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

June 12, 13, and 14, 2013

Wednesday, June 12, 2013 8:12 A.M. – 4:10 P.M. Thursday, June 13, 2013 8:07 A.M. – 4:32 P.M. Friday, June 14, 2013 8:10 A.M. – 12:32 P.M. The US Access Board 1331 F Street, N.W., Suite 800 Washington, D.C. 20004-1111	**Board Members**	
	Present	Absent with regrets
	Matthew Thomlinson (Chair), Microsoft Julie Boughn, DHHS /CMS Christopher Boyer, AT&T Greg Garcia, Garcia Cyber Partners Brian Gouker, U.S. Army War College Toby Levin (Retired) Edward Roback, Department of Treasury Phyllis Schneck, McAfee Inc. Gale Stone, Social Security Administration Peter Weinberger, Google, Inc.	Kevin Fu, University of Michigan

See Annex A for list of presenters and visitors.

Wednesday, June 12, 2013

The ISPAB Chair, Matt Thomlinson, called the meeting to order at 8:12 A.M., and began with the Board members providing a brief introduction and preparing for the first presenters of the day. Also discussed were specific agenda items and issues of interest to the Board such as:

- The next two days were to be Federal Information Security Management Act (FISMA) follow-on topics.
- Cloud / Federal Risk and Authorization Management Program (FedRAMP) review (interest in progress)
- Getting Agency view of Cloud opportunities
- Government Accountability Office (GAO) reports review
- New topic - Automated Security Indicators and Information Sharing

Continuous Monitoring and its Ability to Create Efficiencies

Information Sharing Protocols / Automated Indicators

Suzanne Lightman, Senior Information Security Advisor, National Institute of Standards and Technology
Danny Toler, Deputy Director, Federal Network Resilience, Department of Homeland Security (DHS)
[Presentation provided][1]

Ms. Suzanne Lightman discussed information sharing outside of the government and Mr. Danny Toler focused on continuous monitoring and shared indicators. Ms. Lightman explained that by working as a controller in a startup company and managing a helpdesk, she noticed problems with the line of communication in reporting incidents. There was a disconnection with small entities within an organization. The problem was that the same incident could be occurring in other assets of the company/organization but they were not communicating with each other. The incident could be considered small, but if it was occurring throughout the organization, it could easily become a much larger problem.

Ms. Lightman pinpointed issues to consider with information sharing and reporting incidents within an organization:

- Most people deal with what is in front of them.
- Emergency response centers are not fully utilized or are unaware an incident even occurred.
- Within entities, information sharing is hard; between agencies it is even harder.
- Information Sharing takes a lot of training and a lot of attention
- US-Community Emergency Response Team (CERT) would tell you the problem but the incident reporting process was too long and agencies felt no value was gained. The US-CERT perspective was that no value was gained because agencies are not reporting their incidents (Issue: Agencies would not be able to communicate back as it takes too long to report an incident and nothing of value is gained from the CERT reporting process).
- Most reporting was on the privacy breach side with very few security information cases.
- Private sector and government agency sharing can be difficult. At some level, private industry does not trust the government to protect their information and respond back to them and, at some level; the government does not trust private industry to do the right thing given the information. This is the same concept with CERT. Agencies are not getting information that is valuable from CERT and CERT is not getting information that is valuable to report.

Ms. Lightman emphasized that it is important to establish a single point of trust and she encourages CERT to have a single account holder in each agency to mitigate information sharing through people. Most agencies typically treat themselves as islands and people's concerns usually focus on their own agency. They are unaware of the larger picture and are perhaps not capable of recognizing symptomatic concerns. Part of this is lack of training. This philosophy could be fixed by teaching people within the organization the best practices for information sharing and enforcing continued practice and monitoring. Mr. Toler added that departments

[1] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_toler.pdf

within agencies had no idea how data points could be mitigated. Root cause analysis and resolution are of crucial importance; many agencies were still not aware of *where they were* in addressing the resolve and communicating that information back.

In response to Board's remarks of whether agencies may not be supporting the role of reporting incidents or may not have people to support the issue, Mr. Toler explained that it varies by agency and the overall size affects the organization and resources while GAO reported many such cases. Agencies within departments do not really share information. Even after mitigation is identified, there is a lack of tools that can account whether a patch has been distributed. System administrators do not have the tools or sophistication to know. They may perhaps have data, but mining that data is difficult.

Mr. Toler discussed the thoughts behind Continuous Diagnostics and Mitigation (CDM) Program (Slide 5 in the PowerPoint deck – CDM is for .GOV sites). The main purpose of CDM is attempting to reduce the number of data calls and shorten the response time between corrective actions taken by having an automated process.

The Benefits of CDM are:

- Searching for, finding, fixing, and reporting the worst cyber problems first in near-real time

CDM also enables System Administrators to (see PowerPoint slides):

- Respond to exploits at network speed
- Fulfill A130,[2] Management of Federal Information Resources, responsibilities as intended
- Implement NIST Publications on Continuous Monitoring (800-137 and parts of 800-37)
- Use strategic sourcing to lower cost

Regarding information sharing with CERT, and overlay of different paths of information sharing such as sector agencies, Information Sharing and Analysis Centers (ISACS), and CERT, Ms. Lightman agreed that this is one symptom between government and the private sector. At a recent Executive Order (EO)-directed Cybersecurity session, the EO had information that there was this same information sharing discussion of "*Where do you get most trusted information?*" The answer was likely competitors. A few said, "From the ISACS." ISACs have an information infrastructure – and analysts that went above and beyond what the companies could do themselves. They trusted what the information from ISAC, and actionable information from the ISAC that would require sector leads to come together and understand what they want and need.

Mr. Toler is in the process of establishing a set of Blanket Purchase Agreements (BPAs) for tools and services for CDM functions intended for those agencies that have gaps and those that have none and provide the services that would run them. The ceiling is $6B. The intention is for

[2] Circular No. A-130 Revised, Memorandum for Heads of Executive Departments and Agencies – *Management of Federal Information Resources* http://www.whitehouse.gov/omb/circulars_a130_a130trans4

Department of Defense (DoD) and the Intelligence community to use this vehicle under DHS. In addition, state and local government can use it since there is an interest at the state level.

Mr. Toler referred to Slide 6 of his presentation in his discussion on whitelisting and how will it actually work. The baseline is set up, and the tool requires good configuration management by maintaining the baseline, not trying to force it, but simply identifying the issues. The CDM tool will provide the insight to see deviations from the baseline. For example, the dashboard configuration will prioritize the worst offenses from low to high. Each bureau can use its own unique whitelists. Danny Toler pointed out the challenge with whitelisting is what goes on the whitelist and what does not. CDM will provide system automation to Chief Information Officer (CIO) communities, government agencies, and bureaus. Each organization will have to define how much time they need to fix and distribute an incident patch and address intensive processes that will focus on the issues at a management level.

Responding to Board's Remark: To reiterate, if a bureau signs up for the CDM tool, they will be able to feed their whitelist to the tool. Also, focusing on the worst incident first is so important and will help us to improve mitigations. Other information helps with understanding vulnerabilities and information sharing on threats. Do you understand your posture and have you mitigated it in the right way? Mr. Toler pointed to slide 13 in his PowerPoint deck as a reference and explained that every 20 minutes the dashboard cycles and provides a letter grade from A+ to F, which allows the user to drill in and see why a patch was not applied and allows users to focus on activities. The priority of concern can be set by a top level department or agency or by the US-CERT. Setting those values and making those grey determinations will allow the allocation of resources to be assigned to fix the issues.

