protection, and her work impacts both users and interaction with international users. There are three specific aspects of mobility protection:

- Communication Protection
- Mobility Information protection
- (Focus on) Mobility Service Protection

Dr. Chen also discussed the switch from wifi to 4G, which has been highlighted in the IEEE 802-21 document. She stated that even non-cellular service providers can use this information and they have received many contributions from Europe and Korea. One of the biggest challenges is when employees bring their own personal devices to work (BYOD), and it would interesting to set up pilot to explore how end users will actually use them. There are many situations, such as telework, emergencies, and weather conditions, when people are only interested in getting the work done and security become their secondary concerns.

Derived Credentials, FICAM, PIV and more

Hildegard Ferraiolo, Computer Scientist, NIST (Presentation available) [13]
Catherine Tilton, Vice President, Standards & Emerging Tech, DAON (Presentation available) [14]
Elaine Newton, Computer Scientist, NIST (Presentation available) [15]
Tim Polk, Cryptographic Technology Group Manager, NIST

Elaine Newton stated that SP 800-63-Rev.1[16], Electronic Authentication Guideline, was finally published in December 2011. The list of authors from NIST includes Donna Dodson, William Burr, Ray Perlner, W. Tim Polk, and Elaine Newton. It is consistent with the original document. The

[11] http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf
[12] http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-155
[13] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_der_cred_ferraiolo_h_fips_201-2.pdf
[14] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_der_cred_daon_tilton_c.pdf
[15] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb1_nist-800-63-1_overview_enewton.pdf
[16] http://csrc.nist.gov/publications/nistpubs/800-63-1/sp-800-63-1.pdf

document covers topics such as identity proofing, token and credential management, and it basically lays out a framework for implementing electronic authentication. A presentation of the authentication model, players, and overview of different levels of authentication was provided. Tim Polk added that the document is harder for government than for private sector to use. This revision added two new factors - Authentication Technologies and Derived Credentials.

Hildegard Ferraiolo talked about NIST FIPS 201 and the introduction of derived credential. Homeland Security Presidential Directive (HSPD-12)[17]: Policy for a Common Identification Standard for Federal Employees and Contractors sets the goals for FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors. In adopting a smart card based solution for FIPS 201-1, security is an important consideration. There are different levels of security. When Draft FIPS 201-2 was released for comments in late spring 2011, many comments were submitted. After resolving comments, NIST will be preparing to release a revised draft in 2012. The standard strategy goal is a PIV card to comply with HSPD-12 and OMB-11-11[18] guidance, while supplying the same credentials to mobile devices. One approach is an enhanced PIV card linked to your device, and if it will be able to read the PIV card within a close proximity. Another approach is derived credential, whereby a PIV Card authorizes a mobile device manager (MDM) to create derived credential, and in this way the card and the device do not have to be in close proximity to each other. Hildegard Ferraiolo further illustrated the pros and cons of derived credentials. The NIST team is still reviewing 1200+ comments. FIPS 201-2 needs to be finalized and released ahead of any other relating publications and revisions.

Catherine Tilton presented Use Case of Derived Credentials based on SP 800-63-1. In presenting examples of a few high-level possible use cases, she also discussed the challenges of identity management as well as three areas that need to be balanced: Security, Compliance Management and Business Enablement. She foresaw a huge increase in digital interaction in the future of identity and digital interaction, and there is a need for trusted identities.

The meeting recessed at 5:21 P.M., Wednesday, February 1, 2012.

[17] http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#1
[18] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011m11-11.pdf

Thursday, February 2, 2012

The meeting resumed at 8:30 A.M., and the Board reviewed the discussions and presentations from February 1, 2012. The Board agreed that data sovereignty is a huge issue and would like to organize a panel consisting of representatives from DOJ, GSA, and a cloud provider to discuss Cloud and Data Sovereignty. The Board also interested in the following topics for the next meeting: mobility and mobile device, and telework. They also appreciated the good work on derived credentials and would be glad to hear more on this topic.

