INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

MINUTES OF MEETING

October 10, 11, and 12, 2012

<table>
<tr><td rowspan="3">Wednesday, October 10, 2012
9:15 A.M. – 5:20 P.M.

Thursday, October 11, 2012
9:12 A.M. – 5:30 P.M.

Friday, June 1, 2012
8:52 A.M. – 12:40 P.M.

Courtyard Washington Embassy Row, (General Scott Room)
1600 Rhode Island Avenue, NW, Washington, DC, 20036
(202) 293-8000</td><td colspan="2">Present:</td></tr>
<tr><td>Board Members</td><td>Non-Board Members</td></tr>
<tr><td>Daniel Chenok (Chair), IBM
Julie Boughn (via phone), DHHS
Christopher Boyer, AT&T
Kevin Fu, University of Michigan
Gregorg Garcia, Garcia Cyber Partners
Brian Gouker, NSA
Toby Levin
Edward Roback, Dept. of Treasury
Phyllis Schneck, McAfee Inc.
Gale Stone, SSA
Matthew Thomlinson, Microsoft
Peter Weinberger, Google</td><td>Donna Dodson, NIST
Annie Sokol (DFO), NIST
Kevin Stine, NIST
Megan St. Clair, NIST

See Annex A for record of presenters and visitors</td></tr>
</table>

Wednesday, October 10, 2012

The ISPAB Chair, Daniel Chenok, called the meeting to order at 8:50 AM, and began with the Board members providing a narrative of their recent and current activities. Dan Chenok, Chair, paid tribute to and reflected on the life of F. Lynn McNulty. Mr. McNulty[1] served on ISPAB Board, 2006-2011, passed away on June 4, 2012.

Julie Boughn joined the meeting on the phone during the 2½-day meeting.

NIST Updates
Donna Dodson, Chief,
Computer Security Division, NIST

Donna Dodson has fully assumed responsibilities as Cybersecurity Advisor from William C. Barker. W. Curt Barker who was previously Chief, Computer Security Division (CSD), NIST, and Cybersecurity Advisor, retired recently but will continue to work part-time at NIST. Donna Dodson stated that CSD has completed the final reorganization.

There are a number of initiatives relating to cloud computing and particularly combining with Big Data. In the areas of mobility and cloud computing in USG, Adam Sedgwick has

[1] http://fcw.com/articles/2012/06/15/feat-people-lynn-mcnulty-cybersecurity.aspx

been a major help.

She also discussed the activities relating to National Cybersecurity Center of Excellence (NCCOE). Ms. Dodson provided an overview of NCCOE funding and mission. She discussed ONC (Office of the National Coordinator for Health Information Technology) and NIST collaboration work on electronic health records, and with health IT focused on doctors in hospitals. NCCOE supported development of several use cases as starting points. NCCOE is hosting various outreach events and is working closely with NICE (National Initiative for Cybersecurity Education) to develop education programs. These activities aim at finding ways to work with small business, manufacturers, and communities.

SP 800-53 Rev.4, Security and Privacy Controls for Federal Information Systems and Organizations

Ron Ross, NIST Fellow, Computer Security Division, NIST (Presentation provided)[2]
Dom Cussatt, Senior Policy Advisor, US Department of Defense (Presentation provided)[3]
Greg Hall, Identity Management Program Manager, ODNI/CIO
Tim Ruland, Chief IT Security Officer, US Census Bureau

Dr. Ron Ross's presentation focused on: 1) update on the development and publication status of NIST Special Publication 800-53 Rev.4; 2) Implications of this revision; and 3) provide a status report on the transformation to the unified information security framework and potential impacts with this revision. He explained the work of the joint task force and the milestones accomplished with this revision. The elements that influenced major changes to this revision were also discussed. One of the changes involved moving the appendix on Industrial Control System to NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security[4]. Privacy requirements and controls will be part of standard lexicon. The changes are intended to increase strength of IT infrastructure as well as every aspect of security controls. It is necessary to build security programs using the integrated project team concept. The final draft of 800-53 Rev. 4 was scheduled to be completed by end November or December.

Dom Cussatt's presentation titled, DIACAP to Risk Management Framework (RMF) Transformation, included background and benefits of DoD Information Assurance Certification and Accreditation Process (DIACAP) to RMF Transformation. A Joint Taskforce formulated with NIST to look at the core information assurance (IA) policies to normalize them into a common body: SP 800-50 series. Mr. Cussatt explained how the transformation is executed - DoD is transforming IA policies and practices to align with Federal government risk management policies and practices, and NIST policies will align

[2] Ron Ross's presentation (http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_oct2012_rross_sp800-53-rev4.pdf)
[3] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_oct2012_dcussatt_dod-rmf-transition-brief.pdf)
[4] http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

with policies of DoD and NSS/IC. The transformation was under review and scheduled to be ready end October.