Lastly, Mr. Toler discussed the implementation timeline which is projected to be completed by FY18; however, it will be functional very soon in FY14. The dashboard features will not have all functions and reporting features quite in place. Sequestration has affected the timeline by limiting the purchase of licenses and pushed their timeline back from FY16 to FY18.

Executive Order (EO) and Legislative Actions

DHS Information Sharing Update

Jenny Menna, Director, Stakeholder Engagement and Cyber Infrastructure Resilience Division, DHS

Ms. Jenny Menna considered main focus on information sharing as critical infrastructures, which included state and local governments. She explained that DHS's first Cyber Security Information Sharing and Collaboration Program, known as CISCP, which is a program that DHS shares with information analysis organizations and with individual companies that either do not belong to an ISAC and/or prefer a direct bilateral relationship with the government. CISCP evolved years ago from a pilot program. Ms. Menna witnessed valuable information sharing being exchanged within this pilot and inclusion of critical infrastructure representatives and representatives from other companies. Based on the representatives' feedback, the consensus suggested a trilateral pilot that involved DOD, DHS, and initially the Financial Services sector to see if a similar construct would work. It was done as a pilot for 18 months and learned many lessons about how DOD differs from Defense contractors: DOD is mainly concerned about information being stolen. A lot was also learned about the legal construct that was made available to all sectors.

CISCP developed a legal tool that is a cooperative research and development (R&D) agreement that covers bi-directional information sharing and identifies what and how information can be shared through the government and private sector.

On whether same agreement is used or each needs to be customized per the agency / organization, Ms. Menna stated that it is a bilateral legal agreement from a standard template, roughly 4-6 pages long. To date, there are 45 signed agreements covering fourteen different sectors although not in their entirety.

Ms. Menna explained that the problem with Cooperative Research and Development Agreement (CRADA) is Intellectual Property, and if shared, it would be community property. It is entirely up to the signer to determine if they want their participation / information to be shared. The CISCP offers automated indicator sharing and are roughly almost at 20K indicators. Information is shared up to 40% from the private sector and 60% from the government. Another part is broader mitigation strategies and a useful collaboration found is analyst-to-analyst communication where there are quarterly advanced threat technical exchanges. These exchanges consist of meetings where speakers can be from the private sector or government agencies, which allows people to have the opportunity to reveal their experiences and may use a traffic light protocol. They can be marked as Traffic Light Protocol (TLP) read, eyes only, amber, or even public information (TLP White), which it seems to work. When information comes into DHS, it is shared with federal agency partners and stripped of CISCP attribution. The information is made available to other <dot>gov agencies through US-CERT.

The machine readability is maturing. This started with PostScript Document Format (PDF) formatting, then Comma Separated Values (CSV) files are being sent, and for a while now in STIX format and also in Incident Object Description Exchange Format (IODEF) format. The portal is used to display data, but some companies are concerned with displaying their participation.

Of the 45 CRADA / CISCP agreements, 12-13 are ISACs and the others are all companies. It is not difficult to get a seat on the Board at this time. While participants are using the US-CERT portal and logging in with tokens, there has been little interest. There is no encrypted email like DOD has. CISCP products are located on the Mercury portal and indicators are located on the US-CERT portal.

In order to coordinate and complement the CISCP program, Enhanced Cybersecurity Services (ECS) is required. ECS was started through a government pilot, was enabled by the EO. This was enabled for CSP (Commercial Service Providers) to provide services to 16 critical infrastructures. CSP is providing data to secure their customers networks. This one-way out-going data is provided from the government once a week and will be changed to twice weekly. CSP can provide data back, such as 75% hit on the indicator. Initially, it was just Internet Service Providers (ISP), it is now open to a broad set of commercial service providers (managed security, etc.), two countermeasures (Domain Naming Service (DNS) Sinkhole and Email filtering) to begin with. Information does not become unclassified and does not leave CSP. Security is maintained internally.

The government does not pay for CSPs to build-out infrastructures. There is no relationship with the purchaser of the service. The operational implementers are in place and there are two pieces: legal and getting it built – a secure facility to handle secure data. If an organization such as a bank wants to buy a service from an ISP, the government has no idea what the ISP is charging the bank. Century Link and AT&T have completed the process, and an additional eight organizations are moving forward. It is a multi-step accreditation process, although it is not known if anyone has turned on the service.

On the topic of measuring effectiveness, the studies were organized on the pilot setup methods for measure. Metrics are being built to determine effectiveness, but it is necessary to have a dialogue on how to shape it moving forward.

If a unique sector is attacked, either government or private sector, information about the act of intrusion will be fed into the CISCP program and participants would receive unclassified information from CISCP program. There will be overlapping information, and those indicators will be found and established uniquely by organizations.

The following reference materials were provided by presenter:

- Homeland Security[3] – CIKR Cyber Information Sharing and Collaboration Program (CICP)
- Homeland Security[4] – Enhance Cybersecurity

Board discussion

The Board will address the legislative proposals with Adam Sedgewick during his presentation on June 13, 2013. In the meantime, the Board would like to discuss on efforts to be directed for the next year and actions to be taken. From previous discussions on FISMA, cloud computing throughout agencies and decided upon automated information sharing as it relates to the EO and it ties into FISMA. The Board explored the next course of actions for the following discussion points:

- It is the intent of this Board to try and bring transparency to information sharing operations and identify gaps. People on the outside have difficulty getting a quality level of security. The Board's ongoing challenge is to determine if they have a good picture. Are there any missing components? How do they increase transparency?
- FISMA and the Inspector General (IG) provide transparency but the driver of Cross Agency Priority (CAP) goals is twofold - drive transparency and prioritization. Public metrics by agency are of utmost importance, and therefore, it is good to maintain consistency of those goals. The Board should pay more attention to these CAP goals or focus on transparency.
- It is recommended that the Board to be updated of GAO oversight as the GAO reports provide good information. For example, the material received for February 2013 was

[3] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_menna_ciscp_one_pager.pdf

[4] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_menna_ecs_fact_sheet.pdf

agencies' compliance with Risk Management was a decrease from 13 last year, which is a valuable piece of information.

- Letters previously sent from the Board re. 1) on security and medical devices, 2) on using outdated software on OS and risks, 3) on information sharing and indicators, and 4) congratulatory note on 800-53R4. The Board's involvement in these discussions seems to have lent a hand in the ability to influence and provide insightful thought, which helps to assist in tying things together. Board's action is not necessarily resolutions but increase awareness.
- The Board would like to hear more about reasonable procedures for incident response and its effectiveness.
- There are lots of activities on information sharing and IR. The Board is interested to look at how/what those activities are and if they can provide any guidance on effectiveness which the Board will be able to provide recommendation on the EO.
- It was recommended to invite the Chair, Privacy and Civil Liberties Oversight Board (PCLOB) to the next meeting. PCLOB is working on building momentum and has a backlog of issues. It needs more visibility and to establish itself outside the White House. The Board should provide that visibility, and would like to hear from them regularly.
- The Board noted that Information Sharing (IS) means a lot but there are IS pockets in agencies, leads of ISACs, sharing between agency Security Operations Centers (SOCs) and CERT, sharing between centers, sharing with the private sector. It is hard to pinpoint on a certain piece of information sharing whether all of it or underground information sharing. There is an amazing set of individual relationships where information is shared without formal mechanisms. It is very fast and valuable, official and unofficial. There are international aspects and law enforcement aspects.
- The focus on IS affects cybersecurity and focuses on federal information systems. Cybersecurity should not be considered in the same way as terrorism.
- Most of NIST's work is technical, and mostly on R&D. Finance sector commands a top 10 R&D agenda. The question is what structures are in place – processes, advisory committees, and for example, how do DHS's cyber priorities engage with the National Science Foundation (NSF). The following suggestions were raised:
  1) Should the Board be more aggressive in identifying other folks who set agendas and priorities?
  2) Are there specific areas or things we would like the Board to explore in R&D priorities and technologies?

