INFORMATION SECURITY AND PRIVACY ADVISORY BOARD (ISPAB)

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

MINUTES OF MEETING

March 23, 24, and 25, 2016

U.S. Access Board
1331 F Street N.W., Suite 800, Washington, DC 20004, 20850
Agenda http://csrc.nist.gov/groups/SMA/ispab/documents/agenda/2016_agenda-ispab-march-meeting.pdf
ISPAB homepage http://csrc.nist.gov/groups/SMA/ispab/index.html

Board Members	Board Secretariat and NIST staff
Dr. Peter Weinberger, Chair, ISPAB, Google Dr. Ana I. Anton, Georgia Institute of Technology Chris Boyer, AT&T John R. Centafont, NSA Dave Cullinane, TruSTAR Technologies (joined via phone) Greg Garcia, McBee Strategics Consulting Jeffery Greene, Esq., Symantec Corporation Toby Levin (joined via phone) Edward Roback, US Department of Treasury Gale S. Stone, Social Security Administration **Absent with Regrets:** J. Daniel Toler, US Department of Homeland Security	Matt Scholl, NIST Annie Sokol, DFO, NIST Robin Drake, Exeter Government Services, LLC Warren Salisbury, Exeter Government Services, LLC

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

Wednesday, March 23, 2016

Welcome and Remarks

Dr. Peter Weinberger, Chair, ISPAB, Computer Scientist, Google

The Chair welcomed the members present and opened the meeting at 8:06 A.M. A quorum was not present at the start of the meeting. Dr. Ana Antòn, who was joining the board for the first time, introduced herself to the board.

Threat environment

Tom Blauvelt, Symantec Solutions Architect, Symantec (presentation provided)
Kent Landfield, Director, Standards and Technology Policy, Global Public Policy, Intel Corporation (presentation provided)
Christopher Porter, Senior Threat Intelligence Analyst, FireEye (presentation provided)

The Chair welcomed Tom Blauvelt from Symantec Corporation, Kent Landfield from Intel Corporation, and Christopher Porter from FireEye Inc. to the meeting to present current threats in the cybersecurity landscape. Attackers are moving faster, and successful attacks are increasing. The majority of larger companies have sustained increasing numbers of successful attacks against their infrastructure. Smaller and midsize business are increasingly coming under attack. Digital extortion is also on the rise. Malware is getting smarter; it is now virtually aware. It knows not to act in environments where attempts to detonate are present. Zero day threats are on the increase as well.

The time to compromise is beating time to discovery by an increasing amount. The good guys are not moving as quickly as the bad guys. Attackers are exploiting vulnerabilities more quickly and adjusting tactics. They blend in and stay entrenched in systems. Breaches are often not detected for months. Lack of investigative skill sets contributes to breaches not being discovered or analyzed. Meaningful intelligence and related workflows get mired in sharing difficulties, use and automation.

Anticipated security spending will increase dramatically over the next few years. However, breaches continue to increase despite already increased spending. Medical information has become a prized target for attackers. Increased federal spending has not cut the loss rate. Federal agencies have also seen increased attacks.

Statistics show fifty percent of online adults have been attacked in the last year. Cybercrime as a whole will cost 2 trillion dollars by 2019 worldwide. The Internet of Things (IoT) has grown exponentially, and the attack landscape has increased accordingly. Symantec did a vulnerability study and found that none of the fifty devices tested in the study used strong security. Most organizations surveyed in the study did not know where their sensitive information was.

Attacks succeed because basic cybersecurity is lacking. Most successful attacks only use basic hacking techniques. Cyber hygiene techniques include patch management, sensitive data protection, etc. Studies have shown that doing the following things can reduce attack risk by nearly ninety percent: White listing – knowing what applications and processes should be running in the environment; rapid operating system and application patching; and reducing administrative privileges.

The Department of Homeland Security (DHS) does different scans for organizations. Results from the cyber hygiene scan show the following three areas are at the top of the list of cybersecurity deficiencies: Patch management, sensitive data disclosure, and cross-site scripting. These have been longstanding issues, and are likely to remain so until there is a cultural change regarding cybersecurity.