Greg Hall using the same presentation from Mr. Cussart, discussed the process that Office of the National Intelligence (ODNI) used to update its document. This is to leverage work completed by NIST and Committee on National Security Systems (CNSS) to build/develop cybersecurity policies. There are challenges to provide appropriate controls for the real world with appropriate policies. In particular, it is challenging to implement the RMF when they are making major changes to the infrastructure.

OIG Perspectives on Cloud Computing and FISMA (OIG Panel)

Gale Stone, (Moderator), Deputy Assistant Inspector General for Audit, Social Security Administration (SSA)
Dr. Brett M. Baker, Assistant IG for Audit, National Science Foundation (NSF) (Presentation provided) [5]
Kathy Buller, IG, US Peace Corps
Special Agent Charles Evans Coe, Jr., AIG for IT Audits and Computer Crime Investigations, US Department of Education
Andy Patchan, Assistant IG for Audit, Federal Reserve Board (Presentation provided) [6]
Sabrina Segal, General Counsel, US International Trade Commission

IG Panel noted that cloud providers sell service packages to Agencies that do not include forensics, thus generating additional cost to Agencies when the cloud provider needs to help access files for forensics or following a breach. Discussion was around the need for agencies to report breaches, and the future hope to resolve the potential additional unexpected costs incurred from cloud providers.

Kathy Buller stated that the biggest problem as an Inspector General (IG) is dealing with new and emerging technology. The broad nature of the cloud may require setting up FISMA related review in the future. From law enforcement perspectives, law enforcement and litigation are closely related, which will require access to the data internally and externally. There are difficulties with meeting multi-jurisdiction – circuits with different regulations. She pondered of how to limit storage of data outside of the US.

Charles Evans Coe Jr. discussed subcontracting issues and control of data, cloud environment, and the push to provide appropriate contract language for cloud computing. The OIGs developed a paper on Cloud Computing contract concerns and contract language. The paper was presented to the GSA FAR Council and the contractual language was applied to business use cases.

[5] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_oct2012_bbaker_oig-presentation.pdf
[6] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_oct2012_apatchan_oig-perspective-cloud-computing-fisma.pdf

Andy Patchan has a lot of experience in system administration and recently been briefing congress on FISMA and FISMA reporting. He illustrated a baseline of OIGs reviews; OIG responsibilities under FISMA, and also described annual evaluation on policies, procedures and systems.

Dr. Brett M. Baker discussed current FISMA Overview at NSF. He showed a framework of FISMA Oversight that is used by most of the IGs. He explained the framework and talked about the OIG FISMA narrative report. Dr. Baker suggested to supplement OMB questionnaire with a narrative report and to ensure results are communicated between FISMA and Financial Statement auditors.

Data and issues with Public Safety Communication

Matt Blaze, Professor, Computer and Information Science, University of Pennsylvania (Presentation provided) [7]

Matt Blaze stated that he generally discussed the practical point of view on application of cryptography and usability in system. He explained that Apco Project 25 ("P25") is a project that has been started by his department, but it is currently NSF funded. It is a security standard for digital two-way radio (voice and low-speed text). It is intended as a digital replacement of two way radios. The goal is to encourage interoperability and non-disruptive. The system includes cryptographic security options with a one-way protocol.

There were no obvious cryptographic weaknesses in the security of the P25. He discussed attacks such as there is no authentication of voice traffic or displayed metadata. Matt Blaze also discussed potential usability problems including; poor feedback about crypto state, frequent rekeying and unreliable rekeying. He suggested the best way to fix is through standards and implementation practices.

Security/ Privacy/ Information Sharing

Dan Chenok, Vice President for Technology Strategy, Public Sector Strategy & Innovation Practice Senior Fellow, Center for The Business of Government IBM Global Business (Presentation provided) [8]

This was the last meeting that Daniel Chenok will be the Chair of ISPAB. It is ISPAB's tradition to reserve a session for every out-going member.

