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

February 11, 12, and 13, 2015

U.S. Access Board, 1331 F Street N.W. Suite 800, Washington, DC, 20004, (202) 898-4000
http://csrc.nist.gov/groups/SMA/ispab/documents/agenda/2015_agenda-ispab-february-meeting.pdf

Board Members	
Peter J. Weinberger, ISPAB Chair, Google Chris Boyer, AT&T (via phone) John R. Centafont, NSA Dave Cullinane, Security Starfish. LLC (via phone) Kevin Fu, University of Michigan Greg Garcia, FSSCC Toby Levin Edward Roback, US Department of Treasury Gale Stone, Social Security Administration Daniel Toler, US Department of Homeland Security	Board Secretariat and NIST staff Matt Scholl, DFO, NIST Annie Sokol, DFO, NIST Tatiana Laszczak, Exeter Government Services, LLC See Annex A for list of participants

*** Footnotes are added to provide relevant or additional information*

Wednesday, February 11, 2015

Welcome Remarks

Peter Weinberger, Chair, ISPAB
Computer Scientist, Google

The ISPAB Chair, Dr. Peter Weinberger, called the meeting to order at 8:38 A.M. Each Board member provided a brief introduction and also reported on their recent activities since the last meeting in October 2014.

After the Chair introduced and welcomed new member, Daniel Toler, to the Board, Dr. Weinberger introduced the topic with Presidential Policy Directive 28 (PPD28)[1] – Signals Intelligence Activities that was released in January 2014. PPD 28 was a policy, which included information on false surveillance and, as a consequence, the Office of the Director of National Intelligence (ODNI)[2] conducted a feasibility

[1] http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

[2] http://www.dni.gov/index.php/newsroom/press-releases/210-press-releases-2015/1161-national-academy-of-sciences-releases-ppd-28-report-bulk-collection-of-signals-intelligence-technical-options.

study on replacing fault collection by clever software. Dr. Weinberger was a member of the panel, and the panel report was a definitive "no," but it did suggest other alternatives to ensure data is handled correctly.

Mr. Edward Roback, U.S. Department of the Treasury, reported that the agency's budget for this fiscal year and several initiatives were approved. The budget has been allocated to improve analytics for prevention of data leakage and for Standard Occupational Classification (SOC), and to improve security at US Treasury headquarters. Currently, the agency has 23 people assigned and is working to fill an additional 17 vacancies. Mr. Roback requested the Board to encourage interested parties to apply for these positions.

Mr. Danny Toler, U.S. Department of Homeland Security (DHS), echoed Mr. Roback's comments regarding numerous openings. His group is not necessarily planning to change many of the programs, but looking to accelerate and to expand into untapped areas of cyber activities.

Mr. Greg Garcia, Financial Services Sector Coordinating Council (FSSCC) mentioned that in the last few months, there has been a large amount of activities within the finance sector. FSSCC has formulated a new set of initiatives and priorities. The initiatives and priorities include a new series of cyber exercises, in partnership with the government, including the US Treasury, the White House, DHS, law enforcement, and the intelligence community. In addition, a threat-sharing analysis, launched in December 2014 and based on the Structured Threat Information Expression (STIX) and Transparent Asynchronous Transmitter and Receiver Interface (TAXII), included over 100 financial institutions with machine-to-machine sharing as the primary objective. Mr. Garcia mentioned that the Sony breach has provided much food for thought, one of which was examining areas of responsibility and the scope of the response, and to extrapolate lessons learned across the financial sector.

According to the ISPAB Charter, the Board should have twelve members and a Chair. Dr. Weinberger asked for suggestions to fill the remaining three positions.

NSS Update

J. Michael Daniel, Special Assistant to the President and Cybersecurity Coordinator
National Security Staff, The White House

Mr. Daniel emphasized the importance of the White House – Summit on Cybersecurity and Consumer Protection,[3] February 13, 2015, at Stanford University, California. It is anticipated that the White House will release an Executive Order – Improving Critical Infrastructure[4] to address cyber security in the twenty-first century.

Mr. Daniel and his NSS colleagues intend to highlight effort to improve our cyber defenses in the private sector, infrastructure, and government. The four areas of focus are:

- How can we improve our capability to respond to cyber threats?
- How can we build and implement cyber threat solutions?
- How to do so in the international context and how to enhance international cooperation?

[3] http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit

[4] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

- How can we accomplish these steps while keeping an eye on the future?

The strategy is aimed solely at defense is *not* a "winning" strategy and detailed an array of activities in each of those four focuses mentioned above. He stressed that no one particular entity, either outside or within the government, can do the job alone. The key for next several years, he said, is crafting the nature of the partnership.

There is an ongoing effort to partner with the financial services industry at a much deeper level, but as of now, it is unclear as to the precise nature of the partnership. He did, however, acknowledge that the effort will not follow the standard regulatory model, but will require a change in culture – both within and outside the government. For that reason, he eagerly anticipated outcomes from the Summit as well as major announcements on federal security that follows.

In response to the Board's question on legislation to begin to support the activities presented above, Mr. Daniel acknowledged the importance for legislation. NSS recently put forward a package addressing information-sharing, data breaches, normalization, and provisions for law enforcement modernization. All of these elements are critical to getting the job done. These measures are intended as a *foundation*. The NSS looks forward to working with the current Congress and Mr. Daniel is optimistic about building on the momentum generated in the last Congress.

The Board stressed the difficulty of building on these four initiatives; however, acknowledged the progress made by speaker and his group, particularly in partnering with the financial sector, and in the increasing sophistication of awareness between the parties. The Board enquired on how to manage sourcing and diplomacy, specifically with China, to strengthen US banking industry. Mr. Daniel acknowledged the sensitivity regarding cyber and diplomatic perspectives associated with US relationship with China and Europe.

Mr. Daniel responded that many of the rules initiated by China do not further cyber security. He acknowledged that, while China has an interest in improving cybersecurity as much as we do, the country's policies have complicated every aspect of regulation and anti-competitive – in some cases, allowing back doors in their to software. Our objective, he said, is to work alongside China, recognizing their and our concerns for cyber security, but without having adverse impacts on US industry. From the administration's part, we've actively fought back against those provisions with an appropriations bill because simple geographic restrictions are not useful for improving cyber security. Mr. Daniel suggested that there is a need for further dialog, raised with the Chinese government.

The Board noted that the White House has been emphatic on cyber defense, and would like to know how the administration manages the tension in the case of law enforcement. Mr. Daniel responded that the President did address this area and he advocates the need for strong encryption. NSS clearly recognizes the need strong encryption while also to enable people to carry out a multiplicity of online financial, social, and research transactions. Simultaneously, acknowledging that "bad guys" also have this technology, and from the perspective of law enforcement if they continue with impunity, it is a real problem for *any* society. The solution involves a synthesis of technology and policy, which fosters a dialogue with academia and encourages other creative thinking about crafting and implementing policies. At the same time, we do recognize that we are living in a global market and tension exists when addressing the impact of cyber-crime while facilitating business activity.

In response to the Board's query on staffing and leadership, Mr. Daniel stated that the NSS envisions assignees from different agencies to comprise a staff of 50 with the President providing specifics on implementation. Over the last year, gaps were identified when addressing cyber security threats and any organizations should address those gaps, and this would enable government and industry to better

coordinate their efforts. To achieve this goal, NSS staff is putting together a team consisting of permanent members and others, on a rotating basis, with requisite industry knowledge.

The NSS had previously learned a lot from the Heartbleed Bug and the Bash Software bug. When the JASBUG patch[5] was released on February 10, they were able to improve and prepare promptly for the patch deployment. DHS and Office of Management and Budget (OMB) have been doing a good job in managing the process and that the challenge is a configuration in the code entailing several steps. In order to ensure that action is taken by the multiple agencies affected is implemented correctly, US CERT is offering as-needed technical assistance.

On the topic regarding the role of law enforcement and international cyber-crime, many types of crimes that are perceived as local but are now international in scope. For example, a local cyber-crime committed against a French citizen using email could instantaneously become international in scope. A key question is how to increase level of cooperation between law enforcement agencies and how to facilitate prosecution of cyber-crime. There is continuing effort to modernize the legal assistance treaty capabilities through U.S. Department of Justice including an effort to determine the "rules of the road" concerning international cooperation. For instance, if a cyber-crime emanates from one area, the governing entity in that area has the responsibility to alert other areas that might potentially be affected by the attack.

On whether the effort is country-to-country or an international organization is playing a pivotal role, Mr. Daniel described an example of the Budapest Convention as an emergent organization designed to formalize a body of laws confronting cyber-crime which should be implemented internationally. The task is envisioned as a long-term effort, since even efforts to coordinate among nations adhering to British common law has proven to be challenging.

The Board asked Mr. Daniel to comment on the twin challenges of gathering resources and coordinating efforts, citing the DHS Science and Technology Division as proactively working with the financial sector to help prioritize allocation needs, but that coordination remains a key challenge. Considering recent budget restrictions, Mr. Daniel stated that NSS has invested $50 million dollars to address cybersecurity and $30 to $40 million on cyber education. Furthermore, the Vice President recently announced monetary support to universities to foster consortiums to address issues related to cyber-crime.

Mr. Greg Garcia noted the successful deployment of the Structured Threat Information eXpression (STIX) and the Trusted Automated eXchange of Indicator Information (TAXII)[6], but he was interested to know about successful deployment across the Federal enterprise and how these efforts interconnect with the private sector. Mr. Daniel reported on the plan to expand these efforts and capabilities across the public sector. The President has tasked DHS as the portal from which to deploy across government agencies. The challenge now is implementing the process. It is similar to a "weather map" for cyberspace in which data, gathered from a large array of sensors, can help eliminate the "noise" in which cyber-criminals hide. Mr. Daniel acknowledged the need for mandatory standards and especially with the advances in the private and government sectors. It is necessary to craft an evolving set of best practices. Michael Daniel said that the expectation that everyone will be able to be his or her own mechanic is not a feasible strategy or sustainable.

---

[5] http://www.scmagazine.com/microsoft-addressed-56-bugs-issues-fix-for-jasbug/article/397477/;

[6] https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

The Board questioned the feasibility of best practices in a quickly changing environment and suggested that major software supplies be especially scrutinized regarding their adherence to company-specific best practices. Mr. Daniel reasoned that the larger companies have greater resources to apply to best practices compared to smaller companies, which may struggle with sustainability.

The Board opined that addressing cyber-crime by deploying an increasing number of anti-virus software packages may not be effective as implementing changes in operating systems. Mr. Daniel remarked that the cyber-security ecosystem is complex, and more research, analysis and testing are needed to understand how to identify and address points of failures.

Continuous Diagnostic and Mitigation (CDM)

Grant Schneider, Federal Cybersecurity Advisor, Office of Management and Budget (OMB)

Mr. Schneider began with a brief background about himself. For the past four months he has worked within the OMB and, for the past seven years, has been assigned to the Defense Intelligence Agency (DIA) as the Deputy Director of Information Management and Chief Information Officer (CIO).[7]

CDM[8] program is his main topic of focus, and it directly influences our defense as well as our ability to recover and understand, in real time, the nature of a cyber-attack or threat. Mr. Schneider described the program as government-wide and focused on federal unclassified <dot>.com or <dot>.gov[9] websites. At present, CDM is not intended to deploy to the US Department of Defense (DOD) or to the National Intelligence Council[10] (NIC) that was implemented by the DHS and funded by the OMB. CDM is the first program of its kind to provide control at the central DHS-level and at the agency-specific level.

The CDM[11] program follows a 3-phase deployment:

- Phase 1 facilitates real-time situational awareness regarding the state of a network. Specifically, what devices comprise the network, its boundaries and configuration level, patch levels, and what has entered the network. Mr. Schneider said that without CDM, a case such as JASBUG makes it difficult to know when a monitoring task has been completed because the start- and end-points are not supported by a stable and verifiable baseline.
- Phase 2 is designed to assess the activity performed *by* people on a network.
- Phase 3 is about your ability to directly protect and directly respond to cyber security events. When events are observed, CDM provides the option of blocking or attacking the threat.

CDM is controlled at two dashboard levels: centrally, from DHS, and at the agency-specific level.

---

[7] http://www.dia.mil/Portals/27/Documents/About/2012-2017-DIA-DS-Strategic-Plan.pdf

[8] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

[9] http://www.nextgov.com/cybersecurity/2015/02/white-house-debuts-dot-gov-cyber-enforcement-squad/104313/

[10] http://www.dni.gov/index.php/about/organization/national-intelligence-council-who-we-are

[11] http://www.dhs.gov/cdm; https://www.us-cert.gov/cdm

In describing CDM's capabilities, Mr. Schneider also noted what CDM is *not* – an entity that mandates centrally-controlled guidelines at the agency-level, in which DHS directs an agency to take specific actions on the agency-specific network or on its personnel. Instead, CDM is designed to provide *advice* on what is required to mitigate or patch vulnerability and to evaluate overall risk. The advice might take the form of recommending upgraded security training, based on monitored human behavior on an agency's network.