Stolen credentials are the number one cause of breaches. Multi-Factor Authentication (MFA) is an effective measure against stolen credentials. MFA is a risk decision for every organization. Administrative users are starting to use Two-factor Authentication (TFA). Ease of adoption for TFA is still

an issue, but work is being done to improve ease of use. The top 500 passwords demonstrate that complexity of passwords is still a user issue, with "abc123" and similar combinations still being among the most frequently used.

Threat intelligence is coming into increasing use. Good repositories of threat intelligence exist, and sharing intelligence more quickly is a priority. Work is being done to make sure intelligence is usable and prioritized correctly. Sharing practices are improving. Many processes today are manual, which adds time to the response effort. The goal is to automate these efforts by analysts and greatly improve response time. On generating intelligence, various vendors are producing capabilities to detect new malicious payloads, with positive results. When combined with better analysis, there are better results. Improvement must continue in order to make progress. As organizations recover from incidents, they share lessons learned from those experiences. The real issue is getting organizations to utilize the information in a timely manner to defend against incidents.

A lot of things need to be done with the intelligence we do have. Detection is key, and it must occur quickly. The source must be determined-- where is it in the organization, what domains are involved, etc. Remedies may include new filters in email, or other necessary steps. Today these are manual processes; automation needs to replace manual processes if responses are to become rapid enough to actively deter attacks.

Response actions need to be orchestrated. Sharing threat intelligence involves knowing if threat intelligence is good. Policies can assist with taking appropriate action. People, service, and process issues exist in many places. Volumes of information exist, but the question is how to prioritize and make sense of all of it. Symantec is working in this area. Companies get information, but do not know what to do with it. There is a lot of information sharing, but in order to be valuable, intelligence requires context.

Determining that context requires human analysis on top of automated information sharing. Detection capabilities must react rapidly and then information must spread quickly across organizations. Determining IPs and domains are key determinants in taking action against malicious payloads. Once a threat is detected, often responses are not orchestrated or automated. Ideally, all control points ought to update automatically and immediately harden the environment against attacks. Progress starts with having the building blocks and a clear framework to work from.

Mr. Porter presented six general discussion topics: Lack of effective cyber deterrence has increased advanced persistent threat (APT) groups; sophisticated groups do not rely on zero days (APTs now have the capability to turn the operating system against itself), Commoditization of cybercrime has spread APT-like threats worldwide, threat groups are figuring out the formula for causing critical infrastructure outages, and threats to mobile are likely to rise precipitously following the FBI case against Apple. Intelligence sharing (intelligence is defined as information within a context), is necessary to improve protection from cyber threats.

It used to be true that there were more opportunities for attacks than actual attacks. The world is no longer that way. These days, attacks are bolder. Threat groups are figuring out how to cause critical infrastructure outages.

A documented attack from the APT29 group used spam-style email. The attacks did not target individuals. Phishing by the Russians was strongly suspected behind APT29. APT29 used links to legitimate, compromised websites. Operationally, it is very difficult to detect. Real voicemails were also used as lures to steal information. The attack escalates privileges within the network by using built-in and publically available Windows tools without writing anything to disk.

Malware now does not need to write to disk to be effective. These types of malware use legitimate system privileges to accomplish goals against targeted systems. Threats like APT29 must be actively hunted to discover them; passive network-edge detection does not work. Organizations must actively hunt to detect this type of attack. The need for active hunting is especially true of government systems as they are closely interconnected. Attackers targeted system administrators personally, to the extent they would know when companies bring in remediation measures.

The cybercrime market has matured. APT-like behavior is now being shown by criminal groups. The Board asked why we are not breaking into bad-guy machines. Why not steal zero days? There are numerous ways to collect threat intelligence. Why is it not routinely done? Threat attribution is a challenge. To develop a steady stream of zero days, requires some economy of scale.

