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

August 4, 5 & 6, 2010

Washington Marriott Hotel
1221 22nd Street NW
Washington, DC 20008

	Present:	Absent:
Wednesday, August 4, 2010 8:45 A.M. – 5:15 P.M. Thursday, August 5, 2010 9:00 A.M. – 4:15 P.M. Friday, August 6, 2010 8:15 A.M. – 10:57 A.M. Meeting was accessible via webcast <http://csrc-nist.granicus.com/ViewPublisher.php?view_id=2	Dan Chenok (Chair) Ari Schwartz Jaren Doherty Brian Gouker Joe Guirreri Alex Popowycz Matthew Thomlinson Peter Weinberger Lynn McNulty (via teleconference for parts of the agenda) Cita M. Furlani Donna Dodson Matthew Scholl Annie Sokol (DFO)	Lisa Schlosser Fred Schneider Gale Stone

Wednesday, August 4, 2010

The chairman of the board called the meeting to order at 8:45 A.M., Wednesday, August 4, 2010.

The board began the discussion with the new e-FACA Webcast and all agreed that it was valuable. The chair, Dan Chenok, reviewed the agenda items with the board. He announced that he has taken a new position with IBM. As board members provided their individual updates, Ari Shwartz announced that he will be starting a new position at NIST and Brian Gouker has a new job position at NSA. It was also confirmed that Lisa Schlosser will no longer be active on the board as she has taken a new position. NIST will work on finding replacements for Ari Schwartz and Lisa Schlosser. The replacement for Howard Schmidt is presently in the process of being vetted and approved.

Cita Furlani, Director, Information Technology Laboratory (ITL), NIST, talked briefly about NIST's reorganization that will take effect on October 1, 2010. Under the reorganization, NIST will realign with six laboratories reporting to three associate directors. ITL is not affected and will remain unchanged.

Donna Dodson, Division Chief, Computer Security Division (CSD), NIST, recognized the dedicated service of Pauline Bowen, as the DFO of ISPAB. Pauline Bowen has retired recently from a long service as federal employee. Annie Sokol was acting as the DFO for this meeting. Donna Dodson described the upcoming events involving CSD – three workshops relating to security issues and e-voting. She next sought suggestions from the board on NIST's R&D opportunities for the next five years including Crypto space, Commercial space and Identity Management. The discussion also covered fundamentals and algorithms for cryptography, key management, development of standards and matrix, identity proofing, and maintaining interoperability with

PIV card. In addition, the board pointed out the necessity for clear leadership with a structure to describe how everything fit together and NIST's role in the international realm.

The Board's draft letter re. National Initiatives for Cybersecurity Education (NICE) – Matt Scholl, NIST, reported that the general counsel at NIST raised some questions after reviewing the letter prepared and approved by the board at the last meeting. The Chair provided a summary of the recommendations in the letter. During the 3-day meeting, the board further reviewed and edited the letter. A motion was proposed to edit letter by Brian Gouker and seconded by Joe Guirreri. The board approved the changes to the letter. Donna Dodson will discuss the letter with the general counsel, and if necessary, NIST will arrange a face-to-face meeting between the Chair and the general counsel.

Usability Research in Support of Cyber Security: A Password Policy Taxonomy

Kevin Killhoury, NIST
(presentation provided)

Mr. Killoury started work at NIST about two months ago. He is a graduate from Carnegie Mellon with a degree in Computer Science/Security. He discussed developing taxonomy, collecting a corpus and analyzing the corpus by reducing policies to an unambiguous language. Mr. Killoury discussed the different policies and rules, and how password policies can cause confusion. He further presented an example of the security policy of federal agencies: passwords contain a combination of letters, numbers and at least one special character. While policies are meant to regulate behavior, answers to a lot of questions in password policy can also be found in developing taxonomy. The research did conduct a 50-question survey for 45 days. The research team received a total of 600 responses for 30-35% response rate.

Mr. Killoury will be returning to Carnegie Mellon after the summer, and Mary Theofanos and Yee-Yin Choong, NIST, will continue working on the project. Mary Theofanos is also running a project on Password Policy.