Mr. Schneider illustrated by citing a pre-CDM scenario. When he first came to DIA, the use of thumb drives was not yet prohibited – providing a channel through which a virus could enter a network. If CDM were implemented *at that time*, a virus residing on a thumb drive would not have propagated on a network because CDM disables all auto .ini transactions. The program would also have alerted the agency of its vulnerability due to poor compliance among its personnel.

To streamline funding issues, DHS enters into blanket purchase agreements (BPA),[12] on behalf of requesting agencies for CDM licenses. CDM also provides a wide range of measurable, data reporting criteria and is deployed in three phases.

Under Phase 1, BPA has been implemented between DHS and the Transportation Safety Administration. Overall, CDM purchased approximately 1.7 million licenses for distribution across the federal government. Recipients are prioritized by groups (A through F) listed below. In total, Groups A through F consist of over 60 federal agencies:

- Group A (test) submitted to the DHS.
- Group B (integration) is slated for deployment in the second quarter of Fiscal Year (FY) 2015 and includes the White House, the Veterans Administration, the Office of Personnel Management (OPM), the Department of Energy, the Department of the Interior, and the United States Department of Agriculture.
- Groups C through E are out for solicitation or are in the proposal stage.
- Group F comprises small agencies for which requirements are being developed.

As part of Phase 2, DHS is holding conversations regarding CDM deployment in private industry, with expected deployment slated for FY 2016.

Finally, Phase 3 consists of requirements-gathering, due to complete in FY 2017.

In response to Board's question as to how CDM is linked with the insider threat program, Mr. Schneider stressed that CDM encompasses network infrastructure *and* people, but that CDM is not designed to address this area specifically and that insider threats are addressed by Information Security Continuous Monitoring at the state and local level. In other words, CDM is not designed to monitor if an individual overloads his/her workstation, but will detect threats from outside.

Regarding the CLOUD and the latest on configuration data for external providers serving multiple agencies, it is a service performed by external providers on behalf of the agency. As the agency acquires those services, they would be included in the contract with the individual cloud service provider.

The Board noted that cloud service providers are much more efficient reporting threats than most government agencies. Assuming that the BPA process was good at assessing these third-parties, the Board queried on whether the third-party agency providing tools to agencies are Cloud service

[12] http://www.dhs.gov/cdm-benefits; http://www.gsa.gov/portal/content/176671

providers. Mr. Schneider responded that there are additional integrators to ensure that tools are being used properly. CDM is set up to share information across agencies, providing a critical tool for all federal agencies. CDM will facilitate faster network performance and enhance security.

Updates on Executive Order (EO) Cybersecurity Framework[13] and Legislative Action

Adam Sedgewick, Senior Information Technology Policy Advisor, NIST
Matthew Barrett, Program Manager, NIST

Mr. Barrett introduced himself and began by thanking the Board for its advice. Mr. Barrett is a Senior Policy Advisor at NIST and is currently phasing-in as Program Manager for Cyber Security Framework to replace Kevin Stine, who will fulfill broader duties in computer security.

He proceeded to recount cyber security activities at NIST since last presentation to the Board in October 2014, as well as presented key areas of upcoming projects. He again thanked the Board for providing much-appreciated advice.

Since last October, NIST published a Request for Information (RFI),[14] which generated 245 responses to help NIST formulate a framework. The nature of the RFI solicited information about user awareness, experience, and attitudes concerning the roadmap. A second RFI generated approximately 57 responses, many of which reflected considerable backgrounds in IT and energy. The RFI also generated responses from academia, the product sector, service providers, auditors, and government representatives at the state level.

An overarching theme derived from the RFIs indicated an ongoing effort to understand the nature of the framework. As a result of conversing with respondents, NIST stabilized the framework, delaying an upgrade to version 2, focusing, in the interim, on facilitating an understanding of the existing cyber security framework. Mr. Adam Sedgewick added that it was not a matter of respondents having to learn the framework on their own, but helping them by sector guidance and supporting tools provided by NIST.

Mr. Barrett then discussed the 6th Cybersecurity Framework Workshop[15] located at Florida Center for Cybersecurity (FC2), University of South Florida, Tampa, Florida, which was the last workshop conducted nationwide. This workshop fostered an increased awareness of the cyber network framework. The last panel included several UK presentations, one of which was a keynote address.[16] An additional panel included policy-makers from the European Union (EU), the United Kingdom, and the state government of Rhode Island. Members were also brought in from the U.S. Patent and Trademark Office, and state regulators.

All of these six workshops, each deployed in a unique location, had provided NIST with a wide range of responses from industry audiences. In the aggregate, these six workshops drew a total of 435 registrants

[13] http://www.nist.gov/cyberframework/

[14] http://www.nist.gov/cyberframework/cybersecurity-framework-rfi.cfm

[15] http://www.nist.gov/cyberframework/6th-cybersecurity-framework-workshop-october-29-30-2014.cfm

[16] http://www.nist.gov/cyberframework/upload/6th-workshop_agenda.pdf

representing over 300 organizations. The workshops generated a number of panels comprised of members from the US as well as from the United Kingdom and representatives from several Asian countries. A status update on the RFI followed.

Mr. Barrett has been working on improving the web presence of NIST's cyber security framework that also lists 42 frequently-asked questions. In addition, he is working on developing a Resources page and a page dedicated to Upcoming Events including webinars.

Mr. Sedgewick said that in December 2014, several pieces of legislation passed,[17] two or three specifically impact NIST, including the Federal Information Security Management Act (FISMA) Reform Bill.[18] . More specific to the topic under discussion was the Cyber Security Enhancement Act,[19] containing a segment focusing specifically on the Cybersecurity Framework, as well as research and development priorities. The Act codifies NIST's responsibilities, pursuant to the EO, to develop the Cybersecurity Framework, and provides for work outside the federal government environment. NIST is also tasked with identifying and rectifying the duplication of processes and will work alongside non-regulatory agencies to achieve that goal. The FISMA update requires a Government Accountability Office (GAO)[20] [21] to report on activities over the next six years in two-year increments.

Last week, NIST was invited to a Senate hearing to address activity specific to the Cybersecurity Framework. The senators were especially interested to know how that effort is measured, and Adam Sedgewick's response was that metrics would not reflect *how* entities use the framework

It is encouraging to confirm that NIST did *not* receive overwhelming demand that the framework be rejected, but instead was queried on *how* the Framework is to be implemented. It was suggested that NIST could draw on the experience of other agencies that deployed and implemented security protocols and tools in a similar manner, and by querying respondents regarding how implementation will be launched once on site and how quantitative and qualitative data will be captured.

NIST's focus is on outreach and support, and on understanding and implementing the Framework. At present, NIST will only release output after receiving more input generated from an extensive questionnaire. NIST does not plan to conduct a survey, but will focus attention on examining the requirements as stated in the EO. Another effort is to determine how the Framework functions alongside other federally-mandated methodologies such as FISMA requirements. Simultaneously, NIST will maintain ongoing dialog with industry.

On the international front, the EU published a summary of a NIST workshop conducted in November 2014. The NIST directive was announced at the same time as the EO. The EU invited NIST to attend a meeting to discuss information-sharing, ongoing work, and how to share best practices. In January 2015,

---

[17] http://www.nextgov.com/cio-briefing/2014/12/fitara-fisma-reform-5-key-tech-bills-passed-congress-2014/101916/

[18] https://www.congress.gov/bill/113th-congress/senate-bill/2521

[19] http://www.gpo.gov/fdsys/pkg/BILLS-113s1353es/pdf/BILLS-113s1353es.pdf (4th version passed in December 2014)

[20] http://www.gao.gov/assets/670/665246.pdf

[21] http://www.natlawreview.com/article/fisma-updated-and-modernized-federal-information-security-management-act

NIST representatives traveled to China as part of the US/China legal exchange. Privacy sessions were addressed in the last workshop. NIST received some feedback regarding where the Framework might be deployed in the future.

On responding to the Board's question as to how legislation affects NIST, Mr. Sedgewick said that NIST receives guidance from the OMB on how the latter agency reports to Congress. As to any impact from a regulatory review of the Enhancement Act, Mr. Sedgewick responded that, from the beginning of the effort, NIST has invited input from federal and state regulators and has received feedback consistent with feedback provided in at the Sixth Cybersecurity Framework Workshop in Tampa, October 29-30, 2014. He closed by stressing the need to reach out to regulators and to broaden regulatory technological operations where policy differences can be reconciled.

Overview of 18F – Digital Services Delivery, GSA[22]

Greg Godbout[23], Presidential Innovation Fellow, Executive Director, 18F and GSA Deputy Associate Administrator
Andrew McMahon, Senior Advisor to the Administrator, GSA

Mr. McMahon began the discussion with a question: What were some of the challenges encountered in the IT community? The question reflected three main challenges that 18F is focusing.

The first challenge concerned building the core capacity on "how-to-build" innovative technology in the federal government. The US government did not have the technical expertise to build things in-house and occasionally did not know what was being built by the vendor community when the government did procure those items.

The second challenge concerned addressing the "pre-18F" fragmented and complex service delivery architecture. For example, a citizen needed to better understand the bureaucracy of the government in order to understand where he or she can obtain services from the government. Though the problem still exists, it is something actively confronted by 18F.

In short, the third challenge affected the procurement cycle in that it did not keep pace with the technology cycle. It was often the case that when the procurement cycle began, the technology was out-of-date by the time procurement was completed. Initially, the 18F team thought of addressing the problem by tackling two big issues: the first of which was a simple sign-on and the second, electronic forms.

Mr. McMahon described how a conversation that started the 18F program. The initial concept behind the program was to allow talented people to build teams to decide how to address problems, and to work within a government environment, allowing the market or specific agencies to decide for themselves, rather than relying on the General Services Administration (GSA) to dictate policy. The result at the end of many extensive conversations looks very different from what was originally considered.

---

[22] https://18f.gsa.gov/

[23] Greg Godbout will transfer to another government agency in early April
http://www.executivegov.com/2015/03/greg-godbout-to-leave-18f-executive-director-post-at-gsa/

At its core, 18F is a production floor inside government. It will do much more than produce new technology. It will also help agencies to conduct more effective Development and Operations (DevOps) as well as improve and streamline security-related efforts.

18F's mission is to transform the way the government builds and buys IT services and products. The strategy evolved from the UK's Global Distribution System model, stressing *delivery* as the strategy. The focus is not want to spend a lot of time at the outset by discussing how things were going to be done, but to focus on using several methodologies such as User Center Design, and Agile, resulting in a user-friendly (even enjoyable) exercise, while at the same time ensuring its security.

18F was launched in January 2014, and last year's effort was directed toward building a production floor for the following reason. In order to deliver a digital service to an individual in the government or private sector, it is essentially touches all processes integral to the project as a whole. Using Agile as an example, Mr. Godbout described a case in which the application (Agile) is delivered to an organization's office tasked with implementing it organization-wide. Predictably, the result would be less than efficient.

With the production floor model in place, next focus is building the team. The time needed to have a government employee in place averaged six to nine months (an untenable burden nowadays), has been reduced to six to eight weeks. Mr Godbout credited personnel in Human Resource (HR) who worked with 18F in adapting the DevOps model to facilitate the hiring process. In some cases, HR hiring rate outstripped that of 18F. 18F has received requests for services from numerous individuals and organizations. 18F has an office in Silicon Valley, which competes with all other organizations located in the region.

Addressing the issue of hiring, Mr. Godbout suggested starting with culture in mind and use the most effective business processes to achieve success. As practiced in GSA, the Federal government can compete with other organizations by using the team in the selection process.

The Board asked if the process can be implemented by OPM, and Mr. Godbout responded that they often have direct hiring authority, using Operation A – a business process-through-engineering methodology similar to Agile. It is 18F practice aims to hire civil servants for a period averaging from two to four years.

With regards to the security clearance level for a new hire, every civil servant new hire is interviewed by the Federal Bureau of Investigation (FBI). In some cases that require higher-level clearances, the hiring process could take longer, but applying for a higher-level clearance can still work in the building under authorized supervision. Regardless of the level of clearance, it is important to brief employees about the nature of the process, the status of their own case, and the need for clearance in the first place.

The DevOps model used with a signed Authority to Operate (ATO) to help streamline a process is normally required 18 months to complete. Taking into consideration the amount of documentation required by the ATO, our DevOps model ensures rapid, yet secure, pre-hire vetting.

One of major challenges is scaling the hiring process to meet demand. Mr. Godbout stated that they hire on demand, enabling them to scale and transform. At the same time, and to ensure security, they implement privacy by design, using Agile methodology in managing risk and using the tools provided. They recognize, however, that tools are not synonymous with security. They learn by constantly monitoring and testing agency processes.

The Board was very curious about what 18F has learned about acquisition especially acquisitions and Agile typically do not reside together. Andrew McMahon illustrated that when people are inexperience

about acquisition they tend to make poor decisions. The government is the integrator, but risk management was often outsourced, encouraging passing on the responsibility for questionable decisions. Now, however, responsibility is a by-product of agile methodology.[24]

The subject of oversubscription is currently under discussion between GSA and their partners in DHS. 18F can be compared to a staff of coaches assisting agencies to act independently. They are willing to work with any agency to determine the viability of a project and whether or not it fits the skillset of its present or future staff. Though agency-specific cultures vary, GSA is well positioned to help streamline the decision-making process.

