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 13, 14 and 15, 2013

	Board Members	
	Present:	Absent
Wednesday, February 13, 2013 9:30 A.M. – 5:20 P.M. Thursday, February 14, 2013 8:00 A.M. – 5:10 P.M. Friday, February 15, 2013 8:52 A.M. – 12:40 P.M. The US Access Board 1331 F Street, N.W., Suite 800 Washington, D.C. 20004-1111	Matthew Thomlinson (Chair), Microsoft Julie Boughn, DHHS Christopher Boyer, AT&T Kevin Fu, Univ of Michigan Brian Gouker, NSA Toby Levin Edward Roback, Dept. of Treasury Phyllis Schneck, McAfee Inc. Gale Stone, SSA Peter Weinberger, Google	Gregory Garcia, Garcia Cyber Partners See Annex A for record of presenters and visitors

Wednesday, February 13, 2013

Cybersecurity Policy Discussion
US Department of Commerce, Main Conference Room

The meeting was called to order at 10:00 A.M. by Deputy Secretary Blank who welcomed the audience to the Department of Commerce. She acknowledged attending members of the U.S. Senate and House of Representatives and Cam Kerry, who has done much to lead Commerce's Cybersecurity efforts.

Ms. Blank recognized Cybersecurity as one of the most crucial challenges facing the security and economy of the nation. She described Commerce's commitment to protect and support industry. She described National Institute of Standards and Technology's (NIST) promotion of voluntary standards to protect innovation such as Internet-based commerce. Such innovation has improved the lives of Americans, curtailed risk, fostered innovation, and encouraged growth. She acknowledged that public and private leaders need to work closely together and that the administration is "stepping up to the plate" through unprecedented outreach to the community to keep business community aware and proactive in adopting best practices.

She introduced White House Cybersecurity Coordinator Michael Daniel, who thanked her for the kind welcome and for hosting the event. Mr. Daniel acknowledged those present including Secretary Chertoff, Dan Tangherlini, and Mr. Kerry.

The Executive Order represents a big step forward in Cybersecurity. President Obama signed the Executive Order to improve the Cybersecurity of our nation's critical infrastructure and approved the presidential directive to improve the security and resilience of critical infrastructure in both the cyber and physical realms.

The President recognizes that the ongoing threat is real and serious; the Federal government is continuing to forge new relationships among state & local entities as well as with private sector partners. These issues are hard things that will take time to get right, so the time to start is now.

The effort will rely upon three pillars: information sharing, privacy, and framework of standards. Regarding information sharing, the President will require agencies to increase the volume, timeliness, and quality of information sharing among a broad array of participants. At the same time, regarding privacy, we must protect privacy and civil liberties, embracing efforts such as the FAIR principles. For standards, the Order directs NIST to develop the framework of standards to act as a baseline of Cybersecurity for our critical infrastructure. The administration calls on the primary regulators of agencies to determine the sufficiency of policy and procedures as compared to the framework and address shortcomings to improve resilience.

The Executive Order represents a whole government approach. Cyber is a team sport and no one agency can carry out everything that needs to be done. This Executive Order is a continuation of a long-term conversation that has been going on for quite some time. The Administration took on unprecedented outreach and reflects input from many stakeholders including industry, think tanks, and Congress.

Mr. Daniels asked for all to help make the framework effective and meaningful through a shared, collective endeavor. He pointed out that this is just a down payment on legislation, and looks forward to working with Congress on a bill they can sign to support strong Cybersecurity.

Mr. Daniels introduced General Alexander, Director of NSA (DIRNSA) and U.S. Cyber Command Director. General Alexander thanked Mr. Daniels and remarked that the threats to our information systems are real and growing. He referenced the ongoing distributed denial of service on Wall Street and other destructive attacks that show the need to act and to act now.

We need a way of information sharing between government and industry. This Executive Order tackles what is perhaps the most difficult challenge – how to harden networks that are largely owned by private entities. He stated that he is pleased to see Dr. Gallagher leading a portion of this effort. Gen. Alexander pointed out that U.S. Cyber Command (CYBERCOM) has a vital role defending our nation's systems but that CYBERCOM can't do it all, that the Government can't do it all by itself. We need industry to be part of the team, ensuring that private sector companies have the information they need to protect ourselves including a close look at how we harden our infrastructure.

As DIRNSA, he stated that he supports NIST in development of the Cybersecurity framework. He agreed that this is only a down payment and not a substitute for legislation. The Executive Order is a step forward.

With so much critical infrastructure owned and operated by private organizations, the government is often unaware of critical risks, information it needs to know to defend the nation. For that reason, we need to remove barriers to public sharing. We need to create incentives for cooperation. We need to update and modernize the Federal regulations to, for example, address industry liabilities.

General Alexander introduced Homeland Security Deputy Secretary Jane Lute. She stated that US Department of Homeland Security (DHS) was formed to create a safe and resilient America. Cybersecurity was part of the DHS Quadrennial Review four years ago as a key essential not only for DHS, not only for the Government, but for all who are active in Cyberspace.

The Executive Order consolidates what we have learned and starts us on the way to: 1) enhance the ability to share timely threat information with companies, and 2) expand the Defense Industrial Base (DIB) project to share sensitive, anonymized information and intelligence from law enforcement organizations and other sources. These plans supplement existing efforts. The amount of private sector understanding of threat can dwarf the amount that the government has. We are establishing a voluntary program to promote the Cybersecurity framework in a way that is outcome-based and technology neutral.

Ms. Lute pointed out that Cyber and physical security teams must work together to implement the Executive Order and the Presidential Policy Directive, and promoted the need for holistic approach. She welcomed Deputy Attorney General Jim Cole.

Mr. Cole stated that, last year, the Administration made the importance of privacy and civil liberties clear. He reaffirmed the commitment to sharing information while protecting privacy, confidentiality, and civil liberties. One of the most important elements of the Executive Order is that of timely provision of information to the private sector. Mr. Cole described the ongoing Cybersecurity services initiatives of Department of Justice, Department of Homeland Security, and the Office of the Director of National Intelligence to declassify reports that describe threats that target U.S. interests and to provide timely notice to the owners of those interests.

We need to improve the flow without losing sight of our commitment to protect privacy and civil liberty. We will do this through a transparent process with trained oversight. We will develop and implement privacy and civil liberty safeguards including required assessments, sharing of information with the DHS Chief Privacy Officer and with public reports.