DHS Updates

Bruce McConnell, US Department of Homeland Security (DHS)
Davis Hake, Cyber Security Strategist from Homeland Security, DHS

Mr. Bruce McConnell introduced Davis Hake, Cyber Security Strategist. He briefed the Board on the following topics:

- Comprehensive National Cybersecurity Initiative[19] #5 and National Cybersecurity
- Communications Integration Center (NCCIC) and cyber evaluation tools
- Legislation - Information Sharing and Critical Infrastructure, law enforcement on cyber crimes, variety of statues, information sharing clarifying legal requirements close to real time responses
- Einstein 3 – rich partnership with DoD and NSA
- Cyber Security Incident Plan – mandatory incident reporting and establish a baseline of security
- Health IT, medical device and incident reporting – medical industry is still not ready to handle
- Data breach and intrusion- there are different information requirements
- Continuous monitoring – listening as opposed to simply being alert
- Standards – there are plenty of technical controls but it is best to consider risks and risk control
- Financial sector – increase security measures but should remain flexible
- Raising Awareness on cybersecurity – how to communicate to key level people

Dan Chenok, Board Chair, inquired about cloud security and different international laws relating to cloud. Bruce McConnell responded that they are in the really early stages of discussion on the government perspective.

Progress for Modernizing Federal Desktop Platforms

Matt Coose, National Cyber Security Division (NCSD), DHS
Matt Scholl, Deputy Chief, Computer Security, NIST

DFO did extend an invitation to OMB to join in this discussion, but no one was available. Matt Coose discussed CERT, FISMA, and working with agencies and the executive branch in identifying threats, capabilities and the effectiveness on mitigating threats. Peter Weinberger and Matt Thomlinson (on the phone) expanded on the discussion on FISMA, patches, and addressed the issue of

[19] www.whitehouse.gov/sites/default/files/cybersecurity.pdf

vulnerabilities of Windows XP as not being FISMA compliant. Donna Dodson, NIST, stated that it was necessary to work closely with CIOs and CISOs to find appropriate timeline that will coordinate funding so as to schedule reducing the number of vulnerabilities. To understand the technical side of implementation, applications need to be rewritten to be FISMA compliant, but the cost will be substantial. Peter Weinberger maintained that the government needed to adopt an aggressive approach to get off Window XP as part of cybersecurity priority. It is necessary to build a business case to demonstrate to the CIOs and CISOs of the risks. Matt Coose agreed that CIOs' and CISOs' should decide on how they would like to handle the risks with their applications. USG agencies are balancing funding and priorities for migration, and investment in new technologies.

The move of Window XP will require enormous testing to be conducted. As this is necessitate leadership from the top, Dan Chenok, Chair, suggested that Matt Thomlinson and Peter Weinberger draft some basic discussion points that the board could use to present issues to Howard Schmidt.

Kick Starting NCCIC Information Sharing: Progress Report and Recommendations from the National Cybersecurity and Communications Integration Center.

Greg Garcia, ISPAB Board Member (Moderator)

Scott Algeier, Executive Director of the CISE Division of Computer and Network Systems (CNS), National Science Foundation (NSF)

Patrick Beggs, Director of Operations at National Cybersecurity and Communications Integration Center (NCCIC), DHS

Denise Anderson, Vice President FS-ISAC, Government and Cross-Sector Programs Financial Services Information Sharing and Analysis Center FS-ISAC (Presentation provided) [20]

Scott Algeier, Executive Director of the IT-ISAC and President and CEO, Conrad, Inc.

Greg Garcia provided the background, historical information on, and challenges faced by National Cybersecurity Communications Integration Center (NCCIC). Patrick Beggs described the set up and layout of the operation and a 'Virtual Tour' of the facility, which was finalized in October 2009. There are 24 personnel, and all are US CERT. Integrated Access and Control System (ISAAC)[21] is in the main NCCIC group. There are representatives from major agencies on detail to this group. They are working on bringing people from private companies. While they presently have yet to establish an international presence, they have just begun working with Canada.

Scott Algeier talked about Information Technology – Information Sharing and Analysis Center (IT-ISAC)[22]. It had the same general mission as Financial Service – Information Sharing and Analysis Center (FSISAC)[23]. There are different ISACs with different responsibilities, and there are multi-sector ISACs. IT-ISAC was the first sector to sign an agreement to be on the floor.