On whether the focus is to save money or just showing people how to adopt methodologies and best practices, the position is to learn to do more with less, employing tried-and-true methodologies before purchase. Ideally, they would like to see these methodologies adopted through the entire federal government.

FAA Unmanned Aircraft Systems Update (PPT presentation provided)

Stephen (Steve) George, Manager, Airworthiness, FAA

Mr. George described his role as manager of the Airworthiness and Engineering in the Unmanned Integration Office within the Federal Aviation Administration (FAA). The office has fifty people, and there are fifteen engineers in Mr. George's group that work on a broad range of projects on unmanned systems, including design and construction, the basic relationship between the pilot and the flight crew interface, the C2 (Command and Communications) or C3 (Command, Communications, and Control).

The group is developing standards for the detection avoidance equipment, standards for the radio protocols and the radio design requirements through a federal advisory panel that provides advice to the FAA related to performance standards. The group also works closely with other government agencies including DHS, DOD (the world's biggest user of unmanned aircraft), interfacing with the National Telecommunications and Information Administrative (NTIA) and civil aviation authorities worldwide who, like the FAA, face the challenges inherent in integration.

In addition, there is an operational component concerned with pilot certification and requirements, the issuance of approval using the Certificate of Authorization (COA) process. Mr. George defined COA as a certificate of authorization or a waiver to obtain air traffic approval to deploy an unmanned in the airspace. The waiver is issued by FAA's Air Traffic Organization[25] (ATO) that works closely with Mr. George's office to form together a microcosm of the FAA itself. The ATO is concerned with clearances and separation between aircraft, while Mr. George's office manages safety, including that of the aircraft, pilot, operation location.

One of the challenges facing his office is the wide size range of unmanned aircraft – from hand-held to those the size of a 737 (the Global Hawk). His task is to match approval to risk. He is in the process of promoting a safety continuum, which lets them look at the risk of the aircraft in its operational environment, for tasks not implemented.

As an example, he cited a scenario where one is not informed that an airplane normally can fly over New York during daylight hours. In the past, once design and operational approval was granted, other risks

[24] http://agilemethodology.org/

[25] http://www.faa.gov/about/office_org/headquarters_offices/ato/

were no longer considered. Design and operational approval in a risk-based approach are now jointly considered.

The broad spectrum of unmanned aircraft poses a significant challenge. FAA does not want to be accused of over-regulating the smaller Unmanned Aircraft Systems (UAS)s, thus inhibiting a market for them, and which, by and large, are considered safe. But the same risk criteria cannot apply to craft as large as the 30,000-pound Global Hawk. A new set of guidelines (Part 107,[26] published on February 13) defines and formulates requirements for small unmanned aircraft weighing less than 55 pounds.

FAA does not to impose undue risk to people or property on the ground, or to other users of the airspace. As to how to characterize a small UAS as "probably safe, it all depends on who you talk to in describing a small UAS as "safe." As an engineer, Steve George considers the worst-case scenario. If a large, heavy UAS is to fail, its impact to people and property would be catastrophic.

FAA's primary objective is safety, and efficiency and continuity of service are critical component as well. Levels of severity range from Catastrophic (loss of life), Hazardous (injuries, or increased workload on pilots and controllers), Major (requiring diversion to some other mode of operation), and Minor (posing minimal safety concerns). There is provision for allowed levels of probabilities for each of those criteria. On the discussion of privacy risks, it is covered by other government agencies and FAA's charter does not authorize to deal with privacy issues. Once FAA received permission to proceed, FAA does not anticipate any possible intervention by any other agency concerning privacy issues on FAA responsibilities.

On certain scenarios, there are possible conflicts between safety and security concerns. Security has been mostly concerned with modular integrated avionics systems because that poses the greatest threat in an area. Someone gaining control of the avionics systems can control the flight path of the aircraft. For the past five years, the FAA has a dedicated team based in Seattle, with a dedicated chief scientist focusing primarily on these issues. Security has become more important as technology evolves from analog instruments like barometric pressure indicators connected directly to an air system, air data computers are providing information to the avionics, and faulty or compromised information can cause catastrophic results. The focus is to prevent unauthorized access to those systems.

The issue has traditionally been addressed in our industry standard, the ARINC 429[27] Data bus, which is not addressable as is a Transmission Control Protocol/Internet Protocol (TCPIP) or public network. Instead, it is a closed, proprietary system unique to aviation. The concern would be to prevent someone from gaining access to a closed system, which might be in the form of loadable databases which modifies databases, or operational programs. FAA has stringent restrictions on who can access and/or modify those systems.

When discussing security, it is important to consider:

- Protect occupants (not relevant re UAS)
- Enhancing public safety (relevant for manned and UAS)

---

[26] http://www.faa.gov/regulations_policies/rulemaking/recently_published/media/2120-AJ60_NPRM_2-15-2015_joint_signature.pdf; https://www.federalregister.gov/articles/2015/02/23/2015-03544/operation-and-certification-of-small-unmanned-aircraft-systems

[27] http://en.wikipedia.org/wiki/ARINC_429

- Protect critical infrastructure / preventing unauthorized control of the aircraft?
- Protect the economy. Since aviation is a huge segment of the economy, lack of safety could deter public confidence in using this form of communication.
- Protect system architecture
- Protect the aircraft and the mode of control

FAA is tasked with protecting the points of the National Airspace System (NAS), which includes:

- The aircraft and the critical infrastructure required to keep the system moving
- Surveillance network capabilities (nationwide system of radar systems)
- Communications system to relay information to the aircraft controller
- VHF communications between pilot and controller
- Navigation infrastructure (space-based and terrestrial)
- Security of communication network worldwide

The difference between UAS and hobbyist devices is that UAS carries a payload for commercial or military purposes which is intended for delivery or deployment. Until recently, the FAA defined four categories of security: (1) Network security, which, on traditional aircraft, is mandated by Area 429, but, in UAS, is still undetermined. The latter poses a significant challenge for the FAA, (2) Information Security, (3) Systems security, and (4) Cyber security.

As stated in the published Federal Register notice, the FAA has tasked the Aviation Rulemaking Advisory Committee (ARAC) to provide recommendations regarding aircraft systems information security and protection (ASISP) policy, plus guidance on best practices for airplanes and rotorcraft, covering “both certification and continued airworthiness”. The FAA is working to standardize “security” with the ASISP for aircraft-wide application with particular focus to UAS.

Generally for manned and unmanned systems, the element of reporting aircraft position to the ground is necessary, and real time reporting is critical with manned aircraft. Currently, FAA has position reporting on all aircraft in certain areas of airspace, differentiated by class (A, B, or C). Class A is airspace above 18,000 feet. Class B is airspace around large metropolitan areas (New York, DC, Chicago, etc.). Class C is more regional (Richmond, etc.). In Class D and Class E airspace, no one is required to report their position. Though it is mandated to equip all traditional aircraft with transponders, FAA has yet to set requirements with UAS. If UAS is flying at 500 feet, it would cause frequency congestion and radar interference would add to the information sent to air traffic controllers. It would also complicate UAS navigation itself. For these and other reasons, the issue of position reporting on UAS is still under discussion.

Currently, FAA has implemented regulatory policies, orders, and guidance for non-government services, aircraft systems, and aircraft operations. The FAA is also developing an Airborne Radio Standard. The Radio Technical Commission for Aeronautics, a federal advisory committee, is publishing minimum performance standards for radios deployed on the control stations and on aircraft.

One area not yet addressed: On traditional aircraft as well as on UAS, the pilot communicates with the controller by UHF radio. The radio and antenna are on the airplane.

This may not be the solution for UAS. If the pilot is *already* on the ground, why not put them in a secure terrestrial network, which would not interfere with air traffic control? Resolving these issues must take into consideration standards which allocate radio bandwidth and voice communications. Security issues are being developed in the form of the Command Non-Payload Communications which controls the trajectory of the aircraft in the airspace.

Another challenge is implementing security precautions while keeping pace with rapidly-evolving hardware/software development. This requires the systems engineering remain closely tied to systems development. While the FAA is sometimes criticized as the "tombstone" agency, FAA does try to keep pace by anticipating future challenges. Technological changes in avionics are often slow-paced although slower pace is critical in a safety-conscious organization.

National Security Agency Civil Liberties and Privacy Office[28]

Rebecca J. Richards, Director, Civil Liberties and Privacy Office, NSA

Ms. Rebecca Richards began work with the NSA a little over a year ago. Previously, she worked with DHS for almost ten years. Ms. Richards described the major components of the office of NSA Civil Liberties and Privacy, which began with defining and implementing its goals.[29] Ms. Richards described it as "the science of privacy in support of the art of privacy." One of the first things was to learn the landscape in which NSA functions and how things have changed at NSA for the past 10 to 20 years on threats, technology, and most importantly, NSA's perspectives on civil liberties and privacy. These focus areas have given NSA an opportunity to look "inside the building" and "outside the building," to better adjust to the current IT ecosystem.

One of the biggest adjustments is that NSA is traditionally not been open to talking about its operations. Ms. Richards, however, was hired to "*talk*" about the agency; and, therefore, is a bit of a rarity in the building. The NSA Civil Liberties and Privacy office has a big job to tell the story of how NSA is including value to the country (our abilities, etc.). In the 80s, the focus was clear. In today's world, there are threats to every individual, whose information travels across the internet that all of us use. People have a heightened view of the role of civil liberties.

Ms. Richards is the primary advisor to the Director of the NSA, and she is responsible for implementing his recommendations. It is her goal to help build meaningful privacy and civil liberties processes to achieve a holistic and systematic approach across the organization. She hopes to do this by tackling how her office can improve existing civil liberties and privacies protections and enhance transparency in a meaningful and appropriate way. Although her office has responded to Freedom of Information Act (FOIA) requests, that process alone does not enhance public contact.

The culture at NSA was one of the first things that impressed Rebecca Richards. The organization is very compliant and staffed, in large part, by engineers and mathematicians. When mistakes are made, everyone at NSA is encouraged to recognize, learn, and move forward. NSA is a microcosm of the battlefield in the outside world.

Ms. Richards' office has examined types of data and how to manage and use it in order to calculate a privacy risk. In doing so, it helps them to understand areas where they have more or fewer privacy risks.

---

[28] https://www.nsa.gov/civil_liberties/index.shtml

[29] https://www.nsa.gov/civil_liberties/about_us/

The challenge is to protect civil liberties while protecting privacy. When you're protecting an individual's First Amendment rights, it must be based upon the data related to that individual. Since the NSA is primarily concerned with privacy, the task was to establish parameters within the organization. Most importantly, it must be built on an existing compliance and security framework.

In working on a strategic plan, four distinct strategies are identified. As these strategies were being formulated, efforts were made to reach out to others in the NSA as well as to those in the academic sector in order to reality-check our expectations. Some issues, related to the type of information collected, have a chilling effect on privacy risk, and other risks are purely mechanical that support having an intern with a PhD in mathematics.

To date, her office has published two reports[30] that are available publicly on the NSA website. One relates to the existing safeguards surrounding the Foreign Intelligence and Surveillance Act (FISA), Section 702.[31] The other relates to safeguarding existing or targeted Signals Intelligence (SIGINT) activities under EO 12333.[32] A considerable amount of time was spent working on Presidential Directive 128.

NSA has been spending some time evaluating the value and risk of the information NSA receives using a civil liberties and privacy risk assessment process. This was started in the initial ten months Ms. Richards joined NSA. Based on that effort, a usable assessment tool was built that goes beyond simply checking a box to say "yes, we have a privacy assessment process in place." NSA Signals Intelligence staff provided feedback and asked about the differences between high and low privacy risk and how to differentiate. This demonstrated clearly that acting on gut instinct is insufficient. Historically, data is collected and used for foreign intelligence. But to design a more nuanced tool, it is necessary to analyze the information to determine if its value goes beyond foreign intelligence.

The mathematical application is described by examining data types: biographic, biometric, and contextual data. The data, running in a continuum, is tagged (evaluated) according to a specific set of criteria. For example, when going after a foreign intelligence target, privacy considerations are less important than would otherwise be the case. Despite initial misgivings concerning privacy protection, whenever big data is initially gathered, a broad brush is necessary before drilling-down to critically evaluate privacy on a case-by-case basis.

The controversy is usually centered on the argument that it is not the amount of data that is collected, but the use to which it is applied. In analyzing data for risk assessment, *both* the data type and its intended use must be considered.

The NSA Civil Liberties and Privacy office employs six full-time employees, and also enjoys the support from several intern programs. Since their task requires an informed approach to managing SIGINT, a full-time staff member with a background in SIGINT has been assigned. Ms. Richards spends much of her time reaching out to others and NSA general counsel.

Under the Privacy Act, DHS has to review any records in which it collects personal information. The Act also applies to NSA, however since much of their work is classified, that information it is not covered.

---

[30] https://www.nsa.gov/civil_liberties/reports/index.shtml

[31] https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf

[32] https://www.nsa.gov/civil_liberties/_files/nsa_clpo_report_targeted_EO12333.pdf

Simultaneously, the office examined avenues of redress to ensure that bad things do not happen to good people. While the British have a redress model, NSA does not have such a model because of the Privacy and Civil Liberties Oversight Board, which works independently of other federal agencies. The British have no such oversight organization in place.