He emphasized the Administration's commitment to responsible, effective Cybersecurity standards and information sharing while protecting privacy and civil liberties through transparency and accountability.

Mr. Cole introduced Dr. Gallagher, Undersecretary of the Department of Commerce and Director of NIST. Dr. Gallagher used the audience as a reflection of the desired approach to build the framework – through a broad cross-section of stakeholders from across government and industry. The framework will be a set of practices, standards, guidance, methods – whatever it takes, if implemented effectively, to achieve the desired Cybersecurity performance and resiliency. It will not be a NIST work product, but will belong to industry. He pointed out that it will be an aligned effort, a framework for action, a layered approach for each organization to make their own, leveraging common practices and tools (some sector-specific). NIST's role will be to convene and support the multi-stakeholder approach.

He stated that he believes that the most effective outcome is one where the government depends upon the private sector. Nearly all assets in Critical Infrastructure Key Resources are privately owned and operated. NIST and DHS are working on the performance goals for the effort, the North Star that will guide us to successful implementation.

The approach must be adaptable and take advantage of industry's capacity & know how. We will achieve effectiveness at market scale, resulting in the solutions being driven into technology and operations, making sure efforts are effective through promotion of sharing and adoption. He described the benefits of having these baselines "baked in".

Dr. Gallagher pointed out that the word "standard" is going to create confusion – it means many things to many people. Standards are simply a common basis of comparison. He described performance standards, such as academic standards, as something to be achieved as measured against a goal that someone else defined. He said that the much more common standard is a norm - a mutually agreed upon set of protocols, practices or specifications that allow collective action (e.g. shared business standards like quality management). These types of standards are developed by industry through multi-stakeholder, open, participatory processes, and NIST will help foster that collaboration through the framework development. NIST will conduct a series of workshops beginning in early April. Dr. Gallagher renewed the call for teamwork and invited Mr. Daniel back to close the session.

Mr. Daniel pointed out that the signature of the Executive Order and Presidential Policy Directive are milestones, but that much hard work is ahead. He called on agencies to conduct meetings with sectors and trade associations to conduct a good exchange of ideas.

He thanked the audience for coming to the session and dismissed the meeting at 10:46 AM.

Following the update on the Administration's Priorities for Cybersecurity Policy at the Department of Commerce headquarters, the ISPAB reconvened at the US Access Board conference room for the remainder of the meeting. The ISPAB Chair, Matt Thomlinson, called the meeting to order at 11:30 AM.

Introduction to the FISMA Legislation

David Plocher, US Government Accountability Office (GAO)
Suzanne Lightman, NIST

David Plocher and Suzanne Lightman provided an overview of the origins of Federal Information Security Management Act (FISMA). They described the law's origins in private sector best practices and FISMA's goals of helping federal agencies to adopt an effective risk management approach. Most of the legal definitions are traditional; some definitions were modified to fit the FISMA framework. FISMA is focused on risk management practices and is technology neutral.

The discussion then shifted to some challenges with FISMA. One issue is that the separation of responsibilities from Chief Information Officer (CIO) and the budgetary authority of the Agency head causes difficulty. The CIO is ultimately responsible for FISMA compliance but is not in control of resources to be able to report on assets. Currently, FISMA reporting happens annually; this was not the original intention. There are many sources of information regarding expectations of compliance (Office of Inspector General (OIG), Executive assertions, Special Publication 800-53) and the CIOs have difficulty determining the best path forward. Most agencies want to do better FISMA reporting but lack the budget and qualified people to carry out the task.

The Board then asked about positives of the law. In support of FISMA, the panel cited that the law formalized the CIO position and defined a new role in the CISO. The law also brought Cybersecurity to the forefront of agencies' planning whereas previously it had been an afterthought for some. FISMA also formalized Privacy Impact Assessment (PIA) requirements.

Agency IG Audit and Compliance (Presentation provided)
Gale Stone, (Moderator), Deputy Assistant Inspector General for Audit, SSA
Brett M. Baker, OIG, National Science Foundation
Joseph Maranto, OIG, US Department of Education
Andrew Patchan, Assistant IG for Audit, Federal Reserve Board

The panel began with a discussion on how OIGs conduct FISMA reviews. There are two aspects to reviews: effectiveness of security controls and status of security controls, procedures, and practices. During a review, audits of compliance with required controls and penetration testing of systems could be used. A review may consist of standardized procedures and also some discretionary assessments based on a risk inventory. Cost benefit analysis of systems and system type coverage are two key factors in determining audit targets. These discretionary audits are flexible within the risk management framework.

The panel stressed that a single review does not give any long-term evidence; a review is a snapshot in time dependent on the agency priorities, current control set, and the level of attacks that are present in the ecosystem. Audits of classified systems are conducted and reported separately from unclassified audits.

The Board asked about findings and usefulness of audits. When there is a finding and a remediation is recommended, there is sometimes pushback. For example, agencies may claim that the remediation is not actionable. In all cases, early and frequent communication is necessary to avoid conflict. The panel remarked that agencies communicated through both unofficial and official channels to share information regarding audits. More could be done at the agency level to increase that sharing effort.

The panel listed the following as resulting benefits of the audit system:

- Increase in training
- Increase in incidents report
- Increase in percentage of incidents remediated
- Improvement in culture for identifying and addressing issues

The Board then discussed repeated findings - a key metric in the audits. This is a tough metric to focus on, however, because the severity of the finding may be negligible to the CIO when there are other competing pressing issues.

Discussion of Annual FISMA report, overall progress and current/future priorities

Donna Dodson, (Moderator), Chief, Computer Security Division, NIST
Carol Bales, Office of Management and Budget (Presentation provided)
Gary Galloway, Deputy Director, Informative Assurance, US Department of State

The panel began the discussion with an overview of current cross agency priority goals for Cybersecurity: Trusted Internet Connections, Continuous Monitoring, and HSPD-12. The panel shared the goals that Office of Management and Budget (OMB) is working towards for fiscal year 2013: 95% of assets being continuously monitored and 75% of system users required to use an approved Personal Identity Verification (PIV) Card to authenticate to agency assets. The Board was concerned over the cap in PIV card issuance and actual usage. The panel assured the Board that steps were being taken to close the gap.