  The ISPAB charter is not R&D focused. But the Board would like to explore the processes and structures exist for R&D within the government, effectiveness, contribution to national information security, and the work of the President's science committee.
- The FY14 budget is being planned. The Board could consider building recommendations for FY15 security budget. It could help in presenting to agencies, such as showing the near time challenges they will face in terms of policy and technology that they need to be

ready for, whether security features – challenging from technical point of view or privacy point of view.

- From a NIST perspective – the Board should consider threat environment and trends in information technology (IT) space, including discussions on advances in cloud computing, mobility, and communication.
- It is important for the Board to invite appropriate experts.

FISMA

Perspective from Office of Management and Budget (OMB) and DHS

Dave Otto, Branch Chief for Cybersecurity Performance Management in Federal Network Resilience, DHS [Presentation provided][5]

The Board requested the following discussion points to be covered from the presenter:

- The Board heard at last meeting in February 2013 that agencies complain that OMB guidance comes late and thus their data call is frenzied. Is this truly the case, and if so what can be done to get earlier, clearer guidance on OMB policy?
- How can FISMA be more outcomes-based? Since DHS directs what to measure, and can they give more guidance on actual metrics?
- Can DHS direct & give more guidance on metrics?
- DHS & OMB, who drives what during this process, where does handoff occur?

Mr. Otto addressed the OMB memorandum M-10-28 that clarified the respective responsibilities, activities of the OMB, and DHS duties (please see slide 3). This memorandum created the authority for DHS to develop the mission in respect to federal agency policies and FISMA guidance, as well as oversee cost-effective cybersecurity solutions. The main directives that support the DHS cybersecurity operational activities include tools and automation (a cyber-scope tool that includes auditing). The CyberScope supports approximately 4 million assets that are reported on each month, and about 2 million that are only providing UCCB, CBE, and CPE from DOD. In terms of maturity, this is situational awareness. The tool does not have a feed down to the asset or component level. Some agencies have a clue into their vulnerability based on out-of-service servers that are reaching their end of life.

Mr. Otto stated that there is no metrics on those out-of-service items and there is some fluctuation with those numbers. There are a lot of operational issues with the system continually maturing. For example, they are looking at content as well as the number of indicators specified and reported on. The future direction with FISMA A130 and revision updates are intended to be added components to this process that will complement each other. The intention is to combine the direct FISMA questions with the data collected. The data is available but may have to be validated. When FISMA is used, the data captured is at such a high level that it loses all resolution. Better information is provided through the Change/Configuration Control Board (CCB) so why isn't CCB data used? This is being adopted as a data collection analyst principle and research process. The idea is to utilize all captured information and focus on automatic feeds

[5] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_fisma_perspectives_from_omb_dhs.pdf

as much as possible, after which move on to focus on the validation process, whether it is the CCB or another form of validation. There is good visibility into agencies, and the FISMA report could be used as a validation method. The concept is to present what is known and validate it, and the outcome would be to have a better footprint or understanding of situational awareness.

They also provide operational guidance on enterprise awareness with OMB. A common misunderstanding is that DHS is not superseding OMB regarding FISMA guidance. However, DHS and OMB develop guidance titled Federal Information Security Memoranda (FISM). In regards to a question of whether the guidance is difficult to understand, it is acceptable that some of the questions are difficult to understand. For example, there are limited people within an organization that understand the questions asked and the person who receives the metrics and possibly the right contact may not be able to understand the metrics. Mr. Otto emphasized that it is important to maintain the baseline as any changes even slightly on the FISMA report have to be weighed against its validity. Baseline metrics are the DHS metrics, which are critical to cybersecurity.

There is consideration to help agencies by removing at least 20% of the questions. Some agencies want to know what adequate metrics are; however, each organization must come up with its own baseline metrics. Companies and agencies are turning to the government for directions and provision of adequate metrics. In regarding setting metrics based on SP 800-53, SP 800-53 is considered as a baseline but it is a technical guideline and should not be considered as baseline metrics.

The relationship between Inspector General (IG) with CIO reports is that IGs go online and download the public report in order to map questions together. It is Mr. Otto's belief that FISMA was not envisioned as the modern security technical component.

On whether reducing the amount of questions on FISMA (GAO report)[6] will increase compliance, Mr. Otto emphasized the importance of understanding and clarity could help. However, it would fully take agencies out of noncompliance issues.

Concerning the usefulness of the FISMA reports and the appropriate action to address security, Mr. Otto did not think FISMA was not originally designed for federal IT security constant monitoring.

FISMA

FISMA and A130 Appendix A – OMB circular update

Emery Csulak, Deputy Chief Information Security Officer, US Department of Homeland Security

In his opening remarks, Mr. Emery Csulak emphasizing a single factor with A130 is that agencies and departments consider A130 as an obstacle for information security and cybersecurity. However, A130 is re-enforcing FISMA guidance. Prominently, the guidance supports a risk-based approach in terms of interpretation. Unfortunately, not everyone takes a risk-based approach or they only take one interpretation which creates a lot of conflict.

[6] http://www.gao.gov/products/GAO-13-187

Mr. Csulak predicted future conversation between agencies and DHS to be with or without the updates of A130. NIST has done a great job of putting out supplemental information in regards to continuing monitoring, ongoing authorization, and security control testing. But in order to streamline that conversation, NIST will need to provide many more guidance. The main challenge is how agencies interpret the guidance and the biggest challenge is to get everyone to speak the same language in the discussion. They are trying to establish a road map that is an example for a constructive conversation with the Office of the Inspector General (OIG), GAO, and partners in the mission to make this a more positive experience. There is a lot of misunderstood information in A130. For example a common misinterpretation is that 100% of controls have to be tested, which is not accurate. Some 100% of controls have to be considered and application should be set by risk-based determinations. There is a lot of additional guidance that will help to tailor the process.

When bringing in standard processes and experienced staff to an agency, turnovers affect the interpretation and the standardized process can be compromised with arrival of new people. There need to be at least one or two key people in each department to maintain continuity and smooth flow of the standard processes. The security posture sustained through the International Standards Organization (ISO) plan. In addition, the authorization should be changed. Once authorized, the plan should be changed from testing every 3 years to conducting it daily. There are few lessons learned from the feedback from IG and GAO. It is included in A130 guidance for elimination of 3-year testing eliminated and turns into daily best practice. This is a key part to the methodology and it is important that people use and implement it. Examples from NIST should be used as they meet A130 compliance. Triggers are either event- or time-based. A process and a frequency approaches are needed. This should not be done in a vacuum.