At the center of all of these terms is information. Information is the Connective Fabric in the 21st Century Economy Information Sharing. The concepts need to be incorporated in early planning by design, and privacy as a principles, is to build trust. It is agreed that it is not just about the Information but about the service. In some cases it is more about the

[7] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_oct2012_mblaze_p25-security-analysis.pdf
[8] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_oct2012_dchenok_information-sharing.pdf

service than the information itself. There are many forms of sharing information in the US Government, and information sharing impacts intelligence, homeland security, law enforcement, cybersecurity, as well as many activities of government. Dan Chenok presented government's policy and resources regarding information sharing. In order to be effective at enabling sharing while promoting privacy and security, the following basic steps need to be observed – education, understanding of risks and understanding need to protect PII.

Privacy – there are a few ways to think about building trust. Mr. Chenok included steps based on (Fair Information Practice Principles[9]) FIPPs-based Principles for Info Sharing. He also described new structures and an operational perspective for recognizing security in building trust. In conclusion, Mr. Chenok discussed potential oversight for sharing cyber information in the context of privacy and security.

In closing, Dan Chenok pointed to two newly/future documents relevant to this discussion: CSIS[10] and DPIAC Report[11] due out in November 2012.

[9] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf - The FIPPs are a set of eight principles that are rooted in the tenets of the Privacy Act of 1974 (Privacy Act of 1974, 5 U.S.C. § 552a, as amended.)

[10] http://csis.org/events/all?filter0=information+sharing

[11] http://www.dhs.gov/sites/default/files/publications/privacy/DPIAC/dpiac_cybersecurity_recommendations_11072012.pdf

THURSDAY, October 11, 2012

The Chair opened the meeting at 9:12 A.M.

DoD Digital Strategy

Robert Carey, Principal Deputy, US Department of Defense CIO

Mr. Carey emphasized the role of CIO in cybersecurity, and the needs to have leaders to make decisions with agility and be accountable. He recommended consolidation and centralization managed at one single point such as CIO Council. There were two things that he considered are most important in the mobile space – it would be helpful to clarify the path and connection of FIPS standards, and clarify a simple way to attach identity to any device. It is important to consolidate and standardize network architecture, implement private cloud, and Dos stack so as to prevent information to flow. He acknowledged that there is a struggle between convenience and security.

Rob Carey suggested that NIST to set up working group to define policies, implementation of PKI, privacy, management of devices, enabling interoperability, and most importantly, to sync with SP 800-53 controls.

Mr. Carey credited *FedRAMP*[12] (Federal Risk and Authorization Management Program) for providing applicable use cases. While FISMA (Federal Information Security Management Act)[13] offers a good workable focus, it is not keeping pace with managing risks. Rob Carey encouraged the Board to incentivize the interaction between industry and government.

Executive Office Updates

Andy Ozment, Director of Cybersecurity, White House

Dr. Ozment briefly discussed his responsibilities. Apart from his responsibilities as the internal cyber security advisor, he also covered international and worldwide issues including: secure Federal networks, working with private sector to protect critical infrastructure, incident response, intelligence and reporting, and structuring the future cyber environment.

The priorities for securing Federal networks are strong authentication, continuous monitoring, trusted computing, HSPD12[14], and most critical to follow FISMA. There are fourteen government-wide priority goals as according to the Government Performance and Results Act[15]. Cyber security should be considered as one of those major goals. Einstein III remains critical program as legislation on cybersecurity is still being work on.

[12] http://www.gsa.gov/portal/category/102371

[13] http://csrc.nist.gov/groups/SMA/fisma/overview.html

[14] http://www.dhs.gov/homeland-security-presidential-directive-12

[15] http://www.whitehouse.gov/omb/mgmt-gpra/index-gpra

Protecting Critical Infrastructure: Smart Grid /Electric Sector model was successfully accepted and it would good to have other sectors mirror its success. It has been considered to provide the model to investment sector and to develop to the next level where people will be provided their control systems. The maturity model will need more standards and legislation.

Incident Response and Intelligent Reporting: The national level exercise was very productive and successful. The exercise gained major improvements and made real operational progress, and there was plan to institutionalize this progress.

Engage Internationally: The White House launched the US International Strategy for Cyberspace[16] in May 2011. The International Strategy lays out the President's vision for the future of the Internet, and sets an agenda for partnering with other nations and peoples to achieve that vision. While the strategy is realistic about the challenges we face, it nonetheless emphasizes that our policies must continue to be grounded in our core principles of fundamental freedoms, privacy, and the free flow of information.

Shape the Future Cyber Environment: There are enormous research being done and some of which adopted only fairly recently, e.g. work done through National Strategy for Trust Identities in Cyber Space (NSTIC) and NICE.