Ms. Richards affirmed that NSA has an extensive privacy training program, which is focused on an analysis of protection under the Fourth Amendment. The Civil Liberties and Privacy office is preparing new training programs in addition to those that currently exist so as to build this into the fabric of the agency's thought process.

Currently, they are not working directly with the NSA FOIA office but the offices maintain open and frequent conversations about NSA's efforts in this area. The Board should note that the NSA has not really been public with its program for the past 60 years, and Ms. Richard's office has been working for the past 18 months to establish a voice to the public. She cited one example where Al-Qaeda took advantage of surveillance information that had become public and the group was able to develop a video on how to avoid surveillance.

In closing, the Board asked where will civil liberties and privacy protections be in the case of a catastrophic event like World War II or when senior leadership in the Executive branch insists on misbehaving. Ms. Richards responded that policy-makers should include "big thinkers" who consider possible future events and craft protections in anticipation of those events. These are the questions we should be asking as a society and not to shy away from them.

The meeting recessed at 4:20 P.M., Wednesday, February 11, 2015.

Thursday, February 12, 2015

The Chair began the meeting at 8:44 A.M.

NIST Updates (also see Annex C)
Matthew A. Scholl, Chief, Computer Security Division, Information Technology Laboratory, NIST

Mr. Matt Scholl began his updates with reference to recent activities at NIST since the last ISPAB meeting in October 11-13, 2014. Dr. Willy May is still the Acting Director at NIST; however, NIST officials are anticipating the Senate to officially confirm Dr. May as NIST Director soon. In the interim, Dr. May has appointed Dr. Richard R. Cavanagh as Acting Associate Director of Laboratory Programs, NIST, and Mr. Scholl will invite him to come to the next ISPAB meeting in June. Mr. Scholl confirmed that he was officially appointed Chief, Computer Security Division, NIST, on December 28, 2014.

In June 2014, NIST has established a new laboratory, Communications Technology Laboratory,[33] to explore spectrum capabilities around interoperability, co-existence, de-confliction and technologies standards in this research focus. Computer Security Division, NIST, is supporting this laboratory with security standards and guidelines - mainly in the LTE-3GPP[34] (The Mobile Broadband Standard) standards with DHS and public safety communication technologies for the Federal Partnership for Interoperable Communications. NIST is also interested in Global Positioning Systems (GPS) technologies and Mr. Scholl emphasized that this is an emerging area of interest for NIST in security, redundancy and timing issues. NIST will next be focusing on wireless and engineering capabilities in communications technologies.

A few updates including the Cybersecurity Enhancement Act[35] that was passed in December 2014:

- Public Private Partnership – NIST will consistently facilitate and support the development of voluntary consensus space for the standards, best practices, mythologies for processes and procedures to reduce cybersecurity risks and to continue engagement in the Cybersecurity Framework.
- Cybersecurity Research and Development – NIST will continue their efforts with other agencies and the National Science and Technology Council (NSTC) applying their "Checklist of Security Automation". This also captures some of NIST's research and development work with access controls and supply chain control security.
- Education and Workforce Awareness – This is tied to NIST's coordination role in the NICE.
- Cybersecurity on Technical Standards – NIST Director is to coordinate cybersecurity work on the standards development activities within the Federal Government and also coordinate the annual report that is handled by NIST's Standards Coordination.

Federal Information Security Management Act (FISMA) was also recently updated but the changes that would affect NIST are not significant.

---

[33] http://www.nist.gov/ctl/

[34] http://www.3gpp.org/technologies/keywords-acronyms/98-lte

[35] https://www.congress.gov/bill/113th-congress/senate-bill/1353;
https://www.govtrack.us/congress/bills/113/s1353/text

NIST will participate in other coordination roles, working with DHS and OMB on the revisions to OMB's Circular A-130. This circular provides guidance to government operations.

Matt Scholl reported on several workshops including the Sixth Cybersecurity Framework Workshop[36] in Tampa, October 2014, and National Initiative for Cybersecurity Education (NICE) Conference at NIST, November 2014.[37]

NIST has a "grassroots" program available in which entities can submit a proposal based on new technology and NIST will provide the "seed" funding if approved. As an example, NIST used this program to fund two pieces of work in 2014 – Internet of Things (IOT) and Direct Digital Manufacturing. He explained that NIST held a workshop[38] to discuss 3D printing manufacturing on the security and disruptive nature of it; the workshop resulted in an interesting dialog regarding protection and the integrity of the product manufactured. NIST is exploring this further but has not yet seen any threat models. Many concerns are mostly around intellectual property.

There are a few upcoming workshops that cover various focal points: Personal Identity Verification (PIV)[39] Card Downstream Technical Performance Specifications, PIV card standards around the downstream technical performance specs, and Cryptography (quantum and Elliptical Curve) post. A number of draft documents have been released for comments (see Annex C). NIST is seeking comments/feedback to assist in standardizing a process. Matt Scholl assured the Board that the Cybersecurity Threat template provides a way for agencies to share information that is also uniformly shared with the private sector.

NIST is focusing on insider threats, malware, and phishing emails and not on folks with clearances from a grand scheme perspective with cybersecurity threats. NIST will continue to seek feedback from public and private sectors specifically focus on what would be effective on which correct threats received in their organizations. The intent would be for each entity to design/build their own threat model based on their needs.

Mr. Scholl requested the Board to be alert to the discussions of effective cryptography and law enforcement as this conversation grows and the "Going Dark" issue of wrongful use of technology. The government is anticipated to start a public discussion on how cryptography effects law enforcement, and what can be done. Mr. Scholl also informed the Board that NIST has signed on to the World Trade Barrier Treaty and the focus will be to ensure it is compatible with the technology.

NIST has published a Federal Register Notice[40] proposing the withdrawal of six Federal Information Processing Standards (FIPS):

- 181 – Automated Password Generator
- 185 – Escrowed Encryption Standard

---

[36] http://www.nist.gov/cyberframework/6th-cybersecurity-framework-workshop-october-29-30-2014.cfm

[37] http://www.nist.gov/itl/csd/2014-nice-conference-november-5-6-2014.cfm

[38] http://www.nist.gov/itl/csd/upload/cybersecurity_for_dmm_symposium_agenda_020315.pdf

[39] http://www.nist.gov/itl/csd/fips201-2_workshop_2015.cfm

[40] https://www.federalregister.gov/articles/2015/01/16/2015-00657/proposed-withdrawal-of-six-federal-information-processing-standards

- 188 – Standard Security Label for Information Transfer
- 190 – Guideline for the Use of Advanced Authentication Technology Alternatives
- 191 – Guideline for the Analysis of Local Area Network Security
- 196 – Entity Authentication using Public Key Cryptography

The comment period closed on March 2, 2015. The reason for the withdrawal is because "they are obsolete, or have not been updated to adopt current voluntary industry standards, federal specifications, or federal data standards. Federal agencies are responsible for using current voluntary industry standards, as well as current federal specifications and data standards in their acquisition and management activities."[41]

In closing Mr. Scholl highlighted a few of continued or new areas of interest such as IOT funding, big data, Guidelines in Social Media Security and Privacy, Tool focused evaluation with Open Source review, Cryptography Performance Testing, and FIPS 140 testing. NIST has additional funding and evaluating grant programs with universities specifically in the post quantum cryptography arena for NIST recruits. NIST is currently waiting for the grant funding to be finalized.

Presentation on Federal Trade Commission Report on the Internet of Things

Karen Jagielski, Senior Attorney, Division of Privacy and Identity Protection, Federal Trade Commission (FTC)

The Board welcomed Ms. Karen Jagielski from the Federal Trade Commission (FTC) to speak on the FTC report on Internet of Things IOT report, *FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks*[42] released on January 27, 2015, and to discuss the security and privacy risks in this area.

Ms. Jagielski opened her presentation by providing the Board with some background information on how the FTC Act is enforced within her agency. The FTC Act prohibits unfair and/or deceptive acts and practices affecting commerce. FTC's focus is in the commercial arena, mainly interested in commercial transactions. The continued an act is considered deceptive if there is a material misrepresentation or omission likely to mislead consumers acting reasonably. To be unfair, it has to likely cause substantial consumer injury not reasonably avoided by consumers themselves.

The commission does not do any anti-trust. She explained that the commission is setup into three bureaus: Competition, Economics and Consumer Protection. The FTC put together a workshop, *Internet of Things – Privacy and Security in a Connected World*[43], on November 19, 2014, with the focus on privacy and security on consumer facing devices, including devices that either consumers use or are sold. The workshop consisted of four major areas: Connected Home Network/Devices, Health related Devices (such as FitBit technologies), Connected Cars and a broader view of privacy and security in this space. As an output to this workshop, they created a report and recommendations. The report offered huge benefits (referring to a FitBit collecting healthy daily activity to consumers so they can make better physical daily choices) and ambiguous IOT risks to devices.

---

[41] Crypto Updates_2015Feb13.ppt

[42] https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

[43] https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world

Although she emphasized the benefits, she also highlighted the security risks, including:

- Unauthorized access or misuse of information collected or transmitted "by or to" the device.
- Device security vulnerabilities if there is not an adequate level of security that can result in unauthorized information transfer.

The Board asked about when action is taken and where in the insecurity variant does FTC have authority. Ms. Jagielski replied that the FTC's statute provision to pursue companies that have been deceptive or unfair in their practices and were not reasonable to avoid by the consumer. As an example, in the deceptive arena, the device is often misrepresented to consumers "like the system/device is secure and your information is absolutely protected when, in fact, it's not. Or, in omission, your information is secure as long as you do A, B, C, D, etc." The difference is that it is referring to a multitude of devices that are essentially interconnected and communicating with one another and may jeopardize all devices that are connected without adequate security and privacy measures in place.

Two comments of particular interest and clarification were raised. The first thing is to understanding FTC's approach at the workshop. A forum was organized at the workshop to be used as an educational process to start discussions and to identify potential risks. Secondly, FTC particularly focuses on areas where consumers are unfamiliar and not well informed on the IOT and associated privacy and security risks. Ms. Jagielski explained that it was the workshop that started FTC's discussion with interested parties but the research began six to eight months prior to the workshop.

In the IOT report the major risks involved: privacy, GPS location, health, identity, financial information and beyond those mentioned that rich data is being collected and might prove potentially useful. The FTC asked a rhetorical question in "how are they going to deal with that"?

The FTC formulated the recommendations that were major component of the report. The following recommendations can be found on the FTC.gov website:[44]

- Fair Information Practices and Principles (FIPPS) developed in the 70s are no longer applicable.
- Reasonable data security should be a flexible approach in that the business has to review at the nature of the information being collected, stored, or disseminated and evaluate its sensitivity, and consider all the issues/risks.
- From a security by design perspective the business should think of the entire lifecycle of the product.
- Levels of security may differ, what might be reasonable for FitBits may not be reasonable for one's pacemaker.
- Consumers must be given notice if a business stops supporting products…etc.

These recommendations are just suggestions to assist in best practices. The FTC has no authority to mandate these recommendations as a standard. In the case of any violation, which is deceptive or unfair to the consumer, by law the FTC can take action against the violator/company.

Another focus is big data and to use of gathered data is being communicated to the consumer. The report does recommendations specifically on data collection but did not forbid collection. For example,

[44] https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

if you are collecting big data, consumers need to know how the data is used to make decisions concerning every person. People must be given the option to opt in or opt out. An FTC privacy report was released in 2012, stating that not every use of data requires notice of choice. Recommendations outlined by the FTC are as follows:

- Choice of point of sale – when consumers purchase a product they need to be made aware of collection process and data collected.
- Choices during setup – setup Fitbit, connect to Facebook, Twitter, email – provide the consumer the choice of who or what application can have access to their data.
- Management portals or dashboards – iphone applications (apps) –consumers decide on which dashboards can collect information like GPS location.
- Lastly, out of beam technology – what is out of range for the consumer?

Consumer surveys indicate this is the correct outlook based on the feedback. However, manufacturers must validate the consumers' needs in order to address the device's usability. FTC has an education program that will help to educate consumers without challenging them on design of the device.

Presentation on Breaches and Breach Reporting (PPT presentation provided)

William Wright, Director, Cybersecurity Partnerships, Symantec Corporation

Mr. William Wright has been the Director of Cybersecurity Partnerships at Symantec for past two years. Symantec is the largest security software company in the world with ten security response centers located worldwide that process billions of email and web requests sent to fourteen global data centers. Symantec Global Intelligence Network is made up of millions of sensors to capture security threat data worldwide.

Recent headlines have focused on high-profile data breaches involving the theft of Personally Identifiable Information (PII). These breaches have impacted Michaels, Home Depot, Target Corporation, Niemen Marcus, JP Morgan Chase, the state of South Carolina, and, most recently, Sony Corporation, and the release of over 200 celebrity photographs posted on social media that drew the attention of lawmakers. According to Symantec's most recent internet security threat report,[45] over 500 million identities worldwide were exposed in 2013. Symantec is in the process of compiling their 2014 statistics and will publish its report in March 2015. Within the last two years (2013 and 2014) there have been over 1 billion identity thefts worldwide. Mr. Wright stated that it would be difficult for many reasons to know, from a policy perspective, the number of identity thefts by country. This is partly because most breaches are not even reported.