There are companies for hire who create zero days and sell them. Is there action from government to have a financial impact on this activity? These questions will be covered under the Wassenaar discussion. Does the government track crypto-currency? In the zero-day market, crypto-currency obscures transaction participants, but the actual transaction is in the open. Cybercriminals are not APTs. APTs can use criminal tools to conduct attacks. It makes it difficult to distinguish between APTs and cyber criminals.

An area of expanding threats involves password theft for critical individuals in organizations. It involves targeting individuals directly rather than corporations to attempt to get internal access. Commodity ransomware has ended up in critical infrastructure, causing outages. Precedents indicate worsening threats to mobile. FireEye continuously tracks fifteen Chinese groups that go after telecommunications companies, stealing intellectual property and blueprints, pre-signed software, etc.

Do APTs incorporate vulnerabilities into code? Chinese actors have been known to cause this activity. It is a long term industry wide phenomenon. There are examples in China of legitimate software certifications on malware. Sometimes law enforcement-only tools fall into the wrong hands. The line between law enforcement and the cyber-mafia can become pretty thin. There are at least nine APT groups that target specific ethnic groups and others. APT29 has been exposed many times, but with no demonstrable effect on their operational tempo at all. Indicators alone may not be sufficient to expose APTs. Actors may leave signs for other APT groups in the form of using certain tools.

What is effective cyber-deterrence? Broadly speaking, it means making an impact on the risk-reward calculus. Deterrence in that context needs to be actual deterrence. Pointing out actors later after an incident has little value once the damage has been done.

The need for vulnerability disclosure is expanding into many types of devices. Safety becomes part of the process too. The cyber-physical aspect also comes into play. There must be a better way to register

vulnerabilities, etc. It has to become much more effective than it has been in the past. It is not a legacy software problem anymore. The National Telecommunications and Information Administration (NTIA) effort last year merged disclosure process development work with the FIRST.org vulnerability coordination special interest group (SIG). Vulnerability disclosure should be a living process with living documentation.

Government plays a role in safety. Government safety processes could be useful in this environment. The NTIA and Forum Incident Response and Security Teams (FIRST) are on the right track with their joint effort in producing a beneficial effect on the emerging digital economy.

We must have the capability to identify the vulnerability itself. At least 80% of cyber hygiene problems come from not dealing with basic issues. Vulnerability identification has become necessary for many different technologies. It must be able to deal with basic-level as well as the newest large scale attacks. Vendor bulletins to deal with identifying vulnerabilities will become increasingly common in the future.

There needs to be a single means to identify vulnerabilities in the software of devices. Common Vulnerabilities and Exposures (CVE) is the foundational means for vulnerability identification. It has become radically eroded in its scope. It is not global, but has become US-based and English-language limited.

The Board asked if CVE is also for user control. It is used in that context. Does it impact the time of receipt and time of patching? It is used downstream of CVE to identify and determine the criticality of the vulnerability. CVE is important for locating vulnerabilities within the federal network. Most vendors cannot check for multiple types of vulnerabilities. The need to be able to do this exists. There are international systems that identify vulnerabilities. Some of them map to CVE. Vendor security updates are not what they need to be. Vendors also cannot check for vulnerabilities they do not know about.

There is not a good global approach to identifying vulnerabilities. CVE has been underfunded for many years. CVEs target US software/English speaking software only. Open source software is not well covered from a vulnerability perspective. Delays in getting CVEs issued causes problems in the research community. MITRE will reject submitted CVEs for being "out of scope". CVEs should cover every issue, but do not. Differences exist in vendor-tracked numbers of vulnerabilities and actual CVE vulnerability representation.

Hardware is not represented in CVE. As devices have more sensor capabilities, this will need to change. There is a large migration to open source software going on. The CVE is working with Red Hat and others. Legislators also cause problems. The Royce bill as implemented could be an issue. Does MITRE control what's in a CVE? MITRE runs the program, and as part of the program they have an editorial board. They have done a lot of good work. On the retail side, the work is done by MITRE. Large organizations can purchase large blocks of CVEs for their use which ultimately become part of the National Vulnerability Database (NVD).