The meeting recessed at 4:10 P.M., June 12, 2013.

Thursday, June 13, 2013

The Chair reconvened the meeting at 8:07 A.M.

Continuous Monitoring and its Ability to Create Efficiencies
Automated security indicators – many different investments in standards and sharing mechanisms

Phyllis Schneck, (Moderator), VP & CTO, Public Sector, McAfee, Inc.
M. Lee Badger, Computer Scientist, Computer Security Division, NIST [Presentation provided][7]
Kent Landfield, Director, Content Strategies, Architecture and Standards, McAfee Labs
Kathleen Moriarty, Global Lead Security Architect, Corporate Office of CTO, EMC
Richard Struse, Deputy Director, Software Assurance Program, GCSM, National Cybersecurity Division, DHS

This session focused on the discussion and debate on Information sharing and automated security indicators. The main question becomes how do you successfully share information and what do you gain from it? Mr. Badger began the discussion by explaining his recent projects at NIST, which includes updating guidance from DHS on incident response. This project considered how incident response could be performed more effectively and a standard created. An ecosystem that has some standardization is needed. However, people do not want to be regulated and be restricted by standardization. There are indicators that are part of an event and have information on the context of that event. Richard Struse from DHS offered more details on what those automated indicators specifically are related to Trusted Automated eXchange of Indicator Information (TAXII)[8] and Structured Threat Information eXpression (STIX).

In response to Board's question on where in the information world does sharing of indicators, Ms. Moriarty stated this is a critical stage with information sharing that can change and have a big impact, specifically on the broad dissemination of data. There should be less focus on broad dissemination and focus instead on redirected ways of exchanging information.

Mr. Landfield stated that there is a role for US-CERT incident response, but if we know about a response, we are already too late. It is a diverse ecosystem so cybersecurity needs to be provided on different levels to help prevent incidents. It is necessary to respond rapidly in this ecosystem so that we will be able to move with some agility.

Mr. Struse added that it is essential to use other forms that are more automated and not human-based than PDFs (Portable Document Formats) and word documents. Ecosystems will grow over time. The capability to do analytics is there and something proactive is desired. The incident is useful until someone is compromised. Define level of data and trust for sharing before laying foundation and build on top of it. There are malicious download sites so it is necessary to prevent the user from accessing those sites.

[7] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_badger.pdf

[8] https://www.us-cert.gov/sites/default/files/gfirst/presentations/2012/enable_taxii_struse_barnum.pdf

Ms. Moriarty stated that we need information sharing standards and an international standards focus; for example, the Organization for the Advancement of Structured Information Standards (OASIS) group, which is a common alerting call. They took a large framework and applied it on a small scale. This group took the international standard and this maximized multinational awareness.

Mr. Badger added that infrastructure, the development of the framework, is something to be aware of. There are many ways to communicate but the hard question is which group should be responsible. These groups are not defined in the organization. Furthermore, it is usually just someone in the organization that verifies the information is correct.

Mr Badger agreed that there is a data quality issue, and it is difficult verified. An attacker can see what we can see. For example, your server is deciding what information we are getting through our email. Also, browsers are accessing dangerous site and also acts differently.

When the Board asked whether we could use the indicator before it affected anyone, Mr. Struse explained that part of the problem is finding the indicator before it hits and becomes a problem. We need to think about the event that created the indicator and try to prevent it. Sometimes it takes an attack to see where we are, if we can make the attacks that are happening more meaningful, we can help others.

Mr. Landfield added there is a trust group working on finding incidents today; however, bad guys could potentially be in some of these information sharing networks. Different organizations will have to know that we are dealing with diverse information.

Dr. Schneck asked the panel, "We've talked about models, but is there one large weather map or are we at an embryotic phase with security indicators and standards for incident responses?" For which Ms. Moriarty responded that we should redefine the current information sharing processes and have trusted groups as well as have standards that are continually evolving. We do not have to go out and track everything; for example, this is why blacklists have gone away. This Board has a great opportunity to help define this process.

Executive Order (EO) and Legislative actions

EO Cybersecurity Framework – status of Request for Information (RFI), Notice of Intent (NOI) feedback

Adam Sedgewick, Senior Information Technology Policy Advisor, NIST [Presentation provided][9]

Mr. Sedgewick presented the status and progress of the EO (EO: 13636[10] Improving critical Infrastructure Cybersecurity) status. The focused efforts are on following two main pieces (see Presentation):

1) Sharing of cybersecurity threat information

[9] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_sedgewick.pdf

[10] http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

2) Building a set of current, successful approaches—a framework—for reducing risks to critical infrastructure

- NIST is tasked with leading the development of a "Cybersecurity Framework" – a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

The main focus areas are of information sharing from government to industry and a Cybersecurity Framework that includes a set of standards that broadly define methodologies. A RFI (Request for Information)[11] for this framework was released on February 26, 2013[12], and a draft framework[13] was subsequently developed. A total 244 responses were received. They have to work with an aggressive timeline (see PowerPoint slides). The output of every workshop becomes the input for building the next workshop. Presently, they are preparing for 3rd Cybersecurity Framework Workshop, July 10-12, 2013, San Diego, California, which is directed to define framework components.

One of the challenges at the 2nd Cybersecurity Framework Workshop, was to get everyone on the same baseline for a cohesive and effective communication. As described in the development overview, there are four planned workshops, and the intent of the workshops is to achieve true working / interactive sessions.

Mr. Sedgewick submitted that there were noticeable gaps in the RFI – beginning from scratch perspective and also the mitigation process. He indicated that they have noticed gaps during EO briefing. It is more of a sector area and they are looking at more of an organizational level.

Adam Sedgwick also agreed that the focus should be on an enterprise and not sector-wide. The problem once sector-wide plan is laid out, it rolls up to the enterprise and organization levels and there will be little push to drive into the field. Mr. Sedgewick explained the framework process as grouping the RFI responses and looking for commonalities. The EO is also committed to protect privacy and civil liberties through a transparent process which will require working with those groups.

Key principles outlined in the presentation derived from the EO include comment points, understanding the threat environment, risk models, levels of maturity, incident responses, and cybersecurity. Initial gaps include metrics, privacy, tools, industry best practices, resilience. In two weeks, they are going to present a draft document that will identify those common practices and present common practices such as methods and measures at a high level. They will present a framework[14] that is useable, clear and unambiguous, and suitable for multiple audiences. There will sufficient time to have a public mailing, and follow by third workshop[15].

[11] https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity

[12] http://www.nist.gov/itl/upload/cybersecurity_framework_presentation.pdf

[13] http://www.nist.gov/itl/upload/draft_framework_core.pdf

[14] http://www.nist.gov/itl/upload/draft_outline_preliminary_framework_standards.pdf

NIST Update

Matt Scholl, Deputy Chief, Computer Security Division (CSD), NIST

Mr. Scholl reported that Dr. Gallagher, Director, NIST, is now the Acting Deputy Secretary of Commerce while Dr. May, Associate Director for Laboratory Programs, will be filling in for him while he is in Congress. Dr. Gallagher has two things that he would like to address in Congress:

1) The Advance Manufacturing Initiative, which is a presidential initiative
2) The Executive Order

Mr. Scholl reviewed some items that have happened since the last ISPAB meeting. He described CSD's activities by events, workshops, publications and reference materials published, and anticipated activities before the next Board meeting. Mr. Scholl also discussed some of the budget effects in their division.