While the focus has been on data breaches, it is important not to lose sight of a other types of cybercrime, among which are the IOT, and modalities quickly accelerating from personal computers, phones, mobile tabletware, spam, and phishing. Clearly, for cyber criminals, new technology presents new opportunity. Most people assume that breaches are implemented from sophisticated malware or from well-resourced state-sponsors, but the reality is much more troubling. According to a very recent report from the Online Trust Alliance, 90% of breaches launched in 2014 could have been prevented if organizations implemented basic cybersecurity risk measures.

[45] http://www.symantec.com/security_response/publications/threatreport.jsp

Today, Mr. Wright covered the current threat landscape: the nature of breaches, how breaches occur, security measures to protect against data breaches, and key elements needed to inform data breach policies and legislation. Attackers run the gamut from highly-organized criminal gangs, individual cyber criminals (hackers), and state-sponsored groups. Criminals try to sell their product and their expertise to other criminals. Nation-states often pose as activists, acting in the interest of their home country. Therefore, it is difficult to determine who is behind a specific attack or why it is launched.

A handout provided to the Board by Symantec, attributes the following monetary values placed on hacker tools:

- **Exploit Kit**
  Eleonore – $1,500; Mmpack – $1,000
- **Zero-Day**
  Zero-1 – $250,000; Zero-2 – $5,000
- **Bots**
  Bot-1 – $10,500; Bot-2 – $2,500
- **Trojan Scripts**
  Script-1 – $800; Script-2 – $500
- **Credit Card Information**
  $1.70 per unit
- **Bank Account Credentials**
  $10 to $900
- **E-mail Accounts**
  $1 to $18
- **Full Identities**
  $.67

Though the increasing onslaught of data breaches is heavily documented, what is less understood is why specific breaches occur. Today, breaches primarily result from targeted attacks, human error, and system problems.

Targeted attacks have increased. Email is still a major threat factor; spear phishing (or highly target emails) are a common source. Attackers will send emails to an individual or small group – designed to appeal to people with specific interests.

Over the past two years, nearly half are caused by hackers and would include malware written by hackers. Some attack company servers, where hackers look for unpatched vulnerabilities, websites, or undefended connections to the internet. But hackers primarily focus on traditional social engineering trying to trick someone to open an infected file or directed to go to a bad or infected website. One major attack was so well designed it directed the user to retrieve it from his/her spam folder.

A good attack is just as much about human psychology as it is about technology. Breaches also result from human error – often company employees who fail to follow company security policies. Social media is an increasingly valuable tool, exploiting the trust someone places in a friend's message, not thinking twice about clicking on it. Social media is also increasingly used to conduct reconnaissance on individuals to develop highly-targeted spear-phishing.

It has been observed of a rapid growth of watering hole attacks. Cyber criminals have become highly adept at lying in wait on specific websites, which, when accessed, will spread infection. For instance, one hacker appealed to mobile app developers by offering links to tools to develop mobile apps. In another case, we noticed that 500 different companies, visiting a specific site, were compromised within 24 hours. Once inside, hackers typically conduct reconnaissance and then move laterally across the system to compromise your information. Hackers are now becoming extremely focused on targeting and filtering out the others. Retailers are still in the cross hairs, providing the biggest source of point-of-sale (POS) credit card information. On whether POS attacks new or newly-discovered, it is yet to be determined. Although POS attacks began in 2005, there has been an upsurge starting in 2012.

On the discussion of chip-and-signature more secure or chip-and-pin, it is good sign that credit card companies aggressively market to consumers, but it also means that criminals can target a larger source.

The greater question is how to protect and secure our data. The speaker emphasized that it is always good to start with the basics – strong passwords and patch management.

Cyber criminals exploit malware to produce an unlimited number of infected variants, so while malware might detect *known* infections, you're not protected against even moderately sophisticated attacks. Modern security software does not do much more than detect malware. It monitors your computer, watches for unusual traffic, and processes. Symantec has two technologies: Insight Sonar identifies viruses and puts files into context, monitors age, frequency, and location. So if a computer attempts to launch an executable file from an unknown source, it is probably malicious.

It is acceptable understanding that attackers will continue to pursue possible gaps, and with these best practices and preventive measures, attackers may still be able to find something else. Therefore, steps must be taken to make it extremely costly for cyber criminals so as hopefully they will redirect attention to another target. But there is no denying that a determined adversary is still on the horizon and they will continue to find a way to attack.

Encryption is also critical in data protection, rendering stolen information useless to the hacker. It is possible to also tag a specific file or document to track wherever it is stored. Another good strategy is employing an instant management plan after a breach is recommended. Information-sharing among the public and private sectors is also a good strategy at combatting cybercrime.

Symantec has testified three times last year before the administration and before Congress on the subject of data breach notification. There are currently 48 state-specific notification data breach laws. Symantec supports one national standard, based on these principles:

- It should apply to all entities, which collect, maintain, or sell significant numbers of records or personal information and should apply to government, the private sector, and academia.
- Pre-breach security measures should be part of any legislation. This would make it much less costly for companies that proactively employ security measures.
- New legislation should seek to minimize the likelihood of a breach by pushing organizations to take security measures. Best practice standards and guidelines already exist.
- Using encryption to render data unreadable. This will reduce the need for breach alerts when the data has already been rendered unusable.

In conclusion, data breaches continue and unable to eliminate everyone, Symantec helps protect and empower users. The increased potential to capture actuary data will reduce the number of hackers.

Updates on Privacy Engineering Whitepaper (PPT presentation provided)

Naomi Lefkovitz, Senior Privacy Policy Advisor, Information Technology Laboratory, NIST
Sean Brooks, Privacy Engineer, Information Technology Laboratory, NIST

Mr. Sean Brooks opened the presentation by explaining that he and Ms. Naomi Lefkovitz will provide an update of the Privacy Risk Management Framework modeled after NIST SP 800-53 Rev.4.[46] Since the last ISPAB meeting last October they have been trying to figure out the best approach and integrate thoughts on how to structure privacy risks and how to communicate those risks effectively by using a risk assessment process. The question that they want to address was how to integrate privacy from a

[46] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

risk management perspective and use a risk assessment to place controls in those areas from an individual perspective?

The privacy framework has provided the opportunity to narrow down some of the focus for understanding the amplitude of privacy risk assessments. A thought process was developed for understanding privacy and an organizations' development lifecycle for Information technology products and information systems. This process was used on a number of pilots under National Strategy for Trusted Identities in Cyberspace (NSTIC). A number of individuals have volunteered to assist in working through this proposed process. The process illustrated in the presentation is driven to establish 1) organizations' objectives for privacy from an operational perspective, 2) organizations' priorities in providing privacy protections from certain permission levels of privacy to their customers, and lastly, 3) how those objectives are expressed in information systems to reflect how the organizations are managing privacy the way it is structured in the systems.

The framing of those objectives and analysis of how organizations govern their privacy practices have given appropriate guidance to work through some of the NSTIC pilots in assessing the systems design through the organizations privacy objectives. Mr. Brooks stated that the goal, through IT design, is a process that can mitigate the proper tools in place for any risk that may arise – in addition to assessing privacy in an ongoing fashion, just as with any other risk assessment.

Ms. Lefkovitz stated that they are searching for adverse effects on privacy, specifically on adverse effects on individuals through the data lifecycle from a Personal Information Identity (PII) perspective. The impacts on organizations are minor as they are results from those adverse effects on individuals. However, organizations should account for those effects. This privacy risk assessment raises a range of problems that can essentially be used to test against our process. Organizations and agencies could also use this process as a mean to analyze types of risks they could encounter. There is still work to be done to define the distinction between security and privacy. There is an overlap of information but it can be managed in a risk management framework. The main focus is privacy risk management while complementary data actions focus less on security.

The Board noted that these data actions directed more on person than security. A lot of security focus basing on the system behavior does not depend much on how someone thinks about what's happening. For example, the "loss of trust" concept is something people feel and people may feel it under different circumstances.

Ms. Lefkovitz offered an example to the Board -- if a hacker penetrates a system and attains PII information. This will impact on confidentiality and controls to keep unauthorized access from personal information. Having a privacy risk management framework in place will be able to manage these threats. By evaluating the impacts in your risk management assessment would identify any theft of personal information was breached.

During workshops in April[47] and September[48] 2014, agencies and organizations provided feedback that aided in identifying and placing controls related to privacy that differ vastly from security controls. Some examples of potential privacy problems related to individuals are (see PPT slid 4):

- Loss of Trust

[47] http://www.nist.gov/itl/csd/privacy-engineering-workshop.cfm

[48] http://www.nist.gov/itl/csd/privacy-engineering-workshop-september-15-16-2014.cfm

- Loss of Self Determination
- Discrimination
- Economic Loss

The concern is there is no abstract way of thinking about privacy. Primary struggles, Fair Information Practice Principles (FIPPs)[49] in agencies read like controls comparing to NIST SP 800-53, Appendix J. There is not a lot of real guidance related to problems that may exist. Another concern was that the principal controls are important to many organizations but lack of communication on appropriate implementation with privacy. The main focus should be on the objectives in principal disciplines rather than vocabulary.

The feedback from the workshops helps to make some refinements to the objectives (reference presentation slides). The objectives help to define the privacy objectives that will drive design requirements. The reoccurring process objectives are:

- Predictability and Manageability - Are big concepts for personal information and processes of what the system is doing.
- Obscurity / Unlinkability - These objectives are complementary to your business processes although there is an issue with obscurity not linking to the individual or internal leakage not needed by the organization. This concept is still being fleshed out for clarity.

In closing, Ms. Lefkovitz mentioned that the risk assessment process will enable organizations to build a map of data controls and to identify risks. The mapping will assist in identifying possible risk problem areas and / or situations that need to be acted upon.

Updates on OMB Circular No. A-130 Revised[50]

Carol Bales, Senior Policy Analyst, Office of Management and Budget

Ms. Carol Bales is with OMB's cyber unit and has been serving in various capacities within OMB for the past ten years. In the past couple of years, she worked in the Agency Oversight and Communications Team, and was recently reassigned to be a part of the cyber unit, specifically to lead FISMA modernization efforts and Revision of the OMB Circular A-130 that is the policy on federal information resources.

Yesterday, Mr. Grant Schneider, OMB, presented to this Board on the establishment of the E-Gov Cyber and National Security Unit.[51] The new unit is part of how the Office of Electronic Government and Information Technology oversees agency cyber efforts. OMB is reasserting its cyber oversight role with a new group of experts. This unit works very closely with the National Security Council staff, DHS, and NIST to serve federal agencies to execute the administration's priorities and to ensure that best practices are followed.

OMB Circular A-130 is a foundational policy covering information resource management requirements, e.g. information systems, technology as well privacy, security, and the requirements of the government

[49] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

[50] http://www.whitehouse.gov/omb/circulars_a130_a130trans4/

[51] http://www.federalnewsradio.com/513/3798978/OMB-reaffirms-cyber-oversight-role

paperwork Act. In March 2012, OMB prepared a draft revision to Circular A-130, which was circulated to agencies for review and comments in May 2012, and again in June 2013.

We are currently updating Circular A-130 to incorporate new legislative requirements, specifically the Federal Information Technology Acquisition Reform Act (FITARA) as well as the FISMA of 2014. As part of that process, OMB has conducted a number of stakeholder outreach sessions (both internal and external) with the purpose of obtaining lessons learned and other relevant information to assist in updating our policies.

Regarding Appendix III[52] to OMB Circular No. A-130, Security of Federal Automated Information Resources, there are a number of changes recurrent with FISMA and SP 800 series. A process is in place to coordinate with new stakeholders prior to releasing the draft for broader agency internal review. This will be followed by another internal document review, a 30-day comment period, to begin in late spring leading to releasing a comprehensive update by December 2015. This effort is to update the entire circular.

In addition to A130, there are plans to update OMB policies on privacy and incident response. So, at the request of OMB, the privacy committee is establishing a working group, providing OMB input for updating privacy-related policies as described in M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information,[53] and M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments[54]. In conjunction to the FISMA modernization effort, OMB is working very closely with DHS and US-CERT to update new guidelines on reporting security incidents, security performance and threat incident reporting metric guidelines (see M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices).[5556]

The Board is interested in information on staffing build-up and changes that occurred to assist with these changes. Ms. Bales summarized staffing assets each of these focuses on specific aspects of security, privacy, cybersecurity and modernization. Each area is broken out with added staff to support the areas of interest and changes having occurred. OMB is planning to hire more staff and contractors to support their tasks.

Ms Bales confirmed to the Board that OMB does get involved in post-mortem incident responses. Guidelines standards are based on Appendix III and aligned with NIST. These standards have been implemented for years, and therefore all resulting activities have no impact on the budget. Guidance on the Federal Information Technology Acquisition Reform Act (FITARA) was also issued. The goal is to ensure as much consistency as possible among agencies.