There is a desire to create a federated model for CVEs so that others besides MITRE can initiate CVEs. The CVE program needs to be re-vamped to address current threats in the global landscape. The need exists to take a solid look at the program and what it's doing. There must be vulnerability identification

capabilities, or disclosure won't work and fixing problems will be impossible. Plans for the future need to happen now. CVE has US impact but the impact truly is global. FIRST is working on global database exchange capability.

Cyber-physical systems are influencing the need for more a holistic model. New models for threat sharing are emerging. ISAO is being redefined from the 2002 legislation due the executive order. There is an effort to develop information sharing guidelines. CSA is affecting corporate legal perspectives. It provided liability protection that is changing legal perspectives on these areas. It was easier to shut down sharing rather than to try to make changes. The cyber security act has re-opened these types of conversations. The cyber security framework has been well received but there are missing aspects in cyber threat management and cyber threat intelligence sharing.

The Commerce Data Service

Dr. Tyrone Grandison, Deputy Chief Data Officer, Commerce Data Service, US Department of Commerce (presentation provided)

The Chair welcomed Dr. Tyrone Grandison from the Department of Commerce (DOC), to the meeting to update the Board on the Commerce Data Service (CDS),[1] which is DOC has a new startup. Presently, there is a team of 15 that will be expanding to about 100 people in the next six months. The CDS is the initiative for data projects across the entire DOC. CDS wants to change how people are able to interact with government web sites. The CDS mission, "Maximize the positive impacts of commerce data on society."

Major 2016 Initiatives include fueling economic growth, creating data-driven government, and delivering data services. Most government sites were built with compliance in mind, rather than usability. The mission is to make the most positive impact on society.

Project priorities for 2016 include: Trade Data - Many companies are not exporting that could be (helps to create jobs). Income data: Provide people with true understanding and access to data and what it means. The discussion is more academic at present. Patent data modernization: Overhauling the patent system which has not been updated in over 20 years. The goal: Determine how to modernize so that it is possible to get a patent in 3 hours. Dr. Grandison asserts it will happen this year.

The DOC builds and delivers data products; consults on strategies and technologies; training; partnering; assisting with procurement – the single most difficult thing to do in government. DOC assists with procuring software and data products. The DOC data usability rule - Data should be available and useful. DOC data portrays what is happening in the economy, and what is happening in the lives of Americans.

Users of the CDS should have or choose an empowered product owner, have read the stakeholder guidelines documents, have the expectation of a user-centered design, expect that goals will evolve over the course of any project, expect to have lessons learned and immediately derive the benefit of that experience, and be prepared to collaborate during the process.

[1] https://www.commerce.gov/dataservice/

The DOC was extraordinarily helpful in working with NIST, and took great care to make sure the information presented conveyed what was intended. The Board noted it is important to standardize procedures so that the current momentum and enthusiasm for projects continue onward into the future.

One project is Making Income Data Available as a Service data on the MIDAAS site. Conversations on pay are always in the abstract, rather than being based on concrete data. Pay inequality is known to be about $.80 on the dollar for women vs men. It is interesting to note that upper income levels show a greater disparity between men's and women's pay. Regional differences also exist in the size of the disparity between men's and women's pay across the US.

The Opportunity project looks at data sets across Commerce and other agencies to provide people with data to give access and opportunity. Commerce partnered with 50 companies to assist with creating opportunities. Is there a relation with 18F? Dr. Grandison and other staff worked formerly with 18F. The Help Girls of Color project was developed in conjunction with the City of Baltimore on how to collect data and impact policy. The project asked for help to raise awareness of the situation in Baltimore and providing data sets.

DOC hopes to deliver an increase in companies exporting goods. The Commerce Data Academy[2] offers fast courses on technology related topics. Response to the course offerings was well over anticipated levels. CDS is working on web re-design with NOAA[3] on its data portal and BEA[4] RIMS.[5] RIMS calculates impact of creating any new job on the local economy where the job was created. NOAA generates 20-30 terabytes of data every day. Access to the data currently is very difficult. The Big Data project at NOAA is working to make its vast data resources more readily available. Patent data work includes a developer portal, big data science models, and infrastructure for data science projects.