National Initiative for Cybersecurity Education (NICE)

Dr. Ernest McDuffie, NIST

Ernest McDuffie has been the lead for NICE since early 2010. NICE is an extension of CNCI Initiative 8. The plan is to expand it to make it less classified as a federal focus towards a national focus. Presently, NICE is organized into four tracks so as to reach out to everyone from CIO Offices, and education for everyone up to graduate level. There are a number of events beginning with a kick-off workshop on August 11 and 12, 2010, at NIST to provide an overview of the tracks. He emphasized that educating the population in cyber security is the fundamental crossroad. Track 1 is the National Cybersecurity Awareness championed by DHS. Track 2 titled Formal Cybersecurity Education, co-Leads by Department of education and OSTP. Track 2 is the formal education tool across the whole spectrum with many agencies involved and covers online safety, securing systems and network, tools, capabilities, and of course, curriculum. Track 3 titled Federal Cybersecurity Workforce Structure is led by OPM. This track focuses on workforce structure, and hiring and certification of cybersecurity personnel. Finally, Track 4, Cybersecurity Workforce Training and Professional Development, is managed by DoD, ODNI, and DHS. In this track there are four levels and it concentrates on workforce development. Track 3 and Track 4 share many similar functions and they often intersect. In order for this national program to be successful, it is very important to begin reaching out to federal agencies and the private sector. It would be beneficial to pinpoint the common interests and value added through coordination with agencies to gain their supports.

NASA Continuous Monitoring Program

Information System Security: The Path Forward with Automated Continuous Monitoring
Jerry L. Davis, Deputy CIO IT Security Division (ITSD), NASA
(presentation provided)

In his presentation, Jerry Davis discussed Risk Management, Authentic Information Driven Risk Management, and NASA's strategy for IT Risk Management. The strategy is to identify a risk profile from the Incident Management System. The descriptive approach was explained in a memorandum that NASA released on May 18, 2010 [http://www.govexec.com/pdfs/051910j1.pdf]. The memo explained the shift in direction toward "a value-drive, risk-based approach to system security." He began his talk with Automated Continuous Monitoring, the architecture and performance measurement with the use of Risk Score cards. The approach is to concentrate on three major areas with the system owners in the center, each center has center direct and match controls to vulnerabilities. By looking at the different control on the attack tree, ITSD had analyzed thousands of incidents. As the system is totally visible and closely monitored daily and hourly, ITSD is able to gather data on trends, patterns, and define vulnerabilities not only to predict potential vulnerabilities but also for use in training. The program is only responsible for high level assessment and not for personal individual level. Einstein will be implemented in a couple of months.

The meeting recessed at 5:15 P.M., August 4, 2010.

Thursday, August 5, 2010

The Chairman of the board reconvened the meeting at 9:00 A.M.

The board approved the meeting minutes for April 2010, albeit making a few minor changes – correction of typo and adding of page numbering. A motion was proposed by Joe Guirreri and seconded by Matt Thomlinson.

The Chair thanked Cita Furlani and Donna Dodson for NIST's support and for their attendance for the entire meeting. The board evaluated the presentation by Jerry Davis, NASA from the previous day. Brian Gouker suggested providing feedback in an informal email on the following points:

- The notion of outsourcing needs to be analyzed
- There are benefits to conducting parallel comparison of baseline assessment with the current continuous monitoring
- The need to identify the real threats

Dan Chenok agreed to forward this information to Mr Davis.

Federal Risk and Authorization Management Program (FedRAMP)

Katie Lewin, GSA
Kurt Garbars, GSA
Dawn Leaf, NIST
(presentation provided)

Ms. Lewin began by explaining how the Problem Statement was constructed: How do we best perform security authorization and continuous monitoring for large outsourced and multi-agency systems? In the wake for federal agencies to adopt cloud computing, the program is to provide a standard and secure process for a governmentwide authorization for contracted IT services. The program is strictly voluntary but agencies using this program will benefit from a reduction in duplication of effort, reduction in cost, and improved in security. FedRAMP conforms with existing Office of Management and Budget and NIST IT security guidance, e.g. SP 800-37 R3, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* and would not require any new laws or new framework to implement the program.

Mr. Garbars expanded on the scope of FedRAMP. He further emphasized that agencies will have the advantage of continuous monitoring space, and agencies with unique needs will be able to define their own requirements. He proceeded to present FedRAMP Authorization Models and also the two aspects of Continuous Monitoring: The Criteria, and the Physical Space.

Dawn Leaf referenced Peter Mell's work on Cloud Computing and SP 800-37. The program is focused on interoperability and affordability. They are meeting with NIST to define the requirements and boundary as they worked hard to push out FedRAMP by the end of this year.

DHS Threat Vector Initiative

Matt Coose, Engineering Architechture support services for NPPD OCIO, DHS

Matt Coose started his assessment work at DHS over a year ago. His work is to gather information on the strategies not only for improvement in the federal government but also for the private sector. He had gathered progress information from 24 of 110 agencies. The information was used to brief small agencies. There is concerted effort to improve the assessment tests with the use of Continuous Monitoring. Through his interaction with agencies and CSOs, he discovered a number of challenges – funding, raising awareness, understanding and knowledge of specific threats, leadership to provide the necessary guidance, communicating threats, needs for qualified staff, making appropriate decisions based on data and/or policies. He did find a few agencies are doing well.