When an attack is detected, the information is shared with members. Many people are requesting to have security clearances but it is better to declassify information . There is a lot of information

[20] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb2_ispa-nccic-information-sharing_danderson.pdf
[21] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_fema_dmarts.pdf
[22] https://www.it-isac.org/
[23] http://www.fsisac.com/

from each portal, but it is necessary to have a non-disclosure agreement to stimulate greater cross sharing. DHS spends huge budget on creating policies and less on operation. Patrick Beggs worked hard to convince DHS attorneys to allow more joint R&D. The vision of a few years ago is finally happening.

The two-tiered model that they have been working on includes a free membership facilitated by the government, in which the member would get basic information from the operation center. There is also a paid membership, in which the member would have exclusive paid membership advantages. Many members are IT companies, but not from large organizations. If members developed products and/or services based on information gathered through this operation, the companies cannot use the name of this operation as endorsement.

Panel Discussion: Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program[24]

Pat Muoio, Chief, National Information Assurance Research Lab, NSA

Keith Marzullo, Director of the CISE Division of Computer and Network Systems (CNS), NSF (Presentation provided) [25]

Chris Greer, Associate Director, Program Implementation, ITL, NIST

Bill Newhouse, Cybersecurity Advisor, NIST (Presentation provided) [26]

Bill Newhouse talked about the purpose and scope of the Federal Networking and Information Technology Research and Development (NITRD) Program, as well as the NITRD structure for US Federal Cybersecurity R&D coordination. It is about trustworthiness and reaching out to get ideas from major vendors and suppliers. The R&D Coordination happens through Research Themes: Tailored Trustworthy spaces, Moving Target, Designed-in Security, Annually re-examine themes, and Cyber Economic Incentives. Bill Newhouse's presentation provided examples for each theme, some potential research topics for the Science of Security, support for national priorities, transition to practice, and finally drivers for next-generation solutions. These themes are considered as opportunities and necessary to be inclusive and complete to capture areas of concerns.

Keith Marzullo explained Secure and Trustworthy Cyberspace (SaTC) as a cross-directorate program to address cybersecurity from one or more of the following three perspectives:

- Trustworthy Computing Systems
- Social, Behavioral and Economics
- Transition to Practice

He followed up with program scope and research principles, and added that NIST is working on the scientific part together with production of special publications.

[24] http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

[25] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb2_marzullo_nsf-csia-rd-strategic-plan.pdf

[26] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb2_federal-cybersecurity-rd-program_bnewhouse.pdf

Chris Greer explained that work on and relating to cybersecurity are carried out not only by CSD, but also in ITL/NIST, contributing to the measurement science research and tailored trustworthy space. In addition, DHS and DARPA would have an important partnership. Demonstrating concrete results to address problems would be the ultimate goal.

The only thing that Mr. Newhouse would like to see from the board is to pay attention to hearing the echo of the themes. He said that this discussion with the Board helped with connectivity between people. They would appreciate recommendations from the Board on the basic and transition levels, and pointers on privacy.

Panel Presentation: Cyber Ecosystem and Automated Cyber Indicator Sharing

Phyllis Schneck, VP and Chief Technology Officer, Public Sector McAfee, Inc. (Moderator)
Bob Dix, Vice President, Government Affairs & Critical Infrastructure Protection, Juniper Networks
Ron Plesco, CEO, National Cyber Forensics and Training Alliance
Richard Struse, Deputy Director, Software Assurance Program, GCSM, National Cyber Security Division, DHS

This panel discussion was a follow-up to Kim Johnson's presentation on Cyber Ecosystem – *Enabling Distributed Security in Cyberspace – Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*[27] – a presentation at ISPAB, July 2011[28]. Bob Dix had spoken to the Board many years ago and many of issues previously present were still relevant. When he was working in the government FISMA had a lot of influence on his work. Today, it is necessary to focus on the side of economics and less on how technology advances interaction between industry and government.