The Board asked the panel to explain the challenges in getting the basics of Cybersecurity working in a government setting. The panel said that there are cultural and legacy issues that prevent the agencies from quickly adopting new standards and technologies. The panel also pointed out that since the agencies are largely decentralized there is a lot of uncertainty on the exact amount of compliance that is necessary. With that uncertainty the CIOs do not have budgetary authority over the assets they manage as well as a lack of resources. Further compounding the problem, the return on investment of Cybersecurity has not been fully communicated, thus making cybereconomics unclear.

The Board then asked about whether there is an opportunity to start over with FISMA. The panel said that there had been a lot of expertise gained under FISMA and that it may not be necessary to start over, but instead a modification. To facilitate that modification the panel indicated that they would like to work closer with industry so as to apply the private sector’s lessons learned.

FISMA Process and Development for past ten years

Ron Ross, Fellow, NIST

Dr. Ross provided an overview of the last ten years of FISMA guidance and NIST's role. He stated that FISMA has three legs: legislation, OMB policy, and implementation of standards published by NIST. There were three generations of FISMA compliance. The first was a static set of controls that were subjected to a time schedule or a significant change in a scanned system. The second generation was closer to near real time risk management. The third was a cross community effort at information security.

Dr. Ross turned his discussion to the future – the 4th generation of information security. The main tenant of this generation is specialization. In revision 4 of NIST SP 800-53 there will be a concept of an overlay. This feature will allow organizations to communicate about which controls they are utilizing in an automated manner. An example of an applied overlay is FedRAMP. The other key focus in revision 4 is privacy of the information.

The discussion moved to a more fundamental view of information security. Dr. Ross explained that the bigger question affecting cybersecurity is building better software. He pointed out that if we built more reliable systems from the beginning, then the issues of cybersecurity will become much more easy to handle. To accomplish this task, the security and privacy specialists need to be involved early and often in the software development cycle to ensure that the software meets all appropriate conditions. His mantra was "build it right, then continuously monitor."

The Board asked Dr. Ross about ways to incorporate these concepts in the near term and about the process by which an overlay becomes 'blessed.' Dr. Ross explained that there are two avenues to pursue: consensus driven overlays and legislative mandates. The board inquired about the "center of gravity" for creating overlays. Dr. Ross said that having the CIO group involved would be a good idea and, potentially, ISIMC (Information Security and Identity Management Committee).

In response to the Board's question on key challenges facing the implementation of the next generation of information security, Dr. Ross pointed to CIO/CISO top cover and training. Due to IG oversight, CIO/CISO are conservative about taking on risks but this is holding back innovation. Training of employees on cybersecurity is not at an acceptable level. The goals for such training are not well defined, and thus not implemented.

Dr. Ross believes that there is a common threat but there is a difference between what is reported by press, security companies, and the government.

THURSDAY, February 14, 2013

The Chair opened the meeting at 8:00 A.M.

GAO's View of FISMA (Presentation provided)
Anjalique Lawrence, Assistant Director, US Government Accountability Office (GAO)

Ms. Lawrence began with describing GAO's role in FISMA compliance. GAO issues a government-wide summary report every two years. This report summarizes the overall performance results for covered systems and provides some sample reviews for context. The objective of the review is to make sure proper controls are implemented. She indicated that incident reporting is on the rise, potentially due to both increased reporting and better detection of anomalies. The Board pointed out that an anomaly does not necessarily equate to a security incident. Also, knowledge of incident and reporting requirements differ from agency to agency, further muddling the picture. This year OMB removed the requirement for small/micro agencies (approximately 140) to report annually. Contractor oversight is being included in this year's report (2013).

The Board raised the question of whether agencies have adequate visibility of security incidents. Ms. Lawrence noted that some agencies have increased ability to detect intrusions and thus may have better reporting statistics. Conversely, other agencies may not report as many incidents due to reduced capability to detect those incidents.
The Board asked about where the government has made the most progress. Ms. Lawrence responded that there has been a shift in weaknesses and deficiencies between agencies. Some agencies do well in one year in some areas, then poorly in the next year. Based on the current data, GAO is now developing a baseline to determine whether agencies are trending positively

Each agency has made progress in different areas, GAO does not track all specifics because they only see roll up reports each year. GAO does have visibility into some agencies year over year.

Ms. Lawrence reported that access controls were still an issue. Agencies also are reactive with regards to cybersecurity, mostly depending on whatever topic is popular with the administration from year to year. GAO does not account for severity of incidents in previous reports, but it will be documented this year. There is sufficient data but the presentation methods need not be improved so as to draw better conclusions. Also, report size is shrinking due to better streamlining of the data. Ms. Lawrence noted that US-CERT has implemented a change in how categories are reported.

There are rooms for improvement if they have the tools and people that understand the threats and tools. Cybersecurity training needs to happen early and often.

The combination of leadership, congressional mandates, and additional personnel can counteract the significant turnaround from agencies. It takes a lot to effect a large change and DHS has helped a lot. DHS's role should be legislated so they can better serve the agencies. There are varying models used by each agency and success is not correlated on a specific model. Decentralization makes it difficult to manage policy throughout an agency due to the different operating procedures of each department. This fact makes it imperative that employees are educated on controls. Having people that understand cyber security is crucial to success.

Ms. Lawrence went on to explain that a GAO report on CIO roles and responsibilities was being released to the public this year. In that report, GAO observed that CIO tenure is decreasing, thus continuity of operations is broken. This fact compounds other problems with getting policies and procedures put into place that have a meaningful impact on the overall posture of an agency. The Board pointed out that a CIO may be fired for perceived failure or potentially for spending too much money to avoid failure. It is an almost impossible balance.

DHS/Federal Network Security: FISMA Metrics Deep Dive

Matt Scholl, (Moderator), Deputy Chief, Computer Security Division, NIST
John Streufert, NCSD Director, DHS, Cybersecurity & Communications, National Cyber Security Division
David Waltermire, Computer Scientist, Computer Security Division, NIST (Presentation provided)

Mr. Streufert announced the release of a new Continuous Monitoring as a Service RFP on February 11th. The contract is for the hardening of federal networks in face of attacks. The scope of the contract is the protection of [dot].gov. The objectives of the contract are:

- To find fix and report on status of cybersecurity measures
- To provide hardware management, software management, vulnerability management, white listing

Mr. Streufert went on to describe current continuous monitoring efforts ranging from no activities to minimal continuous monitoring at various agencies. Some agencies have no tools in place, and there are varying levels of maturity of tools with those agencies that do have tools. The focus is to be able to see how federal systems are being attacked and the effectiveness of our investments when under attacks. Ideally the metrics will be outcomes based. The plan is to take 3 phased approach based on critical controls. The highest ROI for $13.3B spent approximately 10% NIST 800-37 implementation, 4% cybersecurity tools, and 75% labor.