The meeting recessed at 3:45 P.M., Thursday, February 12, 2015.

---

[52] https://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii

[53] https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

[54] https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-19.pdf

[55] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf

[56] http://www.fiercegovernmentit.com/story/omb-changes-security-incident-reporting-procedures-tweaks-fisma-metrics/2014-10-06

Friday, February 13, 2015

The Chair started the meeting at 8:38 A.M.

Role of the Chief Information Officer and Federal Information Technology Acquisition Reform Act (FITARA)[57]

Benjamin R. Sweezy, FITARA Strategy Lead, OMB

Mr. Benjamin Sweezy began by stating that FITARA was passed in December 2014[58] and centered on a set of requirements on the role of the Chief Information Officer (CIO) in federal agencies. The FITARA also includes many provisions to report to congress. The law contains seven sections, three of which formalize or put into law management practices for IT, and one defines CIO authority. The authority applies to the largest Chief Financial Officer (CFO) Act agencies. There is a set of overlapping exclusions for DOD and the intelligence community, but overall, in the discussion has been on how we use FITARA and how OMB offers guidance and policy, in the form of a standard while providing more consistency in government-wide implementation of the Act. OMB has a number of strategies, plans, and report metrics, queued-up as reports from the agencies to Congress and from OMB to Congress in each of those management areas.

The main point in solidify central authorities only for the department CIO and barred multiple CIOs. The Department Central CIO is to assert the role in reviewing and improving contract-related information technology, reprogramming funds (a budget execution concept of resources related to information technology), reviewing and improving the hiring of bureau agency Component CIOs for IT leadership, which is in essence, a CIO whether or not the title is conferred. The Department Central CIO also approves the agency's IT budget. Alongside every provision, there exists the possibility of alternative governance processes that do not necessarily rely on the CIO to review every contract, acquisition, or budget. OMB's role in policy and guidance evaluates acceptable processes, and acceptable roles assumed by the CIO as the process unfolds.

Following the approval and passing of the bill, Mr. Sweezy and his colleagues conducted outreach to effective stakeholders, and in February, they drafted policy and guidance that should be used to fostering government-wide consistency. The law should clear in March and disseminated in April. Mr. Sweezy stated that sometime in spring 2015 they will make available changes to federal agencies CIO and every step of the management decision process.

On whether FITARA will affect the Chief Information Security Officer's (CISO) role in agencies, Mr. Sweezy replied that the CISO role is not specifically mentioned in the law by name, however, it may affect the role in other ways. He explained that much of their outreach is not just in the federal IT community but also include acquisition, CFOs and the Budget Office.

Mr. Sweezy and his colleagues are working with various agencies on how to review major IT programs through an investment review board or through other governance processes. However, FITARA is meant to address all information technologies, and not necessarily conspicuous technologies. Also, agencies are considering on long term of IT decisions that affect the ability of Department CIOs to be accountable

---

[57] https://www.congress.gov/bill/113th-congress/house-bill/1232

[58] http://www.nextgov.com/cio-briefing/2014/12/fitara-fisma-reform-5-key-tech-bills-passed-congress-2014/101916/

for protecting and managing the entire network. The premise of Department CIOs having greater involvement in decisions across the entire department is a step toward meeting FITARA as the law stipulates that "a federal agency cannot enter into contract or other agreements for the purchase of IT or IT-related services without the review and approval of the CIO."

The IT community has a number of questions and request clarification on:

- Define "contract" and "other agreement.
- Level of details required
- CIO must approve on 1) an overall acquisition strategy and certify its requirements, or 2) every purchase, every action on a CLIN, or 3) on any procurement or 4) subject to a governance process designed by the department CIO
- Degree to which OMB is addressing it – versus establishing a set of complex principles
- The law permits the Department CIO to hire bureau CIOs or people acting in that role. But there were questions pertaining on whether Department CIO can only be involved in hiring or only be implemented going forward or can CIOs review current personnel

The spirit of the law requires involvement by the Department CIO in the decision-making process, but the tradeoff is the impracticability of reviewing every contract. OMB does not want to set up the CIOs or IT organizations for failure, if the process is too involved to follow efficiently. The presenter reported that one of the success stories seen in agencies is incorporating Department CIO feedback into the performance evaluation of bureau CIOs. The intent in the planning is to address the *relationship* between the Department CIO and CIOs, and Department CIO's involvement in the evaluation of CIOs in a reporting, supervisory relationship. The Board raised an example of one particular department where the CIO basically controls the creation of half the department CIO's performance plan. Mr. Sweezy had heard it described as "the technical evaluation comes from the Department CIO and the other components come from the program or other rating officials." That is one of the distinctions OMB is reviewing.

Agencies vary in their structure, size, and IT investment processes. Many believe that the IT and the investment are at the agency-level, but they are rather at the department level. It is Mr. Sweezy's interpretation that the law is very conscious of the disparity in organization size, and he would rather not speculate on the process of informing the law. But in some cases, CIOs struggle to testify on their accountability of IT decisions in each department because they feel they have limited role and jurisdiction in their departments.

OMB seeks to tighten the relationship of Department CIOs functions to approve bureau CIOs' so that more decisions being made at the level of the bureau component are consistent with the overall efforts throughout department. The OMB revision of A-130 is definitely a channel to update these authorities and OMB is open to suggestions for improvement and feedback is encouraged from agencies.

OMB would like to set up a meeting with Congress either this year or the next so as to discuss how to ensure the type of authorities and requirements that FITARA levies on department CIOs/agency CIOs in properly defining their roles.

The Board asked whether the reference to "risk" is pointing to high *financial* risk and not security or privacy risks. Mr. Sweeney's response was that "risk" could mean multiple risk impact areas. Currently, they use high risk and a high risk rating as the primary metric for determining follow-up action for issues like struggling IT investments. Agencies are to establish CIO evaluation of IT investment. OMB have

been using for the past six years the evaluation designed based on criteria with a scale of a 1-through-5 or red-to-green. Since risk is a core concept in that evaluation, OMB is evaluating how to define the degree of high risk requirements of FITARA can be applied to the CIO evaluation of major investments. If a major IT investment has high risk or a high risk rating for four quarters in a row, there must be an OMB investment review involving agency and OMB personnel. The review, which includes the outcome, remediation, and follow-on steps, is then reported to Congress. If, after that session, the IT investment remains at high risk for four consecutive quarters, OMB must produce development, modification, and enhancement funding for that investment until CIO can certify that the investment is back on track.

Concerning classified and unclassified information, there is no distinction described in the law. IT telecommunications programs that are completely funded by NIPRnet (Nonsecure Internet Protocol (IP) Router Network) are excluded from the authority. But there are many other sections of FITARA concerned with transparency reporting and data center consolidation to which exceptions apply – whether national security systems referring back to the statutory language of FISMA around national security systems, or systems whose transparency should not be publicly recorded, as determined by the Secretary of Defense, DNI, or the OMB Director.

FITARA addresses at least three approaches to data centers – 1) closures, 2) cost savings, and 3) optimization measures. The measures concerning data center consolidation have been fairly consistent with OMB's practices.

Since 2010, Mr. Sweezy's office has been tracking the closure of data centers to meeting the goal of 40% closure by 2015. OMB is following up with agencies to measure optimization metrics around forming of core data centers. The efforts are to have agencies shut down non-core data centers, moving their operations to more efficient core data centers, and optimize the operations of the core data centers. FITARA is consistent with that effort.

Another major effort concerns cost savings in data center. It requires that OMB and agencies establish a method of standards to measure cost savings. Agencies have many questions and concerns in determining the dollar value to the cost of operating a data center. This difficulty arises, partly because of the variety of resources involved in data centers, whether facilities, real estate, personnel, or IT. Since the budget for data centers is not accounted as individual line items, agencies cannot provide a breakdown of the expenses for data centers, any saving, or the costs. But FITARA requires agencies and OMB to submit reports on cost savings have been and cost savings will be from strategies of data center consolidation to Congress. For the past five years, the agencies and OMB have published agency closure plans for data centers that include detailed descriptions of data centers under review.

The Board noted that some of the provisions seem to have sunset clauses and some are imminent. Congress potentially will revisit some of these management controls. OMB has specifically removed the sunset provisions.

As part of a 25-point plan formulated a couple of years ago, OMB worked with the Office of Federal Procurement Policy to establish the concept of IT acquisition quandary of which consist of folks who particularly work in the IT acquisition and procurement arena.

When agencies submit agency acquisition human capital plans to the OMB, FITARA requires agencies to provide a section addressing an IT provision workforce. This is an important step toward encouraging procurement community involvement with IT, and to better describe where they stand in terms of training and other related provisions.

CIOs on average have short tenure of two years. The Board asked about potential concerns regarding decisions made by departed CIOs. OMB has yet to consider on tenure of CIOs, but focus on their performance on the job. FITARA considers the relationship in the life of IT investments that should improve IT resources. This is also more effective and impactful for customers.

Updates on NIST Cryptographic Standards Program (PPT presentation provided)

Matt Scholl, Chief, Computer Security Division, ITL, NIST
Andrew Regenscheid, Computer Scientist, Computer Security Division, NIST

Mr. Regenscheid began his updates with a summary of his last presentation last October 2014, and his presentation today will include CSP project timeline (see slide #2 of presentation):

- September 2013, NIST published news reports and addressed subsequent concerns over crypto standards.
- February 2014, NIST IR 7977 (Draft) NIST Cryptographic Standards and Guidelines Development Process (1st Draft) was published
- February 2014, the NIST Director charged the Visiting Committee on Advanced Technology (VCAT) to review cryptographic activities.
- July 2014, NIST conducted a VCAT/Committee of Visitors (COV) Review, and a status update to VCAT/ISPAB in October
- January 2015, second Draft of NISTIR 7977[59] was released
- January 2015, proposed withdrawal of six FIPS.

On the subject of openness and transparency, VCAT report[60] recommended the development and implementation of a plan to further increase the involvement of the cryptographic community, including members of academia and industry. NIST's role and process improvements are outlined in the revised NISTIR 7977. NIST welcomes input, including authorship, comments, and responses. Mr. Regenscheid reaffirmed NIST's use of standards as developed by Standards Developing Organizations (SDOs), and its commitment to work with SDOs on global acceptance and standards.

VCAT also recommended an increase in the number of technical staff. The FY2015 budget allocates an additional of $6 million for cryptography-related work. Active recruitment is underway. Funding will also go toward planning grants to expand relationships with academic and research institutions and toward workshops to solicit input from researchers and from industry.

In addition, VCAT recommended clarification of the relation with the NSA. While NIST may seek the advice of the NSA on cryptographic matters, NIST must be in a position to assess and/or reject that advice. To begin on a positive footing, all NSA contributions to NIST will be acknowledged. In accordance with NIST authorship guidelines, NSA authors will be clearly identified. Comments on drafts will be made public. A revision to a NIST-NSA Memorandum of Understanding is also planned.

---

[59] http://csrc.nist.gov/publications/drafts/nistir-7977/nistir_7977_second_draft.pdf

[60] http://www.nist.gov/director/vcat/crypto-review-071414.cfm; http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf

Concerning technical work, development, and processes, NIST has and will work openly with the cryptographic community to determine how best to address a number of specific technical recommendations. This technological effort is defined in a number of reports, including NISTIR 7977, and from solicited comments.

The NISTIR commits to promoting algorithms with security proofs and to developing a policy on intellectual property and on elliptic curve standards. In November 2014, NIST released an edited NIST SP 800-90A Rev 1[61] (Draft) that was previously released in April 2014. NIST IR 7977Revised was released on January 23, 2015, with the comment period ending on March 27. Included in the report are principles of usability and IP, an expansion of other principles, and an outlined seven-stage Crypto Standards Lifecycle (CPL). The CPL process (1) identifies and evaluates the need, (2) announces intent, (3) considers requirements and solutions, (4) defines specific plans/processes, (5) develops FIPS or SP (if applicable), achieves global acceptance from SDOs, (7) and follow-on maintenance.

NIST will focus primarily on Quantum-Resistant Cryptography, Privacy-Enhanced Cryptography, usability, Elliptic Curve Standards, Lightweight Cryptography, and Hash function standards and guidelines. These focuses were included in a number of upcoming events.[62] Between April and July 2015, NIST will host the following workshops: Cybersecurity in a Post-Quantum World (April), Elliptic Curve Cryptography (June), and Lightweight Cryptography (July). A discussion followed on NIST's strategic directions, outreach efforts, collaboration with SDOs, the implementation of recommendations, and the standards/guidelines lifecycle.

Public Participation

Debbie Taylor Moore, Principal and CEO, Cyber Zephyr – See Annex B for written statement

Ms. Debbie Taylor Moore, an independent consultant, requested to provide a 5-minute statement to the Board as described in ISPAB meeting Federal Register Notice.[63] Ms. Moore's statement is included in its entirety in Annex B of this record. During this session, Ms. Moore spoke about the CDM program.

Ms. Moore provided suggestions on CDM Phase II that CDM staffers are working hard to roll out. The objective, as well that of our stakeholders, is to focus on implementation across government agencies. It is sometimes difficult to manage such a large number of people. At the same time, through joint workshops, we have been able to adhere to a documented approach going forward.