Richard Struse considered the biggest challenge to be sharing of information. It is important and necessary for government agencies to be able to exchange information. The private sector should do likewise. It is imperative to enable information sharing, and the federal government should eliminate boundaries and allow/encourage people to share information. The panel provided the following observations/recommendations:

- Identify key standards so that the mechanism can be in place for data sharing
- Provide appropriate frameworks
- Identify gaps and deal with them in a holistic way
- Automated sharing indicators that are useful but still violate privacy
- Experts must be willing to share information proactively without being victimized

Panelists cautioned that NCCIC offers a great opportunity for collaboration, but there is the question of who is in charge. The private sector is leading information sharing using people in operational roles. A structure for a marketplace model was described, and the involvement of a trusted third party is needed. The panelists were finding appropriate examples for people to follow, and then they need to figure out how to explain the differences in sharing between people, and sharing between machines. Leadership is needed to identify and map gaps, and to formulate goals that will be fit for use globally.

[27] http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf
[28] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2011-07/ISPAB_Minutes_July2011_Final.pdf

The meeting recessed at 6:00 P.M., Thursday, February 2, 2012.

Friday, February 3, 2012

The meeting resumed at 8:40 A.M.

Board Review

The Chair thanked Toby Levin for providing notes/comments on the meeting minutes. Joe Guirreri proposed a motion to approve the minutes, Peter Weinberger seconded the motion, and the minutes were approved unanimously.

The Board reviewed the discussions/presentations from Thursday, February 2, 2012, the Board raised the following questions/comments:

- Noted the future state of IP architecture as identified gap.
- How to improve human-to-human organization before machine-to-machine?
- What are the barriers on information sharing and does everything have to be channeled through DHS?
- What is the privacy implication on the infrastructure?
- NCCIC – there were a lot of people involved and work put in, but it is unclear where is the information stored
- There seem to be some gaps between the panel discussion on NCCIC and Cyber ecosystem that the Board needs to explore.

These questions prompted the Board to ask Greg Garcia and Phyllis Schneck to organize panel discussions for the next meeting.

The Board discussed on writing a letter of recommendation based on the discussion on US government continuing use of outdated OS. Peter Weinberger agreed to prepare a draft for Board's review and discussion.

Public Participation:

Mr. Bruce Levinson, Senior Vice President, Regulatory Intervention, The Center for Regulatory Effectiveness, wrote to the DFO on January 3, 2012, requesting an opportunity to address the Board at this meeting. A paper, *Federal Cybersecurity Best Practices Study: Information Security Continuous Monitoring* (see Annex B), was attached to his email request. As stated on the Federal Register Notice announcement, Mr. Levinson was given five minutes to present to the Board. He stated that it is important from regulatory environment and economic standpoint to ask about best practices in relation to FedRAMP and continuous monitoring. He would like to know how FedRAMP is being measured. It is important to know the metric at least from the standpoint of cost and regulatory impact. As it is stipulated that SP 800-53 will be imposed on all critical infrastructure apart from government, it is important to ensure the process is transparent, objective, and economical. He would like to know if the security metric for FedRAMP is sufficient and cost effective, and at the same time is also rigorous. He would like the Board to note that different sectors have different standards; therefore, how does the Board envision regulating sectors? The Board thanked Mr. Levinson for his comments.

Legislature Updates:

Tommy Ross, Senior Intelligence and Defense Advisor to Senate Majority Leader Harry Reid

Tommy Ross worked on legislation that covers a wide gamut and with various committees. There are a handful of authorities to the current law. It is not intended to solve every cybersecurity issue but to focus on national security. It is particularly important for the Government to influence the degree of security in critical infrastructure. It is challenging defining terms, and dealing with eighteen different critical infrastructures. There is on-going work through existing frameworks to tailor approaches to each different sector. Among eighteen sectors, there are limited numbers of frameworks in some sectors and none in other sectors. There are some sectors where any threats would not create any deathly impact. Apart from cybersecurity, there are two areas of pressing needs to drive security across government - information sharing and FISMA. The government needs to do a better job in protecting its own systems effectively when stating standards and regulations, and simultaneously, be responsive to private sector. Standards are not meant to be performance measurement or baseline, but as a bar for cost controls and as provision to help companies.

Tommy Ross also noted that cybersecurity is an important area for US government in terms of lateral and bi-lateral diplomacy. There needs to be great emphasis on standards as it is not possible to legislate diplomacy. The government is working with other countries as part of bilateral diplomacy. Recent meetings with the Indian government about cyber security showed that this was a critical issue to work on together.