Mr. Waltermire described NIST's work on continuous monitoring. The on-going authorization is a topic of discussion in the continuous monitoring group. For example, security checks for applications such as Java and Flash have not been developed yet in SCAP. In continuous monitoring, there are common data formats but not common protocols. Tools and technologies for continuous monitoring are in the requirements phase and have yet to develop capabilities. As an example of encouraging open standards, NIST is working to establish a security automation working group in IETF.

Mr. Waltermire then gave an overview of CEASARS-FE, a continuous monitoring architecture. CEASEARS-FE allows tailorabiliity by differing agencies, and also allowed rolling up and aggregating. The architecture enables the endpoint to make its own assertions by using other artifacts (network data, etc) to verify that assertion. Privacy across agencies is a tough challenge; each agency will need to address PII issues. Access controls at every level must be enforced to ensure privacy. The architecture represents a security and operational view of the network. Ideal state has been identified. The layers are there and just need to be built and integrated.

With regards to security mechanisms in SWID (software identification), which allows for digital signatures, NIST is currently working on guidance to ensure software installers are taking appropriate measures to maintain integrity of the software when installing. Incentives of SWIDs are not necessarily all security related. There are licensing incentives and cost savings based on software inventory management. SWID enables product-to-vulnerability mappings based on software footprint.

The panel noted that there is a need for support from organizations to participate for requirements and use cases phase of CEASARS-FE. The Board could set priorities among negative consequences, collective agreements, and government purchases. To elevate importance of management efforts, the panel suggested the Board to highlight protection as it relates to:

- Loss of Intellectual Property's negative impact on jobs
- Economic losses from identity theft
- Harmful effects of the loss of national security information
- Overall drag on the economy from poor security practices

The panel further suggested that the Board highlights capabilities, not specifications, and to provide a larger vision of the capabilities for overall critical infrastructure.

For the first phase of the CDM contract, the panel believed that the absence of appropriations for tools is a large issue and another issue is getting requirements / engagements from government/industry. It is after the tools have been built that the next phase can start. In proceeding to implement the solution, Mr. Streufert said that in light of the funding being one-year money, it is essential to get early buy in. The right balance needs to be met. At this point it is expensive to do nothing, but funding is required to get over the hump to starting point.

FedRAMP and Cloud Certification (Presentation provided)
Dave McClure, Associate Administrator, Citizen Services and Innovative Technologies, GSA

Mr. McClure started with a clarifying statement: FedRAMP is not an exercise, it's a program. The primary focus of FedRAMP is establishing trust between government, cloud service providers (CSPs), FedRAMP, and the purchasing agency. FedRAMP wants agencies to submit their baselines, Third Party Assessment Organizations (3PAOs), testing plans into the repository that will gain better reuse and cost savings across the government.

FedRAMP has always embraced continuous monitoring. FedRAMP is not just faith based computing; it has bore down into evidential principles of proving security and capability. FedRAMP is not just a gatekeeper, but also work with applicants to get pass to "yes" decision in all cases when the applicant is committed to the process. When NIST does a revision to an 800 series publication, FedRAMP re-evaluates control sets and aims for a 6-month turnaround time.

Mr. McClure provided some statistics regarding the current program:

- CSP: over 80 applicants, 2 provisional authorizations (Autonomic Resources, CGI)
- 3PAOs: over 50 applicants, 16 accredited 3PAOs

The sustainability of the Joint Authorization Board (JAB) is uncertain. The JAB was intended for the most important things, but has been used for constant communication between CSPs and FedRAMP. It is necessary to rethink the structure in the future.

When discussing FedRAMP's privacy obligation, Mr. McClure stated that the obligation is primarily on agency. Some contracts have clear divisions for those privacy concerns. He emphasized that clear contract language is of critical importance. All providers complete a privacy threshold analysis.

For the process for updating controls, FedRAMP relies on public comment period. It is a constant struggle to strike a balance of timeliness versus completeness. Mr. McClure offered some lessons learned from FedRAMP:

- The level of effort for accreditation is greater than expected, at best taking four to six months, with evidential standards are greater than CSPs expected.
- Several common security factors have resulted in “deal breakers” that prevented authorization including: encryption concerns, lack of multi-factor authentication, appliances outside of the control of the CSP, and poorly maintained boundaries.

Mr. McClure said that continuous monitoring data will flow from CSP to DHS and customer agency. Each agency has C&A requirements for the CSP-based system regarding public, multi-tenant clouds. An organization receiving FedRAMP authorization is “on the hook for continuous monitoring". With regards to attaining configuration data of machines, Dave McClure indicated that is an ongoing effort to define.

For the disclosure of results of assessments by 3PAOs, there is a process to guide access to that information (guided by an agency CISO). Redaction is also guided by CISO. Mr. McClure closed by stating that 3PAO accreditation has always been visualized as privatized and has created a small business opportunity.

Mobile Computing Security Baseline Working Group

Kevin Stine, (Moderator), Group Manager, Computer Security Division, NIST
Kevin Cox, Assistant Director, InfoSec Technologies (IST) Team, US Department of Justice (Presentation provided)
David Carroll, Chief Information Security Architect, US Department of Homeland Security

The panel described various approaches to mobile device security and that it is not a "one size fits all" plan. They went on to discuss their current project to define barriers, opportunities, and gaps in mobility in government. Their 12-month milestones are to develop a security baseline and mobile security architecture. They are also working to target industry to get FedRAMP-type level of trust in mobile applications. Currently the tiger team is writing overlays that depend on several factors: Agency control, Mobile Device Management (MDM), Mobile Application Store (MAS), Identity, Credential and Access Management (ICAM), mobile device data, Government Furnished Equipment (GFE), national security systems, and federal employees. It is difficult to reconcile identity while not compromising mission.

Security can be implemented, but legal/privacy decisions need to be incorporated to drive security requirements. The team is working hard to provide the framework to the Project Managers. Cost structure for home devices is not known, therefore, it is difficult to assess risks. The shape of standards in other arenas such as privacy/legal makes it very difficult to write overlays. The security technology exists, however there is no agreement on policy for each agency.