Challenges to VA Information Protection in the 21st Century; Medical Device Security

Jaren Doherty, Veteran Affairs (VA)
(presentation provided)

Jaren Doherty described the problems he encountered at VA. Most of the medical devices have Microsoft operating systems, and there are issues when applying patches to the systems. This becomes an operational problem. The VA has over 50,000 networked medical devices and all locations have at least one device with such operational problem. The devices and the contents are FDA approved which complicated any attempt to load antivirus software as this will violate FDA previous warranties. This creates major concerns including confidentiality, data integrity, malware and more.

Some of the older devices are not FDA certified and not all of the devices are connectable over the internet. The vendors only allow the devices to have standard upgrades but not patches and anti-virus software. Furthermore, the vendors issued manuals with standard login and password. These factors contribute to the opportunities for illegal entries and activities.

The purpose for this presentation is to explore solutions for securing these devices and many other devices used for emergency work. VA has continued to work the issues with FDA, vendors, and other agencies. But it is crucial to resolve the issues on the wired devices so as to move onto the wireless devices. In order to enhance security, VA requires medical device vendors to utilize a Site-2-Site (S2S) virtual private network (VPN). Jaren Doherty discussed the 6-step process using a virtual local area network (VLAN) structure to secure medical devices. He iterated the importance of communicating the threats and of partnership with industry to find solutions. The board will look into inviting a vendor to the next meeting.

GAO Information Security Issues Update

Greg Wilshusen, Director of Information Security Issues, GAO
(presentation provided)

Greg Wilshusen presented a summary for the past four fiscal years of FISMA reports. Some of the key measures required by OMB are around 80-90 percentile. For Information Security, six of 24 elements indicate material weaknesses which are the worst type of weakness. In addition, there are fifteen significant deficiencies. The numbers of reported incidents for FISCAM have increased dramatically and the types varied. Mr. Wilshusen discussed the reports on GAO focus areas including FISMA, Emerging Issues, Consolidation Financial Statements, Training/Methodology and External Liason, Critical IT Systems & Infrastructure and Privacy. All of the recent GAO reports are available on GAO website.

The meeting recessed at 4:15 P.M., Thursday, August 5, 2010

Friday, August 6, 2010

The Chair reconvened the meeting at 8:15 A.M.

National Protection and Programs Directorate Discussion

Bruce McConnell, Counselor to the Deputy Under Secretary for National Protection and Programs Directorate, Department of Homeland Security

Bruce McConnell began his presentation with an overview of activities and followed by activities relating to the Cybersecurity Awareness campaign, which includes Track 1 of NICE. Department of Homeland Security conducted a review this year, which received a lot of attention. Since then, DHS had concluded the entry phase of The National Cybersecurity Awareness Campaign Challenge [http://www.dhs.gov/files/cyber-awareness-campaign.shtm]. The Challenge is a competition to find the most effective and creative plan for educating the American public about cybersecurity. Seven winners were selected. Winners will partner with the Department as part of the planning of the National Cyber Security Awareness Campaign and to ready the campaign for its launch during Cyber Security Awareness Month in October. The Challenge also produced three winning slogans. There are other plans, e.g. setting up of an ambassador program and advisory board to help in awareness campaign; setting up a video making contest, and partnering with social networks. The Cyber Team Advisory Board will be made up of a group of teenagers but will not be set up until next year. They have also selected five tips from tips submitted to communicate and launch with the campaign. A campaign newsletter is also in the work. DHS is working with NIST on a list of things.

In June 2010, National Cyber Incident Response Plan (NCIRP) was released to establish the strategic framework for organizational roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery from a Cyber incident. The NCIRP is designed in full alignment with the Comprehensive National Cybersecurity Initiative and the Cyberspace Policy Review. A data version is about to be tested and they will wait to see the results of the test.

Einstein 2 has been deployed and scheduled to be completed by end of the year. Presently, testing is finished with Einstein 3.

On the topic of cyber ecosystem, the National Strategy for Trusted Identities in Cyberspace (NSTIC – version 6) will provide alignment, security policies, and the vision of the identity ecosystem. Policies play an important part in the defense. Mr. McConnell listed three building blocks – strong authentication, automation, and interoperability. He will be glad to return in six months to provide an update to the board.