How do tools get chosen? They try to demonstrate a diversity of tools. New tools can be requested through the site. How do projects start? Does the service work on self-generated projects? Projects can come from other bureaus, looking for projects that cut costs. Are there any external projects? Yes, they do occur. Does the DOC work with academic data scientists? The group would love to work with academic data scientists. The services are working with five universities currently. More are always welcome.

[2] http://commercedataservice.github.io/Commerce_Data_Academy_Courses/
[3] National Oceanic and Atmosphere Administration http://www.noaa.gov/
[4] Bureau of Economic Analysis
[5] Regional Input-Output Modeling System http://bea.gov/regional/rims/

Wassenaar Cybersecurity and Export Control [6] [7]

Bob Rarog, Senior Advisor to the Assistant Secretary for Export Administration, Bureau of Industry and Security, US Department of Commerce

The Chair welcomed Bob Rarog from the DOC to the meeting to provide updates on Wassenaar Cybersecurity and Export Control. Mr. Rarog began with the background of what has transpired since June, 2015 when he last appeared before the Board. The Federal Register published a notice in May 2015 that would have implemented Wassenaar.[8] Wassenaar is a multi-lateral organization with 41 member nations. Most of the US major allies are members. It develops export control language and seeks agreement for that language. Controls are proposed annually. Technical meetings are held and members sign off occurs in December. Sign off must be unanimous. The concern here is the controls for command and delivery for network intrusion which were agreed to in 2013. In this case, there was a great deal of discussion among agencies. The meetings took place in Vienna. Technical specialists from multiple agencies attended and participated in the drafting of those rules in 2013.The discussion concerned how to handle the actual implementation. The particular controls being discussed related to commercial products that are already controlled. The products use encryption.

A conservative implementation was put forth last May. The interpretation last May was that only a narrow band of products would be impacted. The rule required licensing everywhere except Canada. A large number of comments, mainly negative, were received for the proposal presented last year.

An outreach program was started to talk to companies, agencies, and others affected by this action. It became evident very quickly that there were unanticipated impacts. There was an immediate effect on cybersecurity activity. Impacts reached way beyond the product development aspect it was intended to address. The European Union and others implemented before the US. The level of activity in the US is greater than Europe. Many national implementations were very limited. At a higher level, within companies and governments, export compliance is independent of other functions such as cybersecurity. Often, cybersecurity personnel are not aware of export activity relating to them. Rules are formally vetted with government agencies. At that point, action needed to be taken. More input from the cybersecurity community needed to be integrated into the US implementation of the rule.

There was an announcement on the first of March. The US has already returned to Wassenaar with a proposal to eliminate an important part of these controls 4e1c. An additional part of the proposal is to look at hardware and software controls, and re-open the discussion. When the original notice was published, the analysis was very brief.

The technology problem has been dealt with (as far as the US is concerned). The US must make its case before the Wassenaar membership. However, the US implementation is not up for discussion now. The Wassenaar language is the focus now. It impacts US firms and how issues are managed internationally.

---

[6] http://www.csmonitor.com/World/Passcode/2016/0302/State-Department-reverses-course-on-cybersecurity-exports
[7] https://oversight.house.gov/hearing/wassenaar-cybersecurity-and-export-control/
[8] https://www.federalregister.gov/articles/2015/05/21/2015-10579/wassenaar-arrangement-2014-plenary-agreements-implementation-and-country-policy-amendments; https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items

The focus is on the hardware and software controls. There will be meetings in Vienna to discuss the language for the hardware and software controls. The first meeting will be in April. The members are now examining specifics of the Wassenaar language. There are advantages currently; government and outreach has produced an integrated approach. There are multiple proposals on how to fix the language. It is possible that the US will not be able to make a change. Discussion with the Wassenaar allies will take place. No conclusions have been reached as of today. Some proposals have been reviewed, representing similar groups of ideas. Some originated from the academic community, and some from the private sector. The US will not know what kind of support it will have for its proposals until the meeting happens.