Tommy Ross mentioned of negotiation of provisions with different committees and preparing legislation. They were seeking feedback from agencies, private sector, and various stakeholders prior to introducing a base bill. It is a difficult task to get agreement from majority of the house on the legislation. Tommy Ross agreed to continue to share the latest drafts of legislation with the Board.

Federal Risk and Authorization Management Program (FedRAMP) Updates

(Presentation provided) [29]

Lisa Carnahan, Computer Scientist, NIST
Matt Goodrich, Federal Cloud Computing Initiative, GSA
Ron Ross, NIST Fellow, NIST
Gordon Gillerman, Director, NIST Standards Services, NIST

Cita Furlani called in to the Board, and the Chair took the opportunity to congratulate her on years of hard work as she began her retirement.

Matt Goodrich began the panel presentation with an explanation of FedRAMP – definition of what it is and what it isn't, and discussion of FedRAMP stakeholders and the interaction between them. A chart displayed the phases of FedRAMP and timeline for these phases. They are developing lessons learned and based on comments they received to perfect the process. The Joint Authorization Board (JAB) establishes security controls baseline with recommendations from technical

[29] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-02/feb3_fedramp_ispab.pdf

representatives, industry, and agencies. They have received over 1000 comments on Security Controls document, and on January 8, 2012, FedRAMP requirements (Security Controls, templates, guidance) were released. Revision 4 will include many more privacy controls and will be released before FedRAMP launches.

FedRAMP is coordinating closely with NIST on Third Party Assessment Organization (3PAO) Accreditation. Gordon Gillerman, NIST, illustrated the existing private sector infrastructure as the foundation, which leans on international standards to define certification program, inspection, and evaluation of programs. The federal programs are using conformity assessment approaches. Gordon Gillerman further explained the 3PAO conformity assessment process, technical requirements, acceptance process, and application process.

Lisa Carnahan, NIST, expanded on these processes. She explained that the Cloud providers would need to pay for this processes, which is in effect a certification and accreditation. They had received an overwhelming number of applications. An agency needs to use an accredited 3PAO in order to be reviewed by the JAB. The 3PAO is not an approval process but basically conducts an audit to make sure the organization has done everything in the assessment process. It would refer to the JAB for approval (recommended authorization). The decision by JAB has to be unanimous. A provisional authorization means that the JAB agrees that this organization has met all of the requirements. Dan Chenok, Chairman, suggested that the term "authorization" might need to be changed for clarity.

They are working with DHS to develop a framework that agencies must follow. Within the next week, they plan to release the FedRAMP Concept of Operations[30], and by the end of April, to release the initial list of 3PAOs.

FedRAMP is something that the board has a lot of interest in and they appreciate the work that has been done.

Board Discussion:

In recognition of Joe Gurreri's years of dedicated service with ISPAB, he was presented with a Certificate of Appreciation from Chuck Romine, Director of the Information Technology Laboratory at NIST. This was his last meeting with the Board and he will be sadly missed.

The Board proposed topics as possible agenda items for the next meeting in May/June 2012:

- Legislative update
- HealthCare Security (Kevin Stine, NIST)
- Mobile Device Usabilty
- SmartGrid and Control Systems (SCADA Update)
- DOJ/GSA Cloud Provider Panel
- Information Sharing Panel- Architecture and organizational
- Privacy Assumptions in the research program (Toby Levin, moderator)
- Telework
- Administration's Privacy Program (possible topic for October meeting)

[30] www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf

- Supply Chain
- Topic on conformance activities
- SEC breach notification (Kevin Fu, moderator)
- SP 800-53 Appendix J – Privacy (Ron Ross, NIST)
- Update on SCAP- Security Automation is a key program at NIST
- Red Team, Blue Team
- OMB Update (Steve VanRoekel)
- NSTIC Update (Jeremy Grant)
- Controlled unclassified on NARA
- DIB Pilot, Joint Cyber Security Panel – (Greg Garcia, moderator)
- Information Sharing panel – (Phyllis Schneck, moderator)
- NIST research projects/topics

Kevin Fu provided a draft letter concerning medical device for review's letter. All agreed it had excellent material. The Board discussed inclusion of home usage, which agency should be the lead, and the addressees for this letter. It was agreed to direct the letter to Director of OMB with cc. to NIST Director and Secretary, HHS. The Chair proposed the motion to approve the letter, Toby Levin seconded the motion, and all were in favor.