In response to questions on FISMA reporting and its values, Dr. Ozment stated that the Annual Questionnaire and reporting provide opportunities to engage management. The initial authorization process is very effective.

GAO & Medical Devices

Kevin Fu (Moderator), Associate Professor, Computer Science, UMass Amherst
Vijay D'Souza, Assistant Director, US Government Accountability Office (GAO)
Brian Fitzgerald, Deputy Director, Division of Electrical and Software Engineering, FDA CDRH OSEL
Mark Olsen, CISO, Beth Israel Deaconess Medical Center, Boston, MA (Presentation provided)[17]

Kevin Fu summarized past ISPAB discussions on medical device security, and recommendation letters[18][19] submitted to OMB, as an introduction and continuation for this panel discussion.

Mr. D'Souza began by summarizing GAO Report #12-816 entitled "*Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices*"[20]. This report, released on September 27, 2012, had three objectives: identify threats and

[16] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
[17] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_oct2012_molson_medical-device-security.pdf
[18] http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-ltr-to-omb_med_device.pdf
[19] http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/HealthIT12010.pdf
[20] http://www.gao.gov/products/GAO-12-816

vulnerabilities to devices; explore the extent to which FDA *(US Food and Drug Administration)* examines security in implantable premarket devices; and determine FDA's post market efforts to examine information security problems in these devices. Mr. D'Souza provided a summary of the report, including a review of intentional and unintentional threats and vulnerabilities to medical devices and challenges in mitigating identified risks. The report recommended that FDA develop a plan to focus on these issues. The report was not prescriptive but suggested that FDA work with resources from other agencies such as DHS and NIST to establish milestones for executing this plan.

Mr. Fitzgerald acknowledged that FDA was grateful for the GAO oversight, and stated that the important things to take into consideration include balancing the set of risks, taking into account reasonable foreseeable events. Until recently, proactive attacks on medical devices didn't rise in many people's minds as foreseeable risks. There is FDA precedent for taking into account malicious risks (ex, Tylenol poisoning event gave rise to tamper evident packaging). Mr. Fitzgerald indicated that there are several different types of reviews ongoing at this time, including outreach to industry and consumers of medical devices, and expressed the possibility of additional outreach now that cybersecurity risks could be considered reasonable foreseeable. Mr. Fitzgerald indicated that this additional outreach requires additional resources, development of internal expertise, technology and culture change, and a systematic risk management approach.

Mr. Olsen provided a context for how his organization deploys security today, as well as the exposures that come with that deployment. Mr. Olsen described zoned security at the network layer, with over 12,000 systems actively on the network, including 905 devices on the wired network and approximately 2000 wireless devices (ex, IV pumps). Most devices are using embedded Windows operating systems, including Windows 95, 98, CE, 2000, and XP Service Pack 3. Mr. Thomlinson, Board member, indicated that Microsoft does not support any of these Windows operating systems except XP Service Pack 3, and even that one will no longer be supported shortly. Mr. Olsen indicated that cleaned devices become reinfected in about 10-12 days after being placed back on the network, with some devices running older operating systems taking less than a day for reinfection. Compared to other IT equipment that is controlled through patching and anti-virus, there is a noted different in the time it takes to infect. Mr. Olsen expressed the concern that devices could become infected to the point where they can't provide information needed to deliver care. Mr. Olsen discussed an example of a device used to monitor high risk pregnancy - a control system that feeds data to a central repository for more monitoring. Mr. Olsen indicated that these devices become compromised and no longer record data; the screens still show data to monitor manually but recording stops. Mr. Olsen discussed other types of devices that, if compromised to the point where they can't be used or values are adjusted to provide questionable results, could cause harm to patients. Mr. Olsen indicated that there are no good models for protecting these devices. He described one model of putting all devices on separate wired networks, but indicated that there are major costs to doing this. He indicated that device vendors say they are 510 certified so they cannot add patches or put firewalls on the devices. Mr. Olsen indicated that he is looking to get support in some fashion to convince FDA to make stronger statements and that vendors should not hide behind their 510 certification. Mr. Olsen's desired outcome of this session is for some type of maturity model based on good practices that still provide hospitals needed flexibility to meet business needs.

Mr. Fitzgerald indicated that it is not FDA policy to prevent patching of devices. He indicated that FDA does hear from hospitals that certain manufacturers are unwilling to patch devices. He indicated that it is important for knowledgeable customers in the security field to be involved in the procurement processes for medical devices. Mr. Fitzgerald suggested that patching medical devices for security is permitted from FDA's perspective and that if the manufacturer was not doing that, to notify FDA. Mr. Fitzgerald indicated that patching does not reset the cycle for device certification.