NIST held an event in January called the Trusted Geo-location in the Cloud. This entailed working with a program called Trust Routes, which looks at hardware-based cryptography that holds values and can that be used and pushed up to a higher − possibly a Cloud − level. They brought in some venders with Intel technologies (PXT), who conducted some small-scale demos of enforcing policy in the Cloud. Some of the considerations are where can workload and data be constrained and where can workload and data be isolated. They are extending this work.

They had series of mobility workshops that meet with DHS, Department of Justice (DOJ), and the White House on mobility and the workforce. It is called the Federal Mobility Technical Exchange and they are gaining agency support.

In DOD, they will develop a series of Defense Advanced Research Projects Agency (DARPA) model apps that address access as well as some infrastructure standards for initial use for the government. They have been working to demonstrate different security models. They organized various workshops such as federal, cybersecurity, and with Health and Human Services, to establish trust in the workplace. People use trusted sites and CERTs (US-Computer Emergency Readiness Team)[16].

CSD put out a draft of best practices for CERTs (Trusted Routes) and continued on to forming a program to attribute an access control mechanism that will automate CERTs. A workshop was organized on June 17 for this discussion as well as to discuss small technologies and proof of concept.

Mr. Scholl directed his focus on publication updates. He described those publications that were completed as follows:

- Authentication Guideline (SP 800-63[17]-2, Electronic Authentication Guideline

[15] http://www.nist.gov/itl/csd/3rd-cybersecurity-framework-workshop-july-10-12-2013-san-diego-ca.cfm

[16] http://www.us-cert.gov/

[17] http://csrc.nist.gov/publications/drafts/800-63-2/sp800_63_2_draft.pdf

- FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors – which was a draft at the time of the meeting but was approved and published in September 2013.
- SP 800-73-4 (Draft)[18], DRAFT Interfaces for Personal Identity Verification (3 Parts) – Part 1: PIV Card Application Namespace, Data Model and Representation; Part 2: PIV Card Application Card Command Interface; and Part 3: PIV Client Application Programming Interface
- There is also another PIV document, SP 800-74 under development
- In addition, an update for the cryptography used on PIV cards document draft, which will be released in the near future an update for the Entropy Sources Used for Random Bit Generation, SP 800-90B[19], DRAFT Recommendation for the Entropy Sou7rces Used for Randon Bit Generation
- SP 800-53 Rev.4[20] Security and Privacy Controls for Federal Information Systems and Organizations
- SP 800-82 Rev.1[21], Guide to Malware Incident Prevention and Handling for Desktops and Laptops

Currently, they are looking at updating the risk modeling documents on how their risk management can be leveraged. Whitelisting seems to be relevant for the National Cybersecurity Center of Excellence (NCCOE) and in Research and Development (R&D) in the crypto space (sponge function).

Other research areas include cyber physicals, which is directed at smart manufacturing and it is being extended. There is a question of how released guidelines can be extended, and sequestration did impact this area. NIST did experience an incident, and after a root cause analysis found that they were subject to a zero-day exploit from an Adobe application. The Information Services group patched it within a week. The exploit was not intended for NIST.

NIST is coordinating with Japan and Europe to work on the next generation data model. New technology systems are anticipated to support Cloud-based services.

[18] http://csrc.nist.gov/publications/nistpubs/800-73-3/sp800-73-3_PART1_piv-card-applic-namespace-date-model-rep.pdf

[19] http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90b.pdf

[20] http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf

[21] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf

Continuous Monitoring and its ability to Create Efficiencies

Reduction of Reporting wherever possible

Earl Crane, Director for Federal Cybersecurity, National Security Staff, the White House [Presentation provided][22]

Mr. Crane talked about continuous monitoring and reduction of reporting together whenever possible. It is his philosophy to reduce human-driven processes and improve cybersecurity. An important question when thinking about this is "Are we more secure today then we were yesterday?" The challenge is on your metrics and who is on your network, what is going in and out of your network, and finally, knowing your state of security. Patching is a tactical element and also hard to manage. If measurement cannot be defined, it cannot be reported. The challenge is compliance-based security having to do with checklists for security rather than looking at risk-based approaches. For example, audits can be based on risks. Internal audits will determine your risks.

Mr. Crane has not seen a justified way to define security. Security is the mission objective; it is the means to get mission objectives done which puts the right end goal. The purpose is to enable the mission, generating value, driving efficacies through cloud computing. Security to be effective cannot be obtrusive, obvious, or restrictive. Prioritizing and specializing is important. If everything is a priority, nothing is a priority. Within those priorities, not all priorities are equal – due to confidentiality.

NIST Risk Management – SP 800-39[23], *Managing Information Security Risk – Organization, Mission, and Information System View* – Are we doing the right thing once we set the measures with the right outcome? There are three priorities:

(1) Trusted Internet Connections (TIC) - consolidate external Internet traffic and ensure a set of common security capabilities for situational awareness and enhanced monitoring TIC.2.0.

(2) Continuous monitoring of federal systems.

(3) Strong Authentication: Homeland Security Presidential Directive 12 (HSPD-12) provides for common identity for building access.

A PIV card is just a container with multiple ways to get access. Although it is a good technology, PKI (Public Key Infrastructure) credential is an old technology. The PIV card is just a container of that initial idea of trying to understand where we are. We need a real time reporting model for security. All of those controls have to be done, but you can assert their functions.

In order to get CSOs to make better decisions oriented with output risk-based assessments regardless of the size of the organization and culture, the challenge is finding right controls to perform. By focusing on finding the rights controls, the advantage is once we have them, we can focus on monitoring and control. The next step is to minimize and specialize by focusing on the capability not the control itself. It allows people to focus on larger areas such as cloud computing, by moving towards visibility. OMB and DHS collect the information and report it to

[22] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_crane_reduct_reporting.pdf

[23] http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

the public, which improves visibility. The third part is specializing or focusing on key areas, minimizing these priorities. This elevates responsibility outside the CIO shop, moving it out of the CISO and into the Operations shop. This moves the accountability under FISMA to the agency head that is designated to ensure compatibility.

Mr. Crane anticipates that there will be need to increase cybersecurity as changes in technology, and changing ways in which an agency prioritizes. The important element is not changing goals as we move toward maturity. In an effort to understand the maturation of an agency's processes, all agencies provided updated performance plans (USG CAP)[24]. Based on the performance plan, it is to drive the agencies to do better in their performance. In order to maintain that momentum, it is necessary to push outcome-based metrics to maturity-based metrics. The administrative priority is performance management, to have a minimum level of "*yellow*" and not to "*Red*".

Overall Government Security

Vision of future of "<dot>gov" Network 2020/MTIPS/TIC

Earl Crane, Director for Federal Cybersecurity, National Security Staff, the White House
Tim Polk, Computer Scientist, NIST

Mr. Polk spoke of the current state of the ".gov" internet at large. His views were pessimistic in the short term and optimistic in the long term. In the .gov domain, services being offered could not have been done a couple years ago. However, it does not look like it is sustainable for security such as identity theft. There are vulnerabilities. The internet was designed by a small group of scientists together, and not expecting the security issues that we face today. All the attributes that people love about the internet ─ trying to achieve the level of security that people think they want has been a true challenge. Some parts have not been met. However, Mr. Polk is optimistic because there has been an attitude shift with deciding that cybersecurity is important. The federal government is very interested and trying to create R&D programs. The question is "what do we need to do to get better?" – These are pieces that you will find in the R&D strategy December release – R&D opportunities make a difference:

- Have a whole domain approach that cannot be handled with the host, and to move to network functions.
- Have to create new demands with the host, domain, network, and user. Hosts will have to really determine whether their security is appropriate for their environment, another host on the internet is not good enough.
- Users are going to need better tools – answering those fishing emails – we have never given the users proper tools.