Different types of solutions have been proposed. Regulatory language always has some room for interpretation. One of the issues is that the cybersecurity community does not have the capacity or possibly the time to make an interpretation. Mr. Rarog is encouraging companies and organizations to bring specific recommendations for the hardware and software language and encouraging them to make the case internationally. The cybersecurity function in the US has become much more integrated. The entire process does not need to occur in the next three weeks, prior to the meeting. Export control has a legitimate role in cybersecurity, but what the role is must be examined closely. The final thing is awareness of the issue has proliferated to Wassenaar allies and organizations outside the US. Much progress has been made. It may be awhile until there is a proposal. There is no timeline at present. The regulatory fix will occur.

Implementation of any of these changes will have a ripple effect in the membership. Members will also have to make changes.

Commission on Enhancing National Cybersecurity [9]

Kiersten Todt, Executive Director, Commission on Enhancing National Cybersecurity, NIST
Kevin Stine, Chief, Applied Cybersecurity Division, ITL, NIST

The Chair welcomed Kiersten Todt and Kevin Stine from NIST to the meeting to discuss the Commission on Enhancing National Cybersecurity. Ms. Todt and Mr. Stine will be talking about the Executive Order – Commission on Enhancing National Cybersecurity[10] and NIST's role in the commission. There are two primary charges. The first is to make recommendations, and then to position us to take advantage of advances in IT. The commission will make actionable recommendations. There are many existing efforts. The commission will attempt to identify problems and present actionable solutions.

The goal is to identify a number of area in which to make short and long term recommendations, in order to promote something actionable. NIST's role is provide the commission and the executive director with the necessary support to accomplish its goal. It is incumbent on the commission to build on existing things that work and to be ambitious in accomplishing more.

There is an existing problem with cyber hygiene. The commission is seeking to identify and address issues to create a cultural shift regarding cybersecurity. Americans do make cultural shifts in the area of

[9] https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancings-national-cybersecurity
[10] https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-commission-enhancing-national-cybersecurity

safety. Lack of cyber hygiene is a symptom of lack of education and awareness. The commission will need to define challenges and issues concretely through the use of policies, etc.

What is the appropriate goal of government? It's a combination of defense-driven and corporate-practitioner type solutions. One of the challenges facing the commission is that attacks have become so sophisticated that it is difficult for the average person to comprehend they may fall victim. How will technology deal with response activities? Cyber hygiene and dealing with fall-out from specific attacks will have roles in any response.

The Board asked how the members of the commission will be selected. Ultimately, there will not more than twelve members, with four will be recommended by congress. This is an independent commission, which will develop independent recommendations. Accountability of the commission lies in the executive order. Vetting has been proceeding. It will be done in the near term. The anticipation is that the full commission will be ready in the next few weeks. The final recommendations will be delivered to the President on December 1, 2016. The report will be a dynamic, nonpartisan, non-political document. The commission will look forward to seeing the recommendations in action a year from now. There must be a resilient infrastructure that will keep up with technology.

The commission will rely on input from ISPAB in the areas where it may participate. We will need to determine where education on cybersecurity has not been effective. Educating the public has to be simple, and limit its focus to a couple of areas at a time until they are assimilated. The unfortunate aspect is that it only takes one person to click on a link to launch an attack on a network. There has to be a focus on awareness. The chance that one percent that will click, will always be there. The work plan for the commission lays out a series of public engagements with participants from the private sector and others. Success is defined as acceptance of the contents of the report to be delivered. It will actually present actionable recommendations.

The Chair commented the culture of senior management of public and private sectors who often make wrong decisions regarding risks must be changed. The audiences for this commission include senior executive management. It will not be a technical document. It will be written so that lay people can understand the contents. It will contain technical portions, but the main document will be accessible, and backed up by technical information. The goal is to look at things differently, and to discover what's working and what's not.