For the prioritization of overlays and use cases, prioritizing overlays is the first step. The following stages would be: creation of framework (heavy lift), creation of overlays (enumerations), maintenance /storage of metadata. The panel would like to look for commonality in application. A common language to communicate about mobile security is needed due to the large application diversity. Dual persona is highly subjective right now, and thus difficult to assess.

The communication channels need to be set up and industry input is being sought. The government needs guidance on how to seek out industry contact and input. The panel would like to see anything that fosters innovation in the day to day business world.

Cloud Security Challenges

Ed Roback, (Moderator), CISO, US Department of Treasury
Peter Johnson, CIO, Bureau of Engraving and Printing, US Department of Treasury
Christopher Lowe, CISO, US Department of Agriculture
Roger Seeholzer, Strategy & Requirements Branch Chief, Information Security Office, US Department of Homeland Security (Presentation provided)
Raghav Vajjhala, ACIO for IT Strategy and Technology Management, Office of the CIO, US Department of Treasury

The panel echoed a previous point that one scan at a point in time does not necessarily mean security in a cloud environment. The physical machine could be switched at boot time. The user must relinquish having complete control of the system. In a cloud environment, cost savings drive the business model and not optimization of each node.

Spillage in a cloud environment is tough to clean-up due to the non-locality of the host. However, cleaning is mostly the same process that is present in a non-distributed environment, but more difficult as a result of multi-node processing and policies. Inside the network, services are defined as low risk. For services that are outside the internal network, and when dealing with new services, it is difficult to quantify risk. Thus, when moving a system from inside to outside (e.g., after employee leaves the system, he/she attempts to access or as a 3rd party service) the risk profile increases. Another issue when handling data spillage is human nature (e.g., accidental email spillage). This must be taken into account when mitigating risk.

The panel considered the following questions should be the responsibilities of individual agencies:

1) What is a good way of budgeting for cyber risks including tools, data management, and effective monitoring?
2) How to prioritize systems under tight budget conditions?
3) How to handle classified data in a cloud environment?

The panel next turned to the topic of contract clauses. A general point made by the panel was that Service Level Agreement (SLA) language in cloud contracts must be explicit. In regard to which common contract clauses could be applied, it was agreed that common clauses would be helpful but recognized that updating an existing SLA/contract is difficult. The panel was turning FedRAMP to assist in lowering some of these boundaries.
Being first adopters has benefits (e.g., early access to new services) and detractions (e.g., paying upfront administration costs to get things right). The first agencies have to work through the kinks in the cloud provider services and data provenance issues before the cost savings can be realized.

The panel's view on the state of the union in CSP and security requirements was that there are still questions around the evolution of Personal Identity Verification (PIV) and cloud. Overall CSPs are pretty good (based upon attestation of configuration management), but may not be as far along in the open internet (e.g., ID theft is still an issue). This is discouraging because there are too many vendors and too many requirements to maintain a return on investment (ROI) and a competitive advantage for the provider. CSPs and agencies need to have more conversations around incident reporting. After a Board inquiry, the panel said that the current state is difficult to change due to changing NIST standards. Again, the point about ROI and continuous investment on the CSP's part was stated.

The panel brought up the subject of how FISMA puts emphasis on showing you are secure instead of just being secure. The Board discussed a recommendation concerning overhead reduction to attain compliance, and how to fix the problem of proving the state of security.

On the question of whether there was hope for common methodology for evaluating technical change that could be shared, the panel responded that the inertia is so large for change and that agencies are so different, it is difficult to share information horizontally.

The panel indicated that flexibility in application of NIST 800-53 controls was never communicated clearly to each agency. The panel also expressed concerns over how dynamic the auditing by the IG is. The IG maintains final decision authority and the ability to change the audit from year to year.

The panel provided these final thoughts:

- Product liability is an issue – seller indemnification puts agencies in a tough position
- Increased requirement would lead to better software
- Lift the EULA that government has to accept
- As long as proof by documentation is the norm, large scale CSP is uncertain
- If continuous monitoring is added as a requirement, consider taking another requirement away
- Addition of new idea does not currently replace old ideas, leading to requirements bloat
- OMB's statutes are deemed to be primary

Critical Infrastructure Cybersecurity

Patrick Gallagher, Under Secretary of Commerce for Standards and Technology and Director of NIST

Dr. Gallagher started his presentation by stating that there are three pillars to the Executive Order (EO): information sharing, privacy, and a framework of standards. Regarding the framework of standards at NIST, the structure is to provide a market to produce a security responsive framework of actions to achieve security. DHS sets the level of performance, industry then creates best practices against that. Finally, a discussion regarding the incentives in the adoption of the framework is necessary. With respect to operations, NIST can offer deep technical expertise in the effort; however, NIST is not in charge of anything. NIST's role is to support industry, and not other way around.

Dr. Gallagher offered a set of leading questions:

- What is the framework process?
- There will be heavy industry involvement at all phases. The framework is intended to help industry and thus should be driven by industry.
- How do we create collaborate structure?
- This EO is more like the *Framework and Roadmap for Smart Grid Interoperability Standards* and less like FISMA. The EO starts from "what is industry best practice" and attempts to answer the questions: Where are the overlaps? Where are the gaps? When the gaps are identified, they become the priority.

Please refer to Annex B for a transcript of the Board's discussion with Dr. Gallagher

Executive Order Panel Discussion

Andy Ozment, Senior Director of Cybersecurity, Executive Office of the President
Samara Moore, Cyber Director for Critical Infrastructure, Executive Office of the President
Adam Sedgewick, Senior Information Technology Policy Advisor, National Institute of Standards and Technology
Bruce McConnell, Senior Counselor for Cybersecurity, Department of Homeland Security
Ari Schwartz, Internet Policy Advisor, National Institute of Standards and Technology
Jenny Menna, Director, Stakeholder Engagement and Cyber Infrastructure Resilience Division, Department of Homeland Security

The panel began with a discussion of information sharing. The panel indicated that the government needs to be better at public to private information sharing. In that vein the government will be issuing more clearances. Another step to increase the level of effort will be the sharing of threat information. There will be increased volume, quality, and timeliness of indicator sharing. Finally, there will be enhanced cybersecurity sharing services.