Industry is doing a better job in adopting innovations than the federal government, e.g. cryptography. Basically we need to do this to establish immunities. Networks are going to need to provide better infrastructure.

There are a number of concerns:

[24] http://goals.performance.gov/content/cybersecurity; http://technology.performance.gov/initiative/ensure-cybersecurity/home

- Many ISPs are not doing what they should be
- We unable to do what we already know.
- Improve on sharing information for detecting risks in the security posture. For example, mobile phone security − using the users.
- Millions of sensors are not being utilized.
- Maximize advantages of R&D and situational awareness.

The Board noted that system administrators often do not know how to install security. Mr. Polk stated that users need to be more educated, and at the same time, should be given the proper tools. The government needs to improve on connecting information sharing which resulting in improving security and privacy while not compromising information. He is optimistic for the future because we have some of the right R&D strategies. We should start on Internet Protocol Version (IPV). One of the ideas may be IPV6, which has to become the focus for rolling out this domain. This would be a quantum leap, but may lead to a safer environment.

The industry moves faster than government, and industry as compared with the government is by nature completive. The Critical Advisory Committee for the President is focusing on economic driving factors that consist of three areas:

- Human factor – Teaching and providing the proper tools to enable success in protecting information and security practices
- Organizational Structure – Where in the company is the right place to focus on cybersecurity? Who is the proper authority?
- Technologies – Cloud computing solutions

Board Discussion

Questions to consider:

- Cybersecurity:
  - When discussing cybersecurity, it is not clear how it is going to be done?
  - Why don't they just do it if someone knows how but who would that be? As a good practice, we should default to industry for guidance or turn to agencies that are setting good examples, such as the NIST prospective. Also, it seems that cybersecurity has occupied a small part of the agenda for government agencies – how do we increase the situational awareness? One approach could be to talk to the agencies. We should think about this and possibly come up with actions steps before we invite anyone to ISPAB meeting.

GAO Reports

Gregory Wilshusen, Director, Information Security Issues, Government Accountability Office (GAO)
Eileen Larence, Director for Homeland Security and Justice issues, Government Accountability Office (GAO)

(High Risk Federal Systems, Cybersecurity report, other "national strategy needed", info sharing reports)
National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented

GAO-13-187,[25] *A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges*, February 14, 2013
GAO-13-462T,[26] *Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities*, March 7, 2013
GAO-13-471,[27] *Additional Actions Could Help Ensure That Efforts to Share Terrorism-Related Suspicious Activity Reports Are Effective* [Reissued on March 26, 2013], April 4, 2013
GAO-13-233,[28] *Information Sharing – Additional Actions Could Help Ensure that Efforts to Share Terrorism-Related Suspicious Activity Reports are Effective*, March 13, 2013

Mr. Gregg Wilshusen and Ms. Eileen Larence discussed some of the GAO reports and their findings. Mr. Wilshusen will discuss GAO reports: GAO-13-187, GAO-13-462T, GAO-13-471 and Ms. Larence was to present review on report GAO-13-233 from a national cybersecurity strategy. There were two reports specifically on cybersecurity strategy; one was a report and the other was a testimony which basically summarized the contents of the report. The two reports (GAO-13-187 and GAO-13-462T) were under the authority of the Controller General and the reason these reports were generated was because federal information sharing had been identified as a high risk area nationwide since 1997 and in 2004 included security over critical infrastructure. The Controller General commissioned an audit and wanted the team to look at "Why this is the case" and "What are some of the unknown challenges federal agencies face." The reports were based on two objectives:

1) Identify the challenges faced by the federal government in addressing a strategic approach to cybersecurity
2) Determine the extent of the national cybersecurity community key desirable characteristics.

IG reports from different agencies were reviewed and officials at key government agencies were interviewed. The officials were with government-wide responsibility components like security,

[25] http://www.gao.gov/assets/660/652170.pdf

[26] http://www.gao.gov/assets/660/652817.pdf

[27] http://www.gao.gov/assets/660/653527.pdf

[28] http://www.gao.gov/assets/660/652995.pdf

DOD, MITS, Executive Office of the President, OMB, Office of Science and Technology Policy (OSTP), and National Security staff. Two cybersecurity panels were created and surveyed. The panels comprised of cybersecurity and private industry experts and CIOs from 24 agencies which were covered by the CIO act. Strategy documents that had been issued by the federal government were reviewed. Once the information was gathered and analyzed, they found that there are still a number of challenges that confront the federal government. Working with agencies to design and implement a risk-based cybersecurity program would be beneficial because there were agency weaknesses found in configuration management, segregation of duties, and security management. For example, 19 out of 24 agencies reported that information/security controls were a material weakness for financial reporting purposes as part of their audit and financial statements. Mr. Wilshusen predicted that any large public company would necessarily do better but he does not have clear data to support a public company audit.

In compiling the reports, they did audit other agencies and noticed similar weaknesses in their security vulnerabilities as the executive branch agency findings; however, some agencies have shown improvements. It is assumed that they may have more leeway in the allocation of resources in funding and implementing security.

Also, out of the government agencies, 22 out of 24 IGs at each agency cited cybersecurity as a major challenge. They also looked at how well agencies are using their resources, and agencies that have sufficient budgets to acquire technologies and systems for corporate resources. Some of the data collected also focused on basic IT security and management of current systems and maintaining those. A few other challenges found were:

- Identifying standards for critical infrastructures - The President issued an executive order helping to establish a framework of cybersecurity that touches on standards and also detecting and responding to cyber incidents.
- Promoting education awareness and workforce planning within the federal government on general cybersecurity issues. There should be funding in cybersecurity in research and development. There is not a mechanism to support government agencies to support cybersecurity sharing.
- Securing the use of technologies was also a challenge.
- Managing the risk of the global supply chain.
- Addressing the international aspects of cybersecurity.

Lastly, national strategy documents were compared to attributes in the findings and useful and effective strategies were identified, such as: Does it define the problem? Does it identify the goals and objectives? Does it have a risk assessment process? Does it identify performance measures, roles and responsibilities, and resources that implement those strategies? Does it link up with other strategy documents? It was found to a large extent within specific organizations that roles and responsibilities were not defined nor had they the resources necessary to implement the strategy.

Ms. Larence stated they had been looking on how information could be shared across federal agencies and had been taking a comprehensive look at working with agencies to identify next steps and remaining gaps. They looked at intelligent sharing within the intelligence community

and were looking at DHS intelligent analysis and doing work with the private sector. The federal government is starting to take a look at its domestic intelligence with questions of the joint task forces included what are they and what are they doing. They looked at five field-based entities that were high-intensity intelligent based centers and then examine regional information sharing centers. Basically, they all were generated on their own but overlap was a concern. While it is acceptable with some overlaps, but overlaps could create inefficiencies. Federal agencies have expertise, but they are not holding responsibility.