The Board commented that at some level, are not the problems fundamentally technical? The hope has been to fix the problems without fixing the technology. The problems cannot be fixed without fixing the technology. The general feeling is there are technologies that can fix the existing problems, but the human factor in cybersecurity must also be dealt with. The hope is the commission will find something new, rather than reproducing what already exists. The commission hopes to look at existing problems in a new light, and further establishing best practices. The members of the commission will be trying to define what is working and what doesn’t. There is a two-fold focus of keeping track of basics (cyber-hygiene), and not losing sight of the longer term goals.

The trouble is companies don't want to be told that they have to rearrange their internal processes and incur a large cost. Companies do make changes, and the issue is that the point comes where they must adapt (stop postponing needed changes). Government and the private sector are often held hostage to trends. The commission hopes to strike a balance between what exists and looking forward to what is new. It comes back to whether we're gaining on the threat or falling further behind. It's difficult to see that generally acceptable recommendations from the commission will help to gain on the threat. The commission's goal is to provide solutions within the recommendations that will provide a path forward that represents true progress.

Until the risk gets quantified, people may not feel cybersecurity is worth investing in, or see it is a major problem. The position with cybersecurity ultimately needs to be that no loss is acceptable. Any destruction or disruption, or loss of profit is not acceptable. There is momentum created by repetitive effort, it is the hope that the commission will change the momentum.

The security/technology trade off exists. Audiences for the document will impact how the recommendations are tiered in the final document. The executive order mentions the government, and some of it will be un-doable. Scoping will be one of the critical issues facing the commission. Cybersecurity is the umbrella for the report, and the story that will be told by the report.

Cybersecurity Ratings in the Auto Industry

Jacob Olcott, Vice President, BitSight Technologies (presentation provided)

The Chair welcomed Jacob Olcott from BitSight Technologies to the meeting to update the Board on cybersecurity ratings in the auto industry. The idea of cybersecurity for autos is in a very early stage. The main issues are vulnerabilities that can be exploited to cause harm to drivers, and major themes at RSA involving the internet of things and supply chain security. How are manufacturers working to address these problems? There are a variety of things underway.

Are consumers concerned with cybersecurity? Does it impact buying decisions? This is the focus. Ratings come into play such as crash test ratings, along with other manufacturer ratings and how consumers perceive those ratings.

Statistics from Kelley Blue Book indicate of those surveyed:

- 72% have awareness of the Jeep hacking incident (2015).
- 41% say they will consider the possibility of hacking when buying/leasing their next car.
- 78% say they believe hacking will be a frequent problem within the next 3 years.
- 81% think the auto manufacturer is most responsible to secure cars from hacking.
- 64% prefer to go to the dealership to get security patches installed.

How should patches be installed? The choices are over-the-air remotely or uploaded at the dealer. Two thirds of those surveyed want to take the car to the dealer to get patches.

In contrast, the following impressions came from consumers surveyed in March 2016 (Kelley Blue Book):

- 26% recall an incident of vehicle hacking (note contrast to previous statistics).
- 73% believe hacking will be a moderate/serious problem in next three years.

Of these, millennials as a group are the least concerned about vehicle hacking. It is interesting to note the majority of millennials support more connected vehicles. Technology is a crucial element in a vehicle purchase for millennials. Right now, of the top ten safety concerns for millennials note that the first is other drivers; vehicle hacking ranks ninth; and carjacking ranks tenth. Slightly over half of millennials believe the vehicle manufacturer is responsible for keeping the vehicle safe.

Nearly half of consumers surveyed are willing to pay an extra fee for software ($8.98 per month). Over half would pay for additional insurance to cover hacking ($9.31/month). Millennials will pay more for software and insurance. Kelley Blue Book may be conducting this survey annually going forward. "Hacking" in this context is defined as impacting vehicle safety. As connectivity between applications increases, the danger to personal data in vehicles also increases. There are initiatives underway to share information on vulnerabilities and threats. The Auto-ISAC is doing work in this area.