For privacy and civil liberties, there will be an oversight mechanism with respect to the EO and Presidential Policy Directive (PPD), Federal Information Processing Standard (FIPS) is called out specifically. The topic of task of identifying critical infrastructure includes cyber threat and physical threat. Infrastructure considered for the first report is infrastructure that would cause catastrophic national or regional damage if compromised. The panel explained that reference to government facilities in the EO is meant that the government may own critical infrastructure and that the EO covers that territory as well.

The panel pointed out that Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience,* replaces Homeland Security Presidential Directive (HSPD) 7. They stated that DHS has a unique role with consultative process with industry encouraging a review of the public/private partnership.

As for DHS process, DHS will coordinate with NIST's timing and processes. Some of the performance goals will be established in part through the RFI process. The framework is completely voluntary and everyone is invited to participate.

In explaining the depth of information sharing, the panel said that the end goal is to have all of the private sector included in the program. Sharing within sector (e.g., Bank A, Bank B) is still being worked out.

The panel stated that the capabilities are not fully defined for demo at Day 240 described in the PDD. The Enhanced Cybersecurity Services (ECS) is for all critical infrastructure and is not tied to the voluntary framework. Defense Industrial Base (DIB) Enhanced Cybersecurity Services (ECS) (DECS) is a voluntary program to share threat indicators between commercial service providers and DHS. On the topic of threat consensus the panel said that step one was to raise the bar from 0 to minimal.

The framework could serve as basis of an insurance underwriting market. The framework could also serve as a learning experience for regulators. They may not have the expertise in cybersecurity. It is hopeful that the framework will serve as basis for industrial innovation. Industry has expressed a desire for benchmarks. As for small business protection, the panel stressed flexibility in the framework such that the small businesses could participate.

The panel suggested the following that ISPAB could assist in resolving key challenges for NIST:

- The framework has to gain leverage from now through next year
- A way to engage with key stakeholders that is manageable within the time frame
- Has to be maintainable by critical infrastructure owners and operators
- Encourage adoption of the framework
- Requested the Board to constantly consider the following questions throughout the process: Does the framework answer the mail? Does it help (actionable) at the end of the day?
- What is the SLA between the service provider and the American people?
- Identify representational parts from Notice of Intent (NOI) and Request for Information (RFI)

FRIDAY, February 15, 2013

The meeting reconvened at 8:00 A.M.

Executive Office Update

Andy Ozment, Senior Director of Cybersecurity, White House

Mr. Ozment started his presentation with a review of current legislation. Currently, there are some bills being introduced and the White House is still pushing for full suite of updates. Mr Ozment spoke to the future of [dot].gov which could not be viewed as a classical network. It is a collection of departments and agencies that are also connected to the Internet. Trusted Internet Connections (TIC) was a start of a segregation strategy which utilized EINSTEIN as a tool. Mr. Ozment asked the Board the following questions:

- What should .gov be?
- Is the current model sufficient?
- Currently we are attempting to distinguish between security levels
- How do you reduce return on adversary time?
- What should the goal of network architecture be?

Mr. Ozment mentioned Network Services 2020 and its security implications, and asked the Board to keep abreast of that effort. Mr. Ozment continued with another question: What are the principles in networking? What should government be looking towards in term of investments? Does the ISPAB think there is more to do in the perimeter? Or, should the investment be local/agency level? Instead of how we can build a bigger wall, let's gain visibility into the data and utilize a sensor approach. Mr. Ozment sees the ideal state as utilizing executive branch as a 'do it once' and reuse at agency level.

The Board proposed some metrics from zero day incidents:

- How many machines need to be cleaned out?
- Time to detection

Global Policy Update

Elaine Newton, Deputy Standards Liaison, ITL, NIST (Presentation provided)
Ajit Jillavenkatesa, Senior Standards Policy Advisor, NIST

The panel began with a description of the International Telecommunication Union (ITU) and its various component bodies. The major result from the last meeting of the ITU Telecommunication Standardization Sector (ITU-T) was that the U.S. did not sign ITU treaty. Ms. Newton explained some of the challenges with the proposed changes and thoughts behind the U.S. decision not to ratify the treaty. It is unclear how treaty will resolve telecommunication issues. The treaty could be used as leverage for national regulation in member countries.

There are alternative forums to the ITU regarding cybersecurity. The Forum for Incident Response and Security Teams (FIRST) is a potential alternative, or other standards organizations, however they may not satisfy the one-stop-shop seeking countries.

Automated Indicators in Telecommunication

Chris Boyer, (Moderator), Assistant Vice President, Public Policy, AT&T
Danny McPherson, Vice President and Chief Security Officer – Verisign Labs
Thomas Millar, Chief of Communications, Department of Homeland Security, US-CERT
John Nagengast, Executive Director, Strategic Initiatives, AT&T Government Solutions, AT&T

The panel began by pointing out that hackers don't always get their code right the first time. Therefore it is important to catch them before they have the final, working version. To catch them early, it is necessary to employ security services at all levels (Internet Service Provider (ISP) to endpoint client). Security is not just an ISP problem, as the ISP does not own endpoints. There are some indicators visible at the ISP level; for example, DNS lookups are good indicators of some Advanced Persistent Threats (APTs).

The panel echoed a point by a previous panel: legal issues are a big hurdle. Policy for cybersecurity is unclear regarding what one can share with other companies / customers. There are six regulatory bodies with approximately 900 controls just to satisfy those bodies. Some sectors (ISACs) share fastidiously due to the existential threat of a failure. If they have a cyber attack then their future business will suffer. Sharing in National Cyber Investigative Joint Task Force (NCIJTF) and US-CERT is a call up tree and the director makes the decision. The panel said that legislation is going to be necessary and that knowledge exchange is just as important as the indicators.

Automatic Indicator Sharing Protocols

Phyllis Schneck, (Moderator), VP & CTO, Public Sector, McAfee, Inc.
John Banghart, Computer Scientist, , Computer Security Division, NIST
Thomas Millar, Chief of Communications, Department of Homeland Security, US-CERT

The panel began with an analogy that threat data can be like weather data. National Oceanic and Atmospheric Administration (NOAA) has a great deal of data, including some classified information, but we gain answers for simple questions such as whether it is sunny or whether we need to get out of farm houses. There is an opportunity for that type of information sharing to occur with threat indicators. However, we cannot have multiple standards.