Peter Weinberger provided a draft letter re government continued use of outdated OS for review. Matt Thomlinson would like to provide further edits. The Chair proposed that Peter Weinberger to refine the letter based on the comments from the ISPAB members. He proposed a motion to execute the letter. The motion was seconded by Toby Levin, all in favor with one abstention (Ed Roback).

Before the meeting ended, Donna Dodson invited the Board to provide individual thoughts and suggestions re the Center of Excellence.

The next meeting will be May 30, May 31, and June 1, 2012, at NIST, Gaithersburg, Maryland. The meeting adjourned at 1:00 P.M., Friday, February 3, 2012.

Annex A

LAST	FIRST	AFFILIATION	ROLE
Algeier	Scott	IT-ISAC	Presenter
Anderson	Denise	FS-ISAC	Presenter
Beggs	Greg	NCCIC, DHS	Presenter
Camm	Larry	SEL, Inc.	Visitor
Carnahan	Lisa	NIST	Presenter
Chen	Lily	NIST	Presenter
Cole	Alma	DHS	Presenter
Comley	Sarah		Visitor
Coose	Matt	NCSD, DHS	Presenter
Crane	Earl	National Security Staff, The White House	Presenter
Davis	John C	Teknoworks, Inc.	Visitor
Dix	Bob	Juniper Networks	Presenter
Ferraiolo	Hildegard	NIST	Presenter
Fitzgerald	Kevin	FDA CDRH OSEL	Presenter
Gillerman	Gordon	NIST	Presenter
Glazer	Melinda	PKH Enterprises	Visitor
Goodrich	Matt	GSA	Presenter
Greer	Chris	NIST	Presenter
Hake	Davis	DHS	Presenter
Jackson	Kevin	NJVC, LLC	Presenter
Jacques	Louis	Medicare and Medicaid	Presenter
Karygiannis	Tom	NIST	Presenter
Keller	James	ECRI Institute	Presenter
Kerben	Jason	Department of State	Visitor
Kern	Pamela	National Cyber Security, DHS	Visitor
Lee	GayHee	US GAO Healthcare	Visitor
Levinson	Bruce	CRE	Visitor
Marzullo	Keith	NSF	Presenter
McConnell	Bruce	DHS	Presenter
McNulty	Lynn		Visitor
Mills	George	The Joint Commission	Presenter
Moore	Debbie Taylor	Cyber Zephyr	Visitor
Muoio	Pat	NSA	Presenter
Murrell	Erich P	Office of the Air Force Surgeon General	Presenter

LAST	FIRST	AFFILIATION	ROLE
Newhouse	Bill	NIST	Presenter
Newton	Elaine	NIST	Presenter
Plesco	Ron	National Cyber Forensics and Training Alliance	Presenter
Polk	W. Tim	NIST	Presenter
Ross	Tommy	Senate	Presenter
Shenefiel	Chris	CISCO Systems	Visitor
Simmons	Rob	Mitre	Visitor
Souppaya	Murugiah	NIST	Presenter
Stine	Kevin	NIST	Visitor
Struse	Richard	DHS	Presenter
Tilton	Catherine	Daon	Presenter

Annex B

From: Bruce Levinson [mailto:Levinson@mbsdc.com]
Sent: Tuesday, January 03, 2012 3:38 PM
To: Sokol, Annie W.
Subject: CRE ISPAB Presentation

Dear Ms. Sokol:

Thank you very much for your call this afternoon. I would like to speak to the Board for no longer than five minutes on the topic of FISMA and Continuous Monitoring. The focus of the brief would be the attached paper, Federal Cybersecurity Best Practices: Information Security Continuous Monitoring. A link to the paper may be found on our FISMA Focus site here, http://www.thecre.com/fisma/?p=699. Additional information about FISMA Focus, may be found here, http://www.thecre.com/fisma/?page_id=2. I will, of course, be available to answer any questions.

Bruce Levinson
Senior Vice President, Regulatory Intervention
The Center for Regulatory Effectiveness
202/265-2383
www.TheCRE.com/fisma