Briefing from Cyber Security Coordinator

Howard Schmidt, Cyber Security Coordinator, White House

The Chair welcomed Mr. Schmidt to the meeting. Howard Schmidt previously served as one of the board members. Mr. Schmidt stated that he now has a full staff with two directors. Suzanne Lightman is detailed to his office to cover specifically on FISMA - changing of FISMA, FISMA compliance, the level of security, and visibility. He is working with a Continuous Monitoring type scheme and looking for an ecosystem that people to relate to, not from a government perspective but for the Private Sector as well. Mr. Schmidt plans to finish up these things to present to the President for his approval.

A public report summary for HSPD-12 was released in June 2010. Presently, issuance is at 80% and not full utilization of the cards. The subject of security and identity is often misunderstood as ways to track people on-line instead for protecting people and giving choices to people. Mr. Schmidt highlighted October is National Cyber Security Awareness month. He mentioned the Cybersecurity briefing held at the White House in July 2010, which received tremendous support from the government and was well attended by Commerce Secretary Locke, DHS Secretary Napolitano and many top officials. The briefing was followed a number of activities leading to the National Cyber Security Awareness month. The Comprehensive National Cybersecurity Initiative (CNCI) and various cybersecurity strategies help to reduce vulnerabilities for the government and raise awareness, and simultaneously, convey how the private sector will be able to help.

Howard Schmidt has been meeting with various organizations and agencies both domestic and international. He suggested that the board to invite an internet crimes complaint center so as to see how the ties of local crimes with the bigger picture of cybersecurity and the use of resources. The international groups of countries have agreed to work closely with the US on economic espionage. But it was noted that freedom of speech and laws are handled differently in other countries, and it is necessary for the US to move cautiously. He reported that the US government is coordinating cybersecurity events and set up a structure to work with other countries' crime enforcement. DHS will be responsible for all (.)gov, DoD will be responsible for all (.)mil, and Department of State will be engaged with other countries and trade related entities. Mr. Schmidt will continue to share information with the private sector and continue to encourage private companies to engage both DHS and Commerce. He reported that working groups are set up with senate and congress.

Board Discussion and Action Items

Donna Dodson highlighted on the newly established National Cybersecurity Center for Excellence at NIST that Senator Mikulski is leading. The focus is to create a hub for innovation and development. NIST is working with CIOs on: government-wide mandatory baseline with monitoring checklist for technology structure and architecture, and establish testing so as to understand the environment. It would involve engaging the private sectors so as they will be aware of profile security, coordinating with federal agencies, and working with industries. NIST will be holding a number of workshops to share and gather information.

Action Items –potential agenda topics for November meeting:

- Invite vendors for medical devices (Re. embedded software) from different sectors
- Devices for healthcare records
- A panel on latest legislation on cybersecurity
    - Set up subcommittee consisting of Matt Thomlinson, Alex Popowycz, and Lynn McNulty to review the senate bills. If necessary, the board could call a special session to work on a recommendation.
- Panel discussion on issues with CISOs – aspect of classification, nature of threats classified on NSA's classified systems, methods, activities beside technologies used
- Invite representative from Howard's office – possible strategy
- US Cert Discussion (someone from NIST who have worked on vulnerabilities or US Cert)
- TIS (?) discussion, interesting topic
- SSA's approaches on FISMA and security particularly innovative ones and comparison of small versus large agencies
- Threat trending information —NASA
- FedRAMP — an update at the end of the year
- Donna Dodson to provide a status or share how she would want to make changes
- Emerging issues extracted from the list of reports from GAO/Greg Wilshusen's presentation [see presentation]

- Dan Chenok to check with Howard Schmidt's office for any plan to compile a list of deficiencies and/or gaps
- Matt Thomlinson to research on information on usability issues (standards for identity, privacy, and usability)

The board explored using the various approaches to announcing the board meetings so as to invite and engage public participation and contribution. The approaches raised were Facebook and Twitter, The discussion also examined the length of interactive period, when to open the page for engaging participation, which medium is best suited, uploading of information. There should be a note on the page specifying that questions are for the board members and for the speakers/presenters.

Alex Popowycz mentioned that Howard Schmidt's position as the cybersecurity coordinator is a very challenging role. Dan Chenok asked if there was a sort of map on the National Plan for Cyber Security, Donna Dodson mentioned that she had seen a few diagrams but there is no current, high-level plan. The Chair will research on this with Howard Schmidt's office. Joe Guirreri noted that critical infrastructure protection plan was not discussed from both Howard Schmidt's and Bruce McConnell's presentations. Mr. Guirreri believed it should be a high priority.

The Chair expressed the board's gratitude to Lisa Schlosser and Ari Schwartz for their dedication and expertise that they had brought to the board.

Donna Dodson announced that Annie Sokol, NIST, will be the DFO for the board in all of the upcoming meetings.

The meeting adjourned at 10:57 A.M., Friday, August 6, 2010