The foundation – upon which service, developing a mature model, transforming business, and encouraging behavior change – will come from industry.

[61] http://csrc.nist.gov/publications/drafts/800-90/sp800-90a_r1_draft_november2014_ver.pdf

[62] http://csrc.nist.gov/news_events/events.html

[63] https://www.federalregister.gov/articles/2015/01/02/2014-30780/open-meeting-of-the-information-security-and-privacy-advisory-board

Update on Security and Electronic Health Records (EHR)

Debbie Bucci, Office of Standards and Interoperability, Office of the National Coordinator for Health IT, HHS

Steve Posnack, Director, Office of Standards and Technology, Office of National Coordinator for Health IT, HHS

Deven McGraw, Partner, Manatt, Phelps & Phillips, LLP

Mr. Posnack joined the Office of the National Coordinator for Health Information Technology (ONC) in July 2005. From 2010 to 2014, he led ONC's Federal Policy Division within the Office of Policy and Planning. Working in that capacity, he led ONC's regulatory affairs, legislative analysis, as well as several federal policy development and coordination activities.

In his presentation, Mr. Posnack said that when health records are electronically digitized, there are many security risks. Health Insurance Portability and Accountability Act (HIPAA) notifications were therefore modified to include breach notifications that changed compliance in healthcare. To help in this area, a process of operability to facilitate delivery was initiated.

On Tuesday, February 11, 2014, Interoperability Roadmap 1.0 (*Connecting Health and Care for the Nation – A shared nationwide Interoperability Roadmap)*[64] was released and is currently out for approximately 60 days public comment ending on April 3, 2015.[65] It is a roadmap proposes critical actions for both public and private stakeholders that will advance our nation towards an interoperable health IT ecosystem, advance research and ultimately achieve a learning health. Implementation of the roadmap is divided into three milestones. The roadmap takes into consideration healthcare delivery, efficiency, safety, research, and security.

It was noted recently an increase in adoption resulting in a consequent increase in healthcare records and demand on healthcare providers. This necessitated modifications to the Affordable Healthcare Act. One change pertains to the way consumers in access management and impacts the interaction between patient and provider. Under Patient-generated Health Data (PGHD),[66] when a patient transfers from one provider to another, the assumption was the patient information will also be transferred. The Board noted that the actual utility of PGHD has some serious problems, but EHR is addressing those issues in the form of a standardized method of tracking identity and controlling access.

Much of the work does not attract national attention, but does attract attention in the form of consumer demand for access to their data – an issue impacting database management. This now includes the use of personal apps related to generating, storing, and tracking data related the individual's health. Mr. Posnack acknowledged Debbie Bucci as instrumental in the effort to securely synchronize the data with healthcare providers.

The major reasons for putting together the Interoperability roadmap and the first milestone will address many of the issues and concerns related to that aspect of the project. Issues include the resources available to individual healthcare providers and the security of information-sharing.

---

[64] http://www.healthit.gov/sites/default/files/nationwide-interoperability-roadmap-draft-version-1.0.pdf

[65] http://www.healthit.gov/policy-researchers-implementers/interoperability

[66] http://www.healthit.gov/sites/default/files/patient_generated_data_factsheet.pdf

Ms. McGraw is a partner in the healthcare practice of Manatt, Phelps & Phillips, providing legal, regulatory, and strategic policy and business counsel with respect to the adoption and implementation of healthcare IT and the electronic health information exchange. Since 2010 she has participated in the privacy and security working group, and explored the issue of educating patients in accessing information from their providers through provider portals; their ability to download that information, whether to an app, to a laptop, or other related electronic device; and their ability to upload the information to another provider.

When examining into the issue of accessing provider portals, a national strategy is critical to address many significant challenges. Therefore, it was recommended that, if the *right* of the patient to access their records is critically important, efforts to protect that information should not interfere with that right. The challenge is to design a system to incorporate *both* features without compromising one or the other. To that end, we encouraged vendors to provide functionality for users who may not necessarily be technologically astute. The recommendation is to consider online banking as a model.

Ms. McGraw gained an operational perspective as a full-time volunteer at Suburban Hospital in Bethesda, Maryland and works on a Johns Hopkins system. A NIH patient will get authorization to access the portal site at Johns Hopkins to set up an account, using an individualized authorization code. That's for the first aspects of the process. From that point on, the patient is logged-on, but it is not clear of whether or not there's another security layer in the process. Often, it requires just a phone call to initiate the online process. But, in rural areas it may not always be possible to connect people to the portal.

Mr. Posnack described the elements in the three milestones. This 3-year point in time we're now in focuses on the nature of our ability to send and receive data. How do we enable providers to deploy? That entails access to other healthcare provider systems, either through an intermediary (Debbie mentioned one) providing one infrastructure component. There are others, like regional, state, or national health information exchanges. He mentioned that California has at least 20 health information exchanges. New York has an infrastructure spanning the state, providing information about how individual exchanges link together.

The prospect of connectivity between states poses a security challenge, which must take into consideration individual state laws from a healthcare perspective, changes in state law, and state-specific events, like breaches or other forms of public health emergency. Another consideration centers on possible difference between laws applying to *senders* and *receivers* of the healthcare information. These jurisdictional differences are sometimes used as an excuse to share healthcare information. These issues might often be addressed through policy, not necessarily requiring technological enhancements.

If the technology works, jurisdictional issues can be resolved by standardizing the language and training requirements necessary for membership in "the club." When some providers, for whatever reason, refuse membership in the club, they will be unable to share information with others complying with membership requirements. But this, too, can be addressed through policy.

The Board cited a technology issue for clarification -- providers (not necessarily hostile to one another) encounter problems when an electronic system used by one does not match up with a system used by another? There are numerous cases in which differences exist between system-specific terminologies. What constitutes the constituent parts of a health document? How is medication represented? How are patient problems represented? How are allergies represented? For example, the term "football" has different connotations in the US and in the UK.

In some cases, a patient might face significant costs associated with accessing their healthcare information. This is another area where it had been discussed with FTC regarding any existing policies, which in light of current efforts, might be unfair.

The panelists are considering various models such as subscription models, transactional models, and volume-based models. They have also received data from labs regarding the disparity in the amount of result information is provided depending on tier level. Resolution requires reconciling a number of very complex issues.

Part of the effort is considering the evolution in market models in which functions and standards, privacy protections, rules of engagement regarding government, and other stakeholder concerns all work together. Many different entities at different levels exercise an oversight for administration responsibilities at the state and multi-state levels. The goal is to bring stakeholders together to avoid "islands" or "silos" of information. They are also looking at documentation structure and obtaining a consensus vocabulary level, and have a number of statement development organizations with which we interact.

Ms. McGraw briefed the Board on her group's activities during the past year:

- In Stage 1, we provided advice on privacy and security issues, focusing a great deal, in our first year, on risk analysis as well as on address encryption for data at risk.
- In Stage 2 we offered guidance on compliance with our recommended procedures. If HIPAA didn't require particular functionality, and those features were turned off, it musts be documented why.
- In Stage 3, compliance, determined by audit, revealed a high degree of non-compliance with security recommendations. We found that much of stolen data was not encrypted.

The Board asked if there was any problem when using the checkbox approach without following through on what was claimed. The panelist affirmed the possibilities. Although the Office of Civil Rights (OCR) and CMS issued reports to that effect, and it has been discussed with security information officers who said it was difficult to monitor compliance.

Auditing results could be strengthened when tied to penalties for non-compliance to HIPAA. Companies are randomly selected for audit from the OCR. CMS has shown a reluctance to stretch the meaningful use program into an enforcement tool. It is suspected that mandatory performance tracking will not be enforced. OCR is really wondering what else need to be done to encourage compliance. They do not train physicians in how to protect data and especially there are no allocated resources to training efforts.

Privacy issues contained in HIPAA requirements does not offer much information regarding electronic disclosure. It is the view of Congress that, with electronic disclosure, existing exceptions related to surgeries should be eliminated, and they rely on OCR to develop a standard regarding electronic disclosures.

When a physician in a hospital electronically accesses a patient's records, it is a *disclosure* and should not be considered as a simple act of acquiring information. But again, even if every electronic action is tracked, compliance remains a concern.

The panelists acknowledged at the outset that they have to have an effective technology otherwise people do not know which providers that they cannot use. And when an individual is concerned that his or her health data was inappropriately accessed, the burden should not be placed on the individual to

discover who, where, or when the data was accessed. The individual should be able to initiate an investigation and to have tools in the system to take the appropriate action.

Board Review

During the Board review, the ISPAB Board approved the following meeting dates for 2016:

March 2, 3, 4

June 15, 16, 17

October 26, 27, 28

The Board Chair suggested that dates be reviewed again at the next meeting in June 2015, but in the interim, the dates will be posted on the ISPAB website.

Approval of meeting minutes, October 2014

The Chair pointed two edits. Ms. Gale Stone proposed the motion to approve the meeting minutes and it was seconded by Mr. Danny Toler. All were in favor. The meeting minutes will be uploaded on the ISPAB webpage after correction is made.

The Board evaluated the discussions during this meeting and also considered topics for future meetings:

- UAS drones -- to be included in next meeting
- Carol Bales (OMB) requested to present the eventual release of Circular A-130 Revised at June meeting. It is anticipated that the circular will be released for comments just before ISPAB meeting.
- The Board has agreed to invite Dr. Phyllis Schneck (former ISPAB member), Deputy Under Secretary, US DHS to the next meeting. Mr. Danny Toler, DHS, will facilitate the invitation.
- Invite a representative from FBI to present on information collection
- Dr. Kevin Fu to facilitate a panel presentation on the pros and cons of open source supply chains and the bills of material.
- Re-invite the Chief Technology Officer from the White House presentation – he was called to attend the White House Summit on Cybersecurity and Consumer Protection, Stanford University, CA
- The Board proposed new or continued topics of interest:
    - Big payoffs in cybersecurity were discussed, including browsers, certificate security, and contractual clauses with big integrators.
    - The insider threat program was of interest to the Board.
    - Ongoing Cybersecurity governance: long term plans (NIST Update)
    - National Highway Safety Administration (NHTSA) infrastructure (auto-manufacturer communication and usability)
    - International breach data update
    - Medical device update
    - EU delegates in Washington D.C. (to update)
        - NAS platform and directive on the EU structure:

- International standards and US alignments and positions (slated for the June ISPAB meeting or at the end of 2015)
- State Department will also participate in the discussion
- Communicating cybersecurity and information-sharing between the US and foreign countries: What are the regulatory structures affecting the type of information we can share in light of privacy directives? Does the restriction on information sharing (like PII) in a cyber-security context pose a concern for global adversary attacks? What is the jurisdiction of global industry (like banking) that would affect critical infrastructure?
  - Cyber-storm (cyber exercises)
  - Board comment in incident response: The Board is trying to understand the pressure points of responding to incidents with government and private sector information, and working through a process that is both efficient and effective. This may not be something to which ISPAB can respond, providing meaningful recommendations and council.

- NSS Updates
  - We still haven't cracked the code on relevant information-sharing. CTIC recognizes this as an ongoing issue.
  - Derived Credentials Update (CIO-0716 to update)
- Public comment memos review (action items for Board members)
  - Circular A-130 review in preparation for discussion with Carol Bales
  - Various other papers as they are released for draft
- CDM: No additional feedback or follow-up needed
- Updates on Executive Order (EO) Cybersecurity Framework and Legislative action: No additional feedback or follow-up needed.
- Overview of 18F, GSA – Interesting presentation – No additional feedback or follow-up needed.
- FAA Unmanned Aircraft Systems Update
  - Concern expressed for not having a policy on UAS / drones
  - FAA writes their own standards
  - Who else should be operating in this space?
- NSA Civil Liberties and Privacy Office – No additional feedback or follow-up needed.
- FTC Report on Internet of Things
  - Security minimization for credit and/or employment. Discussion at the federal level as well.
- Presentation on Breaches and Breach reporting
  - Suitability of initial DHS hires (DHS). Do NIST and Treasury have suitable onboarding procedures?
- Privacy Engineering Whitepaper Update

- Board would like to wait until there is pilot feedback before requesting an update in this area.
- Modern risk analysis – recent problems have been unforeseeable (like Jazz Bug).
- Recommends carefully building-out this privacy risk model.

Board Wrap-up

The following Board comments were taken after the last discussion Friday, February 13, 2015. The Chair characterized much of the content as abstract, but reminded the Board that specific issues and principles lay just behind the abstractions.

- FITARA – Interesting presentation but further information or follow-up is needed
- NIST Cryptographic Program Updates
  - It seemed, though, that effort was required to ferret out those issues and principles.
  - Most of what we heard is still in the early stages.
  - One might speculate that, under some circumstances, there would be comments that would be highly relevant to a cryptographic standard that people would not want to make publicly. And no one mentioned that concern.
  - Most of the comments that influence us are things that occur at the standard bar level. So how do we deal with that?
  - Is there a way to capture the information and show traceability?
  - Without such concern, everything comes out all smooth and other-worldly.
  - Those concerns are usually expressed in proposals.
  - Some of the content is diffused in sidebar discussions or submitted anonymously.
  - But anonymous comments have value regardless of who submitted them. We should make it a point to remind attendees that (1) they're free to submit anonymous comments and (2) we will give them the same attention as those whose sender is identified. We should remind them that we're not going to investigate the source of a comment.
- Update on Security and Electronic Health Records (EHR) – good panel presentation but no follow-up is necessary at this time.