Mr. D'Souza indicated that GAO had talked with some manufacturers about the patching issue and manufacturers indicated they did not want to patch devices to jeopardize their certification. Mr. D'Souza indicated that the general feedback was that the possible benefit of issuing a patch is far outweighed by the risk – the issue is one of liability.

The Board discussed reporting of medical device adverse events; the governance framework across government, including roles other agencies such as NIST and DHS could play in the medical device space; the role liability to the consumer plays in the decision; and also manufacturers abilities to test changes to devices and inform customers.

Mr. Thomlinson, Board member, indicated that there appears to be a market failure because no vendor appears to provide good support, to stand behind their product, and to provide a resilient product. Mr. Olsen indicated that consumers do not push back. He indicated that hospitals must buy these devices for treatment purposes, and that if their organization does not purchase, another organization will purchase and provide the treatment. Mr. Olsen also indicated that this is a low volume market product – it is hard to put pressure on the device manufacturers.

Mr. Thomlinson remarked that a baseline standard for safety of this equipment that says manufacturer is responsible for the care of the device is needed. Mr. Fitzgerald indicated that the FDA Office of Compliance would handle complaints, and that FDA rarely hears from users of medical devices. He indicated that users need to come forward because if they do not, it does not appear to be a problem. Mr. D'Souza indicated that an architectural security model is needed for these devices.

Dr. Fu summarized the themes of the session and follow-on discussion: there needs to be a way to get stronger requirements for patching and maintenance of software on a regular basis with responsibility and accountability aligned with those that actually make a difference.; there needs to be engineering, risk management, and purchasing practices; and FDA resources are overwhelmed to carry out this burden.

Compliance & Oversight Principles

John DeLong, Director of Compliance, NSA

Mr. DeLong has served as the Director of Compliance at NSA since 2009. This role specifically focuses on NSA rules and policies that govern foreign intelligence. He indicated that oversight and compliance are two distinct parts of the same coin. Compliance verifiable consistency with clearly defined legal and policy rules, while oversight is independently looking at performance and quality. Mr. DeLong specified the four points he has learned about compliance: it works well when everyone (ex, lawyers, policy, oversight) understands their role in the ecosystem; the compliance organization is a microcosm of NSA (a collection of different roles across NSA); manage across but not within; and focus on understanding the legal and policy requirements, many of which are externally defined, that we must comply with.

Mr. DeLong indicated that NSA colleagues consider compliance as a help; they are invited to budget planning meetings. He also indicated that the earlier compliance is involved, the greater in understanding where compliance can be applied in technology and rules. The benefit for the NSA compliance approach is being able to evolve internal controls over time from human to automated process.

Mobile Security

H. Richard Holgate, Assistant Director for Science & Technology/CIO, Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF)
Bradley Nix, Director/CISO, OIT/Information Security Office, Food and Nutrition Service, US Department of Agriculture
Bryan M. Pagliano, Special Advisor, US Department of State

Mr. Holgate began by indicating that many agencies face issues around mobile security. He continued that the Federal CIO announced the Federal Mobility Strategy[21], and that all panelists are involved in developing that strategy, which is part of the larger Digital Government Strategy. Mr. Holgate indicated that the 10.2 deliverable was to be released on November 23, and deliverable 9.1 (a mobile security framework for government co-led by DHS, DOD, NIST) was to be released on May 23, 2013.

Mr. Nix discussed that are majority of security controls in 800-53 are available for mobile, but that there are opportunities for improvement or revision to tailor to a mobile environment. A concern suggested by Mr. Nix is that we continue to have a data problem inasmuch as we have a challenge in the unclassified space to understand data sensitivity. Mr. Nix indicated that USDA is attempting to understand that data needs to be treated differently (ex, PII, financial, contract) – there are some types of data that must be held more closely when dealing with mobile technologies. For example, Mr. Nix described that providing someone access to data through email, they may be accessing PII with a

[21] http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf

personally owned device. Mr. Nix indicated that it is possible for security officers to say no to these types of implementations but need to find ways to enable these capabilities in secure ways. According to Mr. Nix, data classification taxonomy and guidelines are lacking. Mr. Nix indicated that it is a difficult, but worthwhile process to go through an organization's data, identify the data sources, and identify how the data should be marked – the adoption of mobile technology provides an opportunity to do this. Mr. Nix also remarked that rapid agile product development is intersecting with this mobile technology adoptions, making it challenging for security to keep up.