Finally, performance data was not to be factored in, only to be captured. Some agencies have reservation and resistance. They are looking for ways to provide incentives for GAO-13-471 Report. The Federal Bureau of Investigation (FBI) does have a way that can link information if the report is part of a terrorist attack. However, these reports were not being passed on to the FBI. They have not been tested. They are behind in their training.

The meeting recessed at 4:32 P.M., June 13, 2013.

Friday, June, 14, 2013

The meeting resumed at 8:07 A.M.

Ongoing Authorization via Tools

Jeff Eisensmith, CISO, U.S. Department of Homeland Security [Presentation provided][29]
Melinda Rogers, Acting CISO, U.S. Department of Justice

Mr. Jeff Eisensmith discussed the potential of automated tooling in lieu of or replacing some reporting. He emphasized there is a real need to change. He continued by saying maybe FISMA made sense ten years ago but it is not applicable to the way it is being done today. Since December, a group was established to explore possible changes to ways things are done. The Federal CIO office and the White House are both behind this. They met with GAO and DHS, and the group agrees that NIST has been a great example and they are in support of NIST. This brief is about ongoing authorization on why and how it is changing.

Ms. Rogers's explained authorization as it was essentially putting an authorizing official or executive on the hook to authorize any needed system changes. If there is a change in a system, it is having them acknowledge and take ownership of any risks related to that system.
Jeff Eisensmith added that a sense of nervousness is encouraged for the authorizing official because they control the budget and the resources. In addition, awareness should be recognized.

Mr. Eisensmith emphasized that continued monitoring in cybersecurity is a huge deal. Every federal agency now goes before the White House and takes their business course. The White House is tracking those metrics, which allows visibility into each agency. As CDM gets rolled out, it is easy to see the granularity and really start to understand the security posture, i.e. what is being measured and completed. When considering tools, the idea behind it is the concept of inheritance. In order to authorize a system a while ago, you had to test every control while the system is located in a data center. However, from a security standpoint you will now be able to inherit those controls. So the idea is the system can start focusing on smaller things. We are progressing from being responsible for doing everything to a system to inheriting the systems. In working with tools, if any one of those inheritances has a problem, it is expected that our security risk posture will change in near-real time. The main thrust is to use what automation available. Mr. Eisensmith stated that the Operation Risk Management Board can be created and that this is an environment in which diversity is essential. It consists of people from the network operational center, ISO, and information system owner. They would decide of those remaining controls, where they are going to put resources.

The Board asked about dealing with dependencies since the power of inheritance relies upon the strata beneath it and they do not own those controls. Mr. Eisensmith stated that the ISO Control Board will happen in the CCB and everyone has the visibility to see the data. Changes can be detected and will be known. Ms. Rogers stated that it is not possible remove human element/involvement. It is also about the people, and the ISO Board will rely on the people as well to find out the reports. Mr. Eisensmith referred to Slide #5 of his presentation where

[29] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_eisensmith.pdf

controls should be as an example. It is essentially be able to tailor controls based on requirements.

On whether this methodology can be applied to smaller companies, Mr. Eisensmith stressed that these pilots were created to share with the world. It is necessary for us to be an example, although this might not be the best approach for small business.

In closing, the panelists requested the Board to be a good sounding board to get the information out and possibly remove the 3-year A130, or eliminate or rewrite it.

Update on FedRAMP

Matthew Goodrich, Program Manager, Federal Cloud Computing Initiatives, GSA [Presentation provided][30]

Mr. Goodrich explained that FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for Cloud products and services. It is not an unfounded 800 series document. Mr. Goodrich referred to his presentation in review of his brief:

FedRAMP Policy Framework:

- Agencies leverage the FedRAMP process, heads of agencies understand, accept risk and grant ATOs
- FedRAMP builds upon NIST SPs, establishing common Cloud computing baseline supporting risk-based decisions
- OMB A130 provides policy, NIST Special Publications provide a risk management framework
- Congress passed FISMA as part of 2002 e-Government Act[31]

Mr. Goodrich stated that following the NIST SP 800-37 is a good template for the FedRAMP process. All NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*[32] categories map to FedRAMP standards. FedRAMP also considers cloud from the perspective of a 3PAO, which is a third-party assessment organization perspective.

In response to Board's question as to which agencies should use FedRAMP, Mr. Goodrich stated that agencies must default to cloud related products and services when spending any new money on IT. This included new services and additional services. Agencies must justify to OMB when a cloud provider is *not* selected.

[30] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_goodrich.pdf

[31] http://www.whitehouse.gov/sites/default/files/omb/memoranda/m03-18.pdf

[32] http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

Mr. Goodrich stated that many cloud vendors are new to FISMA and it takes time to meet federal requirements such as:

- Clearly defined boundaries
- Federal Information Processing Standard (FIPS)140-2 encryption
- Authenticated scans
- Remediation of vulnerabilities
- Multi-factor authentication

Some venders are having a problem with defining their parameters. While cloud is not a new idea, it is simply a new term. The authenticated scans are important because we do not allow any high vulnerability, but some providers are reluctant to giving information to the government. FedRAMP is not an easy but rigorous process that requires some time to implement. This is still efficient but it takes a long time.

The Board asked if it is possible that agencies will be able to meet FedRAMP compliant by reusing products. Mr. Goodrich stated that FedRAMP is instrumental to NIST 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*. FedRAMP provides a standard but the security process may involve spending a bit more money.

Mr. Goodrich continued by explaining that the authorization process for FedRAMP requires six months. Everything is gone through to make sure it is on par and all supporting documents are available. It all has to be complete and thoroughly reviewed by many people. This will be a repeatable process. A Joint Authorization Board (JAB) is one of the reviewing parties, which requires 14 weeks for agencies with a cloud provider. JABs has very low requirement for continuous monitoring.

The Board asked if there are any differences for an agency to use FedRAMP template stored in the repository. Mr. Goodwich stated that when Department of Health and Human Services (HHS) came in, all supporting documents and controls were checked from a JAB risk perspective. By looking at the changes, 40 controls were lost and 43 added. There are a lot of controls to review, controls that are truly cloud-specific. This is a good time to go out and get feedback.

With regards to chain management, it is necessary to see if A130 is going to be rewritten. In his opinion, it will not be done in a static environment since there were 40 new controls in the first year. We will see if the analysis plays out the way it was intended for SP 800-53 Rev.4. Also, Third Party Assessment Organization (3PAO) Privatization, the group at NIST can help others. GSA will have someone evaluate it. There will be 20 small and large companies consisting of the 3PAOs. GSA has already done its review and is clearing out the application queue with agencies. Mr. Goodrich emphasized that continuous monitoring and reauthorization be followed and not to create new requirements which can be problematic.

Public Participation

Debbie Taylor, Principal, CyberZphyr, LLC [Presentation provided][33]

Ms. Taylor explained that when she attended the NIST workshops for Cybersecurity Framework, she was entirely clear on the intention of the workshops. It seems that Industry did not understand the process of the workshops. In discussion with other attendees, she realized that not many people actually read the material before they attended the workshops. The attendees seemed to view the workshop as a conference and not a working meeting. The sharing of contribution has to come from people that matter. It is recommended to ask attendees to be familiar with required material so as to be prepared as active participants and not as observers.