Currently there are requirements for gathering and use case efforts being made in the Internet Engineering Task Force (IETF) such as with the Incident Object Description Exchange Format (IODEF) and Real-time Inter-network Defense (RID) Messages. Structured Threat Information Expression (STIX™) would be a standard to turn to.

The panel stated that broadening trusted information sharing outside the community is difficult, but inside is easy and doable. How can we expand that community? These are the considerations:

- Is high, medium, low good enough?
- Where is the sweet spot when talking about granularity of data?
- What level of confidence do we have in an indicator?
- What are companies willing to build into your products?

Board Review of the Meeting
ISPAB BOARD

- A motion was made by Dr. Weinberger to approve the meeting minutes for June 2012, which was seconded by Brian Gouker. The motion was approved unanimously.
- A motion was made by Matt Thomlinson to approve the meeting minutes for October 2012, with amendment submitted by Dr. Schneck. The motion to approve intent and redrafted minutes was proposed by Toby Levin. The amended motion was seconded by Peter Weinberger. The amended motion was approved unanimously.

The Board evaluated the following questions:

- How can we improve the state of cybersecurity workforce?
- Is there a report on EINSTEIN 3 effectiveness?
- How can we reduce FISMA reporting paperwork?
- DHS vs. OMB – 18 months since operational FISMA responsibilities transferred. Should this be more clearly delineated?
- OMB guidance comes late/data call frenzied. Need clarity on OMB policy
- Commend DHS on sticking w/ CAP goals (TIC, PIV, CM). consistency has helped.
- FedRAMP continuous monitoring – flow needs to go to Agency, not just DHS
- Largest costs are people doing paperwork
- Can FISMA be more outcomes-based? DHS directs metrics for measure, but it is necessary to provide guidance on metrics
- DHS – reduce reporting wherever possible by asking for what is required or actionable (eg ‘baseline questions’). How can the Board help to review questions, intent of questions, etc. and potentially provide recommendation in reducing them?
- Does CyberScope improve this? Can it replace requirements for A&A? Can we directly feed to data calls for FISMA reporting?
- Ongoing authorization via tools – replacement of some reporting (monthly, quarterly, annual)?
- Can the country benefit by focusing on a single, big cyber goal (e.g. man on the moon)?

- Secure by design – build it right, develop with security in mind, force discussions with security people.
- Who owns overall strategy for BYOD?

Future agenda topics include:

- Executive Order 13636
- Cloud forensics issues
- OIG assessments of 3rd Parties
- Risk Quantification in general
- 2 new GAO reports (High Risk Federal Systems, Cybersecurity report)
- Non-executive agencies & micro agencies that do not report
- Vision of future of ".gov" Network 2020/MTIPS/TIC
- BYOD: Legal, policy issues dominating and specifics in how this differs in government vs. general industry
- Combined CIO, DHS/OMB, IG panel to dig into "they forced us to do this"
- Replacing A&A with CM/CyberScope – as we automate A&A, how do we directly feed data calls into FISMA reporting?
- What's broken with FISMA (presentation by Alan Paller)
- US-CERT changing reporting categories – does this help drive more understanding of the problem?

The following formal action items were approved:

- The Board will draft a letter in support of NIST Special Publication 800-53 Rev. 4 (Toby Levin to draft the initial outline and Matt Thomlinson will complete the draft)
- The Board will draft a letter on the importance of constituting the Privacy and Civil Liberties Oversight Board (PCLOB) (Toby Levin to draft the initial outline and Matt Thomlinson will complete the draft for the Board's review)
- The Board will continue discussions of E.O. 13636 in virtual meetings and potentially other face to face meetings. Discussion will particularly center around the NIST Request for Information and NOI (Phyllis Schneck is to coordinate the discussions)
- FISMA discussion/follow-up actions – recommendations, questions, comments to DHS/OMB/NIST

The meeting adjourned at 1:36 P.M., Friday, February 15, 2013.

Annex A

LAST	FIRST	AFFILIATION	ROLE
Baker	Brett M.	NSF	Presenter
Bales	Carol	OMB	Presenter
Banghart	John	NIST	Presenter
Barteck	Mike	NIST	visitor
Belcher	Joshua L	Cozen O'Connor	visitor
Bell	Arnold	General Electric Company	visitor
Brickell	Melissa	US Senate Commerce Committee	visitor
Brown	Laura	NERC	visitor
Carnahan	Lisa	NIST	visitor
Carroll	David	DHS	Presenter
Chilson	Neil	Wilkinson Barker Knauer LLP	visitor
Cox	Kevin	US Department of Justice	Presenter
Crum	Jim	VSA	visitor
Cuchask	Jeffrey	NIST	visitor
Cummins	Keren	nCircle	visitor
Davis	John C	Teknoworks Inc.	visitor
Dodson	Donna	NIST	admin
Du	John	ITAC	visitor
Duckworth	Brent	Iron Vine Security	visitor
French	Matthew	US Access Board	visitor
Galloway	Gary	US Department of State	Presenter
Gilsinn	Jim	Kenexis for Automation Federation	visitor
Graldamez	Misael	BITS/Financial Services Roundtable	visitor
Hoehner	Christian	VSA	visitor
Hogan	Trevor	PwC	visitor
Holcomb	Jay	DHS	visitor
Hornstein	Jayne	NSF OIG	visitor
Hyun	Min	Microsoft	visitor
Jillavenkatesa	Ajit	NIST	Presenter
Johnson	Peter	US Department of Treasury	Presenter
Lawrence	Anjalique	US GAO	Presenter
Lightman	Suzanne	NIST	Presenter
Little	Susan	US Access Board	visitor
Lowe	Christopher	US Department of Agriculture	Presenter
Lullo	Joseph	DOJ	visitor
Manson	Antione	DHS	visitor
Maranto	Joseph	US Department of Education	Presenter
Marlowe	Michael	Automation Federation	visitor
McCornell	Bruce	DHS	Presenter
McPherson	Danny	Verisign	Presenter
Menna	Jenny	DHS	Presenter
Millar	Thomas	DHS	Presenter
Miller	John	Intel	visitor