Mr. Pagliano stated that these mobile devices and BYOD (Bring Your Own Device) are upon us – security professionals need to determine how to take the customer wants, secure it, manage it, but not provide the customer with an unusable technology. Policies are needed to help dictate how services can be used within each organization.

Mr. Thomlinson asked about any thoughts on architectural changes – for example, the proper BYOD device configuration, device encryption, separation of personal and enterprise data, data wipe. Panelists responded that translating this into a practical solution is challenging. Panelists also remarked that there is a need for policy, and ways to take technologies and apply them in new ways to address the mobile security challenges. Panelists also remarked that the parallel adoption of a risk management framework (SP 800-37 Rev.1, *Guide for Applying the Risk Management Framework to Federal Information Systems – A Security Life Cycle Approach*), increased continuous monitoring, and greater adoption of mobile technologies also provide a great opportunity.

The Board and panelists discussed FIPS 140-2 and the Cryptographic Module Validation Program as it relates to mobile devices. The Board asked how this cryptographic module validation program can work more smoothly. Mr. Nix remarked that vendors are able to innovate without FIPS 140-2, and it makes it difficult for CIOs to adopt products just because it utilizes a FIPS 140-2 validated cryptographic module. He remarked that it makes CIOs make risk based decisions that could be inconsistent with current law and policy because a cryptographic module is not 140-2 validated.

Donna Dodson indicated that there continue to be misunderstandings about the cryptographic validation program. She remarked that agencies use cryptography when they decide it is an appropriate security control to protect agency data; if encryption will be used, it must be FIPS 140-2 validated. Mr. Nix indicated that there is inconsistent agency understanding and interpretation of FIPS 140-2. Ms. Dodson indicated that NIST would be happy to meet with agencies to clarify the requirements.

Mr. Thomlinson indicated that, in a highly competitive market, FIPS 140-2 is not number one on a vendor's priority list, but that this discussion provides good motivation – if vendors build it in, agencies can buy it; but agencies cannot buy the device if vendors do not build it with FIPS 140-2.

FRIDAY, October 12, 2012

The meeting began at 8:52 A.M.

FedRAMP Updates (Informative)
Kathy Conrad, Principal Deputy Associate Administrator, Office of Citizen Services and Innovative Technologies, GSA (Presentation provided)[22]
John Streufert, NCSD Director, DHS, Cybersecurity & Communications, National Cyber Security Division

FedRAMP[23] is the result of close collaboration with cybersecurity and cloud experts from NIST, DHS, DOD, NSA, GSA, OMB, the Federal CIO Council and its working groups, as well as private industry. Ms. Conrad valued the communication and working collaboration with the private industry. She described FedRAMP progress since its launch in June 2012. FedRAMP has received over 50 applications. Joint Acquisition Board (JAB) established according to OMB policy memo, review the security assessment package based on a prioritized approach. FedRAMP relies on NIST for privacy experts.

When granting an agency Authority to Operate (ATO), Kathy Conrad stated that they are looking for diversity from Cloud Service Providers (CSPs) in term of FISMA readiness, Assessment readiness and Agency demand. In the presentation, Ms. Conrad presented FedRAMP phases and timeline, and indicated that they are currently in an initial operational capabilities (IOC) phase. In FY13 Q2, they progress to full operations, and by FY14, they should be in sustaining operations phase. As part of the IOC phase, they plan to issue three FedRAMP Provisional Authorizations by the end 2012; build up FedRAMP repository, and maintain update in preparation for full operations. During this phase, they work hard in keeping all stakeholders informed through organized webinars and outreach to industry and government, and maintaining security documentation. It is important to work closely with the CSPs to ensure their processes are also working smoothly and seamlessly. All documentation and detailed information of FedRAMP process are publicly accessible on the FedRAMP.gov website.

Ms. Conrad also discussed the JAB Provisional Authorizations that are favored by many CSPs. FedRAMP is mandatory process for adoption of all but private cloud computing. Among many remaining challenges, they are still working on solutions for complying with background investigation requirements. She also unveiled some lessons learned and how best for all partners to achieve success. The heart of FedRAMP is trust from the ATOs. She stated they are pleased with the progress.