Board Review of the Meeting

Board Discussion

The Board reviewed the agenda discussions and each session discussed over the past three meeting days to discuss actions, comments, topics moving forward, and preparation for next meeting.

- The Board approved to February 2013 meeting minutes.
- The Board was in agreement that the information sharing on indicators was insightful information.
- A suggestion was made that it might be helpful to invite DOJ again for additional insight.
- *FISMA Presentation*
  - The Board is interested in hearing Mr. Otto's data that he has collected, which would provide good feedback of current government agency statuses.
  - Follow-up comment – Use the FISMA process and review, prioritize, remove, and score questions on relevance.
  - Flagging a comment – DHS – In regards to training IGs, is there a systematic way to train the auditors? For example, can we make a recommendation to the IG academy that would assist in specific training for a risk-based approach for IGs? The academy is funded by the IG community so it is not clear whether it would be appropriate to make a recommendation.
  - The Board stated that there is a lot of dashboard documentation on OMB. They may want to review the reports for this year to see: 1) the current status on each agency; 2) the barriers based on what OMB is proposing to deal with everyone being in the "Green," and 3) what are they doing with the information that they are capturing moving forward?
  - FISMA A130 is seen as an obstacle from agencies:
    - The new A130 is due to be released before the next October meeting so it was suggested it be reviewed by the Board.

[33] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/public-comment_dmoore_2013jun14.pdf

  - The Board may be able to make a recommendation on the revised A130 after a review of the updates.

- *Automated Security Indicators*
  - Focus on ways that will find a good balance between humans and machines.
  - The Board pointed out that there were absences in the NIST players who were essential to the framework (from a structural standpoint).
  - The Board proposed an ISPAB draft letter on the NIST Framework process as a good example and feedback to the White House – waiting for approval from the Board.
- *GAO Reports*
  - The Board suggests that the GAO data was valuable and is interested in seeing representatives brief the Board on a continuous basis. The Board is interested in seeing reports on:
    - Information Sharing
    - Ongoing Authorization
- *FedRAMP Presentation*
  - Focus on how they control turbulence and map it
- Consider having the Privacy and Civil Liberties Oversight Board (PCLOB) to attend the next meeting in October 2013.

CAP Goals[34]

Matt Scholl, Deputy Chief, Computer Security Division, NIST
Lawrence Hale, Director, Center for Strategic Solutions and Security Services, General Services Administration

(There are the major agencies is GSA, DHS (Danny Toler) / Contributing agencies NIST. Facilitating agencies)

Mr. Hale explained that PIO (Performance Information Officers) from OMB have a top-down perspective that allows logical access within GSA (FedRAMP) within federal agencies. It is not the job of Office of Federal Procurement Policy (OFPP). The Federal acquisition office is the procurement for agencies and leverages the buying for the government. There are two programs for U.S. access in government agencies − PIV cards and HSPD-12 (reference www.fedidcard.gov for the latest statistics). They handle the enrollment, reissue, and maintenance of these two programs. They are the second largest facility that issues PIV cards under DOD. They use government and DOD credentials.

The Board noted that agencies have difficulties issuing PIV cards to everyone PIV cards. They would like to know of issues relating to Medicaid cards and using SSN. The Board also remarked on a report that was sent to congress that they are in fact moving away from use of SSN.

[34] http://my-goals.performance.gov/sites/default/files/images/Cybersecurity%20CAP%20Goal%20-%20FY2013%20Quarter%201%20Update.pdf

Mr. Hale stated the initial focus was to issue PIV cards. Washington DC is the focus, then some urban areas, and U.S. prisons, which have employees in every state. They had to come up with an enrollment standard and a unique authentication process. A RFI is currently out (third generation is coming to an end next year). There is no intention to replicate what they have now, but it is to recognize and encourage that their customers are moving to mobile devices. For example, how many are people are using their access to federal networks? Many agencies use two forms of authentication – using the PIV (PKI) card and using it as their power in the card to the network. Also, TIC (Trusted Internet Connections), the government is reducing the number of connections to improve monitoring them. DHS owns the requirements for TIC and they have implemented the standard. GSA stepped in and the networks contract was modified to allow users to be certified.

Regarding government's view on PKI sites, Mr. Hale stated that maybe 20 agencies could have their own TIC. The card reader validation program that is run by GSA tests PIV card readers. Mr. Scholl stated PIN is used with PIV card. The PINs could be a different amount of characters per person. NIST and GSA are looking to help agencies, and to identify and remove barriers. By focusing on the processes, outputs, and inputs, DOD and Commerce can be barriers. There is a challenge just getting out of the way.

CIO's Perspectives on the reality of the Cloud Computing for Government

Robert Vietmeyer, CIO, US Department of Defense

Mr. Vietmeyer did not attend.

Meeting adjourned at 12:32 P.M., Friday, June 14, 2013.

Annex A

LAST	FIRST	AFFILIATION	ROLE
Badger	M. Lee	NIST	Presenter
Bello-Ogunu	Emmanuel	DHS	Visitor
Benzing	Jeffrey	Main Justice	Visitor/Press
Brown	Evelyn	NIST	Visitor
Chalpin	John Paul	Exeter / TS Alliance	visitor
Crane	Earl	The White House	Presenter
Curran	John	Telecom Reports	Visitor
Czulak	Emery	DHS	Presenter
Davis	John C.	Teknoworks	Visitor
Eisensmith	Jeff	DHS	Presenter
Gerson	Jason	App Developers Alliance	Visitor
Goodrich	Matthew	GSA	Presenter
Greene	Robyn	ACLU	visitor
Hale	Lawrence	GSA	Presenter
Hirsch	Berkeley	Wiltshire & Grannis LLP	Visitor
Hoehner	Christian	Van Scoyoc Associiates	Visitor
Hoppe	Jessica	Williams & Seasen PLLC	Visitor
Jackson	Janice	DHS-USCIS-VER	visitor
Landfield	Kent	McAfee	Presenter
Larence	Eileen	GAO	Presenter
Lightman	Suzanne	NIST	Presenter
Marsh	Adrian	CC-OPS	Visitor
Mayers	Timothy	Price Waterhouse Coopers	Visitor
Menna	Jenny	DHS	Presenter
Miller	Jason	Federal Radio	Visitor/Press
Moore	Debbie T.	Cyberzphyr	Visitor
Moreno	Elena	Wiltshire & Grannis LLP	Visitor

LAST	FIRST	AFFILIATION	ROLE
Moriarty	Kathleen	EMC	Presenter
Naumcnik	Zoya	Williams & Jerren	Visitor
Nelson	Samantha	Van Scoyoc Associiates	Visitor
Newton	Elaine	NIST	Visitor
Otto	David	DHS	Presenter
Panzo	Sonya	GSA	Visitor
Polk	Tim	The White House	Presenter
Rogers	Melinda	DOJ	Presenter
Sedgewick	Adam	NIST	Presenter
Sepeta	Arthur	DHS	visitor
Skompinski	Lauren	Williams & Jerren	Visitor
Snedden	Hal	Potomac Wave	Visitor
Souppaya	Murugiah	NIST	Visitor
Struse	Richard	DHS	Presenter
Sul	Paul	BAH	Visitor
Thomas	Carlos A.	ECI	Visitor
Thomas	Carlos A	ECI	Visitor
Toler	Danny	DHS	Presenter
Wilshusen	Greg	GAO	Presenter
Young	Marsha	SAIC	Visitor