LAST	FIRST	AFFILIATION	ROLE
Miller	W A	DOJ	visitor
Moore	Debbie Taylor	Cyber Zephyr LLC	visitor
Moore	George	DHS	visitor
Mullen	Elise	Senate Commerce Committee	visitor
Mustard	Steve	Automation Federation	visitor
Nagengast	John	AT&T	Presenter
Newton	Elaine	NIST	Presenter
Noble	Marc	ISC2	visitor
Nuriddin	Anthony Z	Scitor	visitor
Nye	John	Automation Federation	visitor
Odderstol	Thad	DHS	visitor
Osterweil	Eric	Verisign	visitor
Ozment	Andy	OMB	Presenter
Patchan	Andrew	Federal Reserve Board	Presenter
Phelps	Amy	NIST	visitor
Plocher	David	US GAO	Presenter
Plocher	David	US GAO	Presenter
Romine	Charles	NIST	visitor
Ross	Ron	NIST	Presenter
Saunders	Scott	Sacramento Municipal Utility	visitor
Scholl	Matthew	NIST	admin
Schwartz	Ari	DOC	Presenter
Scoh	Kristi	DOJ	visitor
Sedgewick	Adam	NIST	Presenter
Seeholzer	Roger	DHS	Presenter
Smith	Matthew	G2, Inc.	admin
Sokol	Annie	NIST	admin
Souppaya	Murugiah	NIST	visitor
Staples	Leo	Automation Federation	visitor
Stevens	Irena	TechAmerica	visitor
Stine	Kevin	NIST	Presenter
Streufert	John	DHS	Presenter
Suh	Paul	BAH	visitor
Thomas	Carlos A	eConsultants, Inc.	visitor
Vajjhala	Raghav	US Department of Treasury	Presenter
Vee	Christopher	SAIC	visitor
Walter	Jesse	The Asahi Shimban	Media
Waltermire	David	NIST	Presenter
Washington	Charles	US Access Board	visitor
Weber	Jim	Inside Washington	Media
White	David	Software Engineering Institute	visitor
Witte	Greg	G2, Inc.	visitor
Wisham	Lorna	First Energy	visitor
Wood	Alex	DOJ OPCL	visitor

Annex B

The following presents a series of questions from the Board and a summarization of Dr. Gallagher's responses:

Board: How can you operate quickly in a collaborative environment?
Dr. Gallagher: The key is having urgency designed in. Once you have made a decision, all parties are in step.

Board: How does NIST work with individual sectors?
Dr. Gallagher: NIST is a convener, we want to lean on those that participate to self organize into working groups. If we cast a broad net, we can catch many fish.

Board: What kinds of authorities need to be written into legislation for everybody to benefit fully?
Dr. Gallagher: Things that were not in the EO are up for legislation. Legislation should look to where authorities are inappropriate or inadequate.

Board: Suppose some of the derived standards are in conflict with current NIST products?
Dr. Gallagher: If derived standards push back on NIST, so be it. We'll deal with it and take it under advisement and blend it back into the process. If it does not make a difference in the standards, then the framework may be too superficial.

Board: Where is the bar for Cybersecurity?
Dr. Gallagher: It is DHS' role to set performance objectives. NIST's primary function is to ask: once you have accepted risk, how do you manage it? This work is not to produce new NIST guidance, but it is about enabling the critical infrastructure community to develop its own framework of practice. The key success component for this framework is not that it simply exists, but that it is put into practice.

Board: A set of incentives is due in 120 days - what is NIST's role in that?
Dr. Gallagher: NIST plans to utilize broad engagement of the private sector. A green paper is already out by Commerce asking incentive questions.

Board: How do we leverage existing frameworks? Sector-Specific Agencies (SSAs) were not set up to be regulatory, so how to keep the framework sustained?
Dr. Gallagher: There is no problem for having cohabitation in the process. The framework is a public/private partnership with many stakeholders. Industry leadership in the process will not preclude government input (some of which will be regulatory.) A standard is not tantamount to regulation.

Board: Who has the say in what their SSAs standards are?

Dr. Gallagher: This is a form of a self-governance model. NIST will help mediate the self-governance. NIST is a neutral third party in the whole process, present as a convener and subject matter expert. NIST's role will be prominent in beginning, then fades to industry leadership as the framework progresses.

Board: Is there a long term role for NIST?

Dr. Gallagher: The mission of NIST suggests yes. As long as Federal agencies are using the framework, then NIST will be involved.

Board: Is NIST properly resourced to do this?

Dr. Gallagher: There is nothing that can be done about budget right now. We just have to make it happen. NIST plans to leverage the players that come to the table to help out.

Board: With respect to the term "Government facilities," how much of the plan is IT related, and how much is plant related?

Dr. Gallagher: Some infrastructure is involved, there will be a lot of commonality between public and private.

Board: 120 days to provide a framework and 180 days for DHS to provide a demonstration – these are aggressive time frames. How will you handle them?

Dr. Gallagher: DHS will discuss this further in the next panel

Board: With respect to Information sharing, the EO states that public to private sharing will occur. Is the other way being put on legislation plate?

Dr. Gallagher: These are authority questions, the answers mostly rest in legislation. Government responsiveness will be addressed however. Privacy is also very important. Protection of information is critical in this effort.

Board: There will be differences in speed of adoption in the SSAs. How do you see leadership developing?

Dr. Gallagher: The goal is to quickly deliver best practices to other SSAs and if we see the same things happening in multiple sectors, make it part of cross-cutting standards.

Board: What is the biggest challenge NIST faces in accomplishing this work?

Dr. Gallagher: Organizational challenge. There will be lots of different types of participants. There will need to be a large commitment to act quickly. There will also be a headwind of misunderstanding. If standards are viewed as regulation, movement will be slow. There will be a lot of constant effort ensuring transparency of process and messaging of non regulation. Moving from a framework to actionable practice will also be difficult, general guidance versus sector specific implementation is a sticking point.

Dr. Gallagher: What considerations should we take?

Board: The Critical Infrastructure Protection Advisory Council (CPAC) process would help deal with regulation fears.

Board: There is no consensus about threat in the private sector, therefore is there no consensus on a reasonable amount of Cybersecurity?

Dr. Gallagher: Threat awareness is getting better. Information sharing will be critical to success. DHS's role will set baseline of performance, which will be a normalization process.

The Board indicated doubt on the private sector reacting to DHS guidance.

Board: What can the Board do to help?

Dr. Gallagher: Early steps will be important, what are things we should be paying attention to in regards to: stakeholders, thoughts about governance, How do we use this to drive consensus against a specific set of goals? Blind spots can happen, alert me to them.