[22] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_oct2012_kconrad_fedramp-status.pdf
[23] http://www.gsa.gov/portal/category/102375

Mr. Streufert talked about the Dashboard of FedRAMP, stating that the Dashboard has sensors connected to it. They wanted to make this a way for state and local government to be able to buy it. He showed a wheel that lists 15 logical areas in the 800-53 controls. Talked about what phase each of these areas are located in, entitled P1, P2, P3 and P4. He talked about Effectiveness Measure Testing and how they are working very closely with NIST on this, including Kevin Stine and Kelley Dempsey.

Public Participation:

Bruce Levinson, Center for Regulatory Effectiveness

Mr. Levinson talked about the Cyber Security Regulation and that he believes an overall principle should govern it and suggested someone from the Private Sector. Cost Effectiveness is the key to govern it. Cost Benefit Analysis, like what John Streufert was discussing, is going to be very beneficial to Cyber Security Regulation. He talked about the importance of early outreach from Industries to Public. OMB working with the agencies shows that they already have the authority. Case studies and best practices studies are a cost effective approach. He would like to the board to recommend to the government to continue to work with industry on case studies and best practices.

NCCIC - Updates

Larry Zelvin, NCCIC Director, DHS (Presentation provided)[24]

Mr. Zelvin has been working in the DHS NCCIC, Arlington, Virginia, for past five months. He is a retired naval officer, and was a staff member of National Security for three 3 years. NCCIC is a 24/7 operation, and involve a wide spectrum of people including government, industry, private and international sectors. NCCIC role is not to direct, but to provide situational awareness. The NCCIC analyzes the information to figure out the ultimate focus and expectation. The in-house and virtual capabilities include NCERT, ICS Cert. 16 ISACS. Mr. Zelvin also elaborated on involvement of international partners and USCERT.

Mr. Zelvin discussed a number of concerns including:

- Commonalties in operating with other partners
- There is not a community standard on threats that are coming.
- Challenges in communicating awareness to the public
- The biggest concern is the speed of the reaction to threats and attacks. The public's expectation is that is the reaction is right away.

Mr. Zelvin stated that some of analysis should be automated as human to human is too slow. But he has to meet with stakeholders individually because they refuse to talk openly. Larry Zelvin would appreciate inputs/comments from the Board and will continue to looks forward to hearing from the Board.

[24] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-10/ispab_oct2012_lzelvin_nccic-overview.pdf

Ethics Briefing (Informative)

Jeffrey Harrington, Senior Counsel, Ethics Law and Programs Division, Office of the General Counsel

Mr. Harrington is an attorney on duty every day. He discussed each of the basic rules of a FACA Board to the ISPAB Board.

Healthcare Security

Kevin Stine, Group Manager, Computer Security Division, NIST

Mr. Stine began his presentation with the question of where should NIST be focusing their health IT activities. He discussed the broad program conducted under Information Technology Laboratory (ITL) at NIST. It is a lean but effective operation, and a lot of work is Applied Security. The three buckets of Health IT within ITL are Coordination, Outreach and Integration. NIST has been working with ONC on electronic health record technology. He talked about the health record technology abilities and Self-Regulatory Programs. He mentioned the NVLAP organization within NIST, and how it has been a model for Electronic Health Records. He stated that ONC maintains a website of products that have been validated and the role in Computer Security Division is to develop the test certifications.

NIST is especially proud of its outreach effort. They have cohosted, with the Office of Civil Rights (OCR), a Health IT Conference[25] and it has been growing over each year. The National Institute of Standards and Technology (NIST) and the Department of Health and Human Services (HHS), Office for Civil Rights (OCR) co-hosted another conference sometime in spring 2013. It is intended to reach out to small and medium size organizations through these outreach efforts.

The outreach effort also helps to promote the HIPPA Security Rule Self-assessment Toolkit[26] and website, SCAP.nist.gov/HIPPA[27]. The toolkit is to help the user with requirements using a plain language, helping to provide tips and strategies of the rule. The Toolkit has been downloaded over 10,000 times since November 2011, and other sectors not related to Health IT have asked if they could use the same idea.

In closing, Mr. Stine informed the Board that they are updating SP 800-66 Rev 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*[28].

[25] http://www.nist.gov/itl/csd/hipaasec.cfm

[26] http://scap.nist.gov/hipaa/NIST_HSR_Toolkit_User_Guide.pdf

[27] http://scap.nist.gov/hipaa/

[28] http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

Board Discussion

A) The Board review of the session discussions for this meeting:

1) *NIST Updates:* Donna's discussion was just informational and the Board would like to have continue updates on NCCOE.