The meeting adjourned at 11:57 A.M., Friday, February 13, 2015.

ANNEX A

List of Participants

Last Name	First Name	Affiliation	Role
Bales	Carol	OMB	Presenter
Barrett	Matt	NIST	Presenter
Brooks	Sean	NIST	Presenter
Bucci	Debbie	ONC, HHS	Presenter
George	Stephen	FAA	Presenter
Godbout	Greg	GSA	Presenter
J. Michael	Daniel	The White House	Presenter
Jagielski	Karen	FTC	Presenter
Lefkovitz	Naomi	NIST	Presenter
McGraw	Deven	Manatt, Phelps & Phillips, LLP	Presenter
McMahon	Andrew	GSA	Presenter
Posnack	Steve	HHS	Presenter
Regenscheid	Andrew	NIST	Presenter
Richards	Rebecca J.	NSA	Presenter
Schneider	Grant	The White House	Presenter
Sedgewick	Adam	NIST	Presenter
Wright	William	Symantec	Presenter
Beutel	Richard	Cyrrus Analytics	Visitor
Bussell	Jack	Access	Visitor
Ford	Kim	First Data	Visitor
Hernandez	Jessica	US Department of Treasury	Visitor
Hettingen	Mike	HSG	Visitor
Jain	Ravi	FAA	Visitor
Kerban	Jason	DOS	Visitor
Larson	Derek	OMB	Visitor
Mayer	Hannah	US DOJ	Visitor
Mitnick	Drew	Access	Visitor
Moss	Robin	US DOJ/OPU	Visitor
Noble	Marc	ISACA	Visitor
Scaville	Douglas	US Department of Treasury	Visitor
Schrader	Matt	Adobe	Visitor
Taylor Moore	Debbie	Cyber Zephyr, LLC	Visitor
Turner	Nathaniel	ACLU	Visitor
Heyman	Mat	Dakota	Visitor

Last Name	First Name	Affiliation	Role
Curran	J.	Telecom Reports	Visitor / Media
Marrs	Joe	Politico	Visitor / Media
Mazmanian	Adam	FCU	Visitor / Media
Michell	Charlie	Inside Cybersecurity	Visitor / Media
Miller	Jason	Federal News Radio	Visitor / Media
Otto	Greg	FedScoop	Visitor / Media
Perera	Dae	Politico	Visitor / Media

ANNEX B

Public Participation Statement for ISPAB – Friday, February 13th, 2015

Debbie Taylor Moore, Founder & CEO Cyber Zephyr, LLC

Debbie Taylor Moore is an independent management consultant who provides strategic management consulting to industry and government to further advance the public and private partnership in cybersecurity. www.CyberZephyr.com

Continuous Diagnostic Mitigation Phase 2

First, let's begin by acknowledging the hard work of many in government and industry who are managing the complexity of the administration and participation in the centralized Continuous Diagnostic Mitigation BPA. One challenge is the paradox of administering a multi-year acquisition vehicle for fundamental cybersecurity capabilities against the backdrop of the cyber threats growing in sophistication, velocity and volume of cyber threats, which it is partially, intends to address. All have good intentions and want to see this program work.

When speaking with both industry and government, a theme of mild frustration emerges. Primarily, there is concern over the distant, disparate chasm of communication and collaboration that exists between the industry BPA holders who provide the tools and services, and the federal agencies that the BPA is meant to serve. Both parties relate instances of restricted access to each other in Phase 1 of the program that they found to be more of a hindrance than inspiring fairness and progress for the BPA. Hopefully, Phase 2 of the program can overcome this challenge.

CDM Phase 2 requires an entirely different approach than the first phase. The focus in CDM Phase 1 was to discover and manage authorized IT hardware and software assets on the network, improve configuration management and offer a near real time view into an organization's status with regard to managing and remediating vulnerabilities. CDM Phase 2 aims for greater visibility into the human element. Who has access to which systems? Are the appropriate behaviors exhibited and associated with the roles, privileges and identity of the user or application to application access of a federal system? Phase 2 establishes a baseline for ongoing monitoring and measurement that ensures user and privileged access rights are aligned with both new and existing policy in order to prevent unauthorized system access, abuse or inappropriate use.

CDM Stakeholders on all sides realize that in the initial phase of the program, government participants were engaged in selecting and implementing long-proven, commodity-based security solutions, most of which have already existed in department and agency environments for many years. CDM Phase 2 represents tools and solutions that are not as familiar and widely deployed in the average government agency. A federal official in the midst of implementing "like solutions" shared that, "Less than 5% of agencies have deployed some of the technologies associated with Phase 2 throughout the enterprise".

CDM Phase 2 will require a significant degree of planning, consultation and understanding of the technologies available. There is a significant internal assessment that must be conducted in order to baseline an agency's current status with regard the way it manages identity and access. This requires the participation of a wider audience of stakeholders and is an intricate process. The steps to rediscovering each individual user's role, current access, lines of authority, and policy enforcement as it

relates to the systems in the agency is a daunting task. Further, making a determination whether an individual's current access and authorization to access systems is within or outside of policy, is difficult. Establishing and enforcing policy, once discovery has taken place-- is complex and potentially disruptive.

All stakeholders and leadership should openly acknowledge that individuals who once enjoyed unlimited, unfettered anonymous access to systems will probably in small part, resist being held accountable under a new program. This is not unusual, but it is precisely why programs like CDM will succeed best with the active sponsorship and participation of the top levels of management. It's precisely why there is a need for communicating the goals of the program at every level of the organization and working with a collaborative project team that understands the goals. Each organization needs to approach the development of:

- A detailed analysis of short falls/ areas for improvement of the current program and departmental priorities and policy goals.
- Complete and explicit documentation of needs specific to systems, applications, and lines of authority and control. (e.g. Network Ops Team has to collaborate with IA/Compliance Team)
- A trial evaluation team and a realistic test environment that has been vetted with other federal reference users.

The federal government must have the space to have a dialogue with industry for phase 2 to be successful. It is important to remind all groups that while CDM is an overlay to existing identity and access management initiatives, many of the foundational initiatives (FICAM/HSPD-12) have not been completed by all agencies. There is also a significant learning curve with regard to new technologies that exist to help combat the intentional and unintentional abuse of credentials.

Some recommendations for implementing CDM Phase 2:

- Consultation first, tools second.
- Ensure agencies and industry understand the end goal of CDM Phase 2 up front.
- Develop and execute CDM Phase 2 Industry and Government workshops, expos and technical exchanges for greater opportunities for collaboration and understanding.
- Consider requiring that BPA holders build technology prototypes for visualization and conceptualization up-front.
- Avoid "grouping" agencies by nebulous criteria for acquisition purposes, instead establish a maturity model that can be applied for sizing each individual agency's level of effort required to meet objectives.
- Frame CDM Phase 2 as a business transformation project that incorporates technology and less of a tool-buying and deployment exercise.
- Provide program updates for all parties that communicate technical, security and threat information in addition to contract administration updates.

The fact that there are an exhaustive number of product choices in a less mature solution arena calls for a more discerning federal buyer in CDM Phase 2. The decision to invest in Privileged Identity Management and other solutions is a part of a multi-step process that requires the consensus of multiple groups of stakeholders. It is critical to establish the appropriate level of planning up-front to determine the best security direction for the agency that also leverages the existing initiatives – FICAM, HSPD-12, etc. An agency should do its own homework and avoid relying solely on product checklists,

Schedule 70, market share data or marketing claims that map to a list of features. They should see an actual prototype that works. This is an endeavor for which departments and agencies need consultative partnerships with industry. Organizations must actually leverage the “in scope” services capabilities of the BPA holders upfront, to ensure accurate understanding of BPA holder capability. Additionally, agencies should review existing use cases deployed inside agencies Federal agencies who have been engaged early in evaluating and deploying solutions and solving the problems related to achieving a least privilege infrastructure.

Work with product vendors and integrators who understand the unique requirements of the U.S. Federal government and the long history of Identity and Access Management initiatives as well as the recent programs. Identify vendors who possess a solid roadmap and bridge to the future of cloud and mobile and the unique challenges of managing identity in these hybrid and emerging environments. These practices will ensure that the CDM implementation successfully overlays the agencies existing efforts without creating a new silo to manage. Let’s make a good program great - through rich and effective collaboration.

ANNEX C

RECENT and UPCOMING WORKSHOPS

Cybersecurity for Direct Digital Manufacturing Symposium
February 3, 2015, NIST Green Auditorium
Direct Digital Manufacturing (DDM) involves fabricating physical objects from a data file using computer-controlled processes with little to no human intervention.
http://www.nist.gov/itl/csd/cybersecurity-for-direct-digital-manufacturing-symposium.cfm

Cybersecurity and Consumer Protection Summit:
Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy
http://www.nist.gov/itl/executive-technical-workshop-on-improving-cybersecurity-and-consumer-privacy.cfm
February 12, 2015, 1:00 – 5:15 pm
Stanford University, Bechtel Conference Center at Encina Hall, 616 Serra Mall, Stanford, CA 94305-6055
The agenda is at https://nccoe.nist.gov/technical-workshop
Registration is limited to 100 participants. There is no fee to attend this workshop. Please register at https://www.fbcinc.com/e/nistcyberworkshop/

Workshop on Upcoming Special Publications Supporting FIPS 201-2
March 3-4, 2015, NIST Portrait Room
The purpose of the workshop is to exchange information on a number of upcoming new or revised Special Publications to align with FIPS 201-2 issued on September 2013.
http://www.nist.gov/itl/csd/fips201-2_workshop_2015.cfm

Federal Information Systems Security Education Association (FISSEA) – Changes, Challenges, and Collaborations: Effective Cybersecurity Training"
March 24-25, 2015, NIST
http://csrc.nist.gov/organizations/fissea/home/index.shtml

Workshop on Cybersecurity in a Post-Quantum World
April 2-3, 2015, NIST Gaithersburg, MD
The advent of practical quantum computing will break all commonly used public key cryptographic algorithms.
http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm

Workshop on Elliptic Curve Cryptography Standards
June 11-12, 2015, NIST – Green Auditorium Gaithersburg, MD
Elliptic curve cryptography will be critical to the adoption of strong cryptography as we migrate to higher security strengths. NIST has standardized elliptic curve cryptography for digital

signature algorithms in FIPS 186 and for key establishment schemes in NIST Special Publication 800-56A.
http://www.nist.gov/itl/csd/ct/ecc-workshop.cfm

Lightweight Cryptography Workshop
July 20-21, 2015, NIST Gaithersburg, MD
NIST seeks to discuss issues related to the security and resource requirements of applications in constrained environments, and potential future standardization of lightweight primitives.
http://www.nist.gov/itl/csd/ct/lwc_workshop2015.cfm

NIST PUBLICATIONS

January 2015

January 29, 2015 - Errata Update for Special Publication 800-53, Revision 4

January 26, 2015 - Special Publication 800-57, Part 3, Revision 1, *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance* has been approved as final.

January 23, 2015 - NISTIR 8018, *Public Safety Mobile Application Security Requirements Workshop Summary*, has been finalized and is now available (click here to see the announcement for this document)

January 23, 2015 - NISTIR 8018, Public Safety Mobile Application Security Requirements Workshop Summary, has been finalized and is now available

December 2014

Release of NIST Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations
http://csrc.nist.gov/publications/nistbul/itlbul2015_01.pdf

Release Of NIST Special Publication 800-157, Guidelines For Derived Personal Identity Verification (PIV) Credentials http://csrc.nist.gov/publications/nistbul/itlbul2014_12.pdf

November 2014

ITL Newsletter - Cryptographic Module Validation Program (CMVP)
http://csrc.nist.gov/publications/nistbul/itlbul2014_11.pdf

October 2014

ITL Newsletter, Release of NIST SP 800-147B, BIOS Protection Guidelines for Servers

Draft Publications Request for Comments Deadlines

November 2014
November 21, 2014 - SP 800-90 A Rev.1, *DRAFT Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
Comments closed on December 31, 2014

November 18, 2014 – SP 800-171 *DRAFT Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*
Comments submission closed January 16, 2015

January 2015

January 23, 2015 - Second Public Draft NISTIR 7977, *NIST Cryptographic Standards and Guidelines Development Process*, is available for review and public comment
Comments Deadline: **March 27, 2015**

February 2015

February 9, 2015 - Draft NISTIR 7621 Revision 1, *Small Business Information Security: The Fundamentals*

February 18, 2015 - Draft Special Publication 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems*

March 2015

March 27, 2015 - Second Public Draft NISTIR 7977, *NIST Cryptographic Standards and Guidelines Development Process*

NIST SPECIAL PUBLICATION 800-170 Computer Security Division 2013 Annual Report - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-170.pdf

Information Security and Privacy Advisory Board – see Page 30