2) *SP 800-53 Rev.4*: Donna Dodson suggested drafting a letter emphasizing the importance of the work on this standard and the excellence work by Dr. Ross and the joint task force. The Chair will draft the letter. *(Action)*

3) *OIG Perspectives on Cloud Computing and FISMA*: There was a question of whether the Federal Acquisition Regulation (FAR) has provided any standardizing contractual clauses. The Board is interested in the information included in the FISMA reporting that is provided to IGs.

   - Potential panel on FISMA reporting for future meeting (*Action)*

4) *Data and issues with Public Safety Communication* (Matt Blaze): It is an interesting discussion and technical presentation.

5) *Security / Privacy / Information Sharing:* Phyllis Schneck and Matt Thomlinson will draft a recommendation letter to OMB with Dan Chenok's presentation as the base concept. Toby Levin suggested to include information on DHS information sharing policies that ODNI required of some agencies.
Brian Gouker proposed a motion to approve the recommendation and
Phyllis Schneck seconded the motion. *(Action)*

B) The meeting minutes for October will be reviewed and approved at the next meeting in February 2013 as the Board did not have sufficient time to review them at the meeting.

C) Matt Thomlinson and Phyllis Schneck will work on the agenda topics for the next meeting in February 2013.

D) *Future Agenda topic:* organize a panel to discuss next generation public safety network. Possible panelist, Anna Gomez, NTIA. *(Action)*

E) Donna Dodson presented a plaque to Dan Chenok in recognition of his dedication and service to the ISPAB Board. Dan Chenok had been a member (2005-2012) and Chair of ISPAB since 2006.

F) The Board agreed on the following dates for ISPAB meetings in 2013:
February 13, 14, 15
June 12, 13, 14
October 2, 3, 4

The meeting adjourned at 12:40 P.M., Friday, October 12, 2012.

Annex A

LAST	FIRST	AFFILIATION	ROLE
Baker	Brett M.	NSF	Presenter
Barbour	J.	RIM	Visitor
Blaze	Matt	University of Pennsylvania	Presenter
Bloch	David	Medtronic	Visitor
Brewer	Tanya	NIST	Visitor
Buller	Kathy	US Peace Corp	Presenter
Camm	Larry	Schweitzer Engineering Labs	Visitor
Carey	Robert	US DOD	Presenter
Chowdhury	Zayed	Infusive Tek	Visitor
Coe, Jr.	Charles Evan	US DOE	Presenter
Coffey	Kaitlin	US GAO	Visitor
Conrad	Kathy	GSA	Presenter
Cussatt	Dom	US DOD	Presenter
Davila	Jonathan	Earthling Security, Inc.	Visitor
Davis	John C.	Teknowork Inc.	Visitor
DeLong	John	NSA	Presenter
D'Souza	Vijay	US GAO	Presenter
Fitzgerald	Brian	FDA	Presenter
Grote	Matt	Senate Homeland Security Committee	Visitor
Guirreri	Joe	PE Systems	Visitor
Hall	Greg	ODNI	Presenter
Harrington	Jeffrey	US DOC	Presenter
Hasting	Nelson	NIST	Visitor
Holgate	H. Richard	ATF	Presenter
Hornsten	Jayne	NSF	Visitor
Huynh	Jim	US Dept of Education	Visitor
Landau	Susan	Privacy Link	Visitor
Larsen	Kristopher	Sprint	Visitor
Lee	GayHee	US GAO	Visitor
Levinson	Bruce	Center for Regulatory Effectiveness	Visitor
Miller	Jason	Federal News Radio	Visitor/Media
Nix	Bradley	US DOA	Presenter

LAST	FIRST	AFFILIATION	ROLE
Olson	Mark	Beth Israel Deaconess Medical Center, Boston, MA	Presenter
Ozment	Andy	White House	Presenter
Pagliano	Bryan	US DOS	Presenter
Patchan	Andy	Federal Reserve Board	Presenter
Porter	Esten	MITRE	Visitor
Rahman	Mushad	Excentium Inc.	Visitor
Ross	Ron	NIST	Presenter
Schooley	Melissa	Nedtronic	Visitor
Sedgewick	Adam	NIST	Visitor
Serban	Jason		Visitor
Souppaya	Murugiah	NIST	Visitor
Stine	Kevin	NIST	Presenter
Streufert	John	NCSD	Presenter
Suh	Paul	BAH	Visitor
Willis	John	Lockheed Martin/US Mint	Visitor
Zelvin	Larry	DHS	Presenter