Auto manufacturers are sponsoring research in these areas and NHTSA[11] is doing research as well. Major universities are conducting research. The Board asked if manufacturers have started doing bug bounties. GM[12] and Tesla have offered bug bounties. Businesses are also offering to run bug bounties.

Senator Markey introduced the "Security and Privacy in Your Car" (SPY) Act[13] on security and privacy in cars. His office released a report on security and privacy gaps faced by American drivers. Letters were sent to the major American manufacturers requesting information on security, how updates are handled, and a list of other areas. The bill requires car manufactures to implement "reasonable measures" to prevent car hacking, and develop designs to isolate critical systems. They must also implement some sort of transparent cyber dashboard that displays an evaluation to inform consumers about measures.

The dashboard should be available to consumers with information for consumers to evaluate the cyber security level of the car. What would representations from manufacturers look like as it relates to the dashboard? Safety of the automobile is paramount. Consumers have made it clear they care most about the durability and safety of automobiles. Crash test ratings do not measure cybersecurity as an indicator of vehicle safety. The cybersecurity dashboard as proposed by Senator Markey may be an appropriate way to provide cybersecurity information. There are proponents for using the crash test rating to provide cybersecurity ratings because it is familiar to consumers.

Senator Markey is also concerned with personal data in cars and vehicle safety. In the future, there could be a rating that gives security information. NTHSA came into being as a result of insurance companies being concerned about crash safety.

Insurance companies have technologies to put in cars today that enable consumers to get better rates on premiums. They are already thinking about cybersecurity technologies that can go into cars. Universally, insurance companies are deeply concerned about underwriting insurance in an

[11] National Highway Traffic Safety Administration http://www.nhtsa.gov/
[12] Genera; Motors http://www.gm.com/index.html
[13] https://www.markey.senate.gov/imo/media/doc/SPY%20Car%20legislation.pdf

interconnected internet of things space. The industry wide approach to cybersecurity insurance is uncertain at this time.

When dealing with cybersecurity in cars, there may be a line between malicious intent, and poorly designed solutions. From an insurance perspective, it is more concerned with the aggregated risk, which if exploited, would cause a significant number of cars to run off the road. Insurance companies were forced to re-assess aggregated risk following Hurricane Andrew in '92. A number of insurance companies went out of business because too many companies wrote policies for hurricane or flood prior to a landmark storm.

Cyber-insurance policies are available that cover against loss and forensics and legal fees. Insurance policies are reexamining D&O (Director and Officer) policies. They are uncertain of the liability caused in a director and officer liability situation.

A dashboard can be imagined in a number of different ways. The question is how to provide certification to another party regarding cybersecurity fitness? How much detail would those certifications have to have? Should there be an independent analysis of code? How would the result be represented to consumers? All these elements are extremely complex, and making a representation would be extremely difficult. Cyber security product ratings are in a very early stage at this time. BitSight is developing security ratings for organizations. Other initiatives attempting ratings of companies and other entities are beginning to emerge.

The movement toward transparency in the process is becoming stronger. Businesses understand there is a greater need for transparency. Again, insurance companies are an influence in transparency. Insurance companies are asking more questions about the security of information. The role of government vs the role of the market is a topic for debate. Times have changed, and cybersecurity reflects a different type of threat than earlier threats from decades ago. There is an emerging marketplace for cybersecurity ratings for applications and other technologies. What is the role of government? The private sector? For many companies, brand impact is a critical consideration. Reputation insurance exists. Cybersecurity ratings in vehicles encompass hardware and software, but also providing services. In the future, privately owned cars will not exist at least in urban areas. Use of vehicles will be by subscription. Protection of corporately owned fleets of cars will become the responsibility of the owner of the vehicle rather than the passenger in the vehicle.

National Cybersecurity Assessments and Technical Services (NCATS) – Service Overview, Success and Challenges [14]

Ken Vrooman, Cyber Hygiene Program Manager, U.S. Department of Homeland Security (DHS), National Cybersecurity and Communications Center
Krysta Coble, NCATS Team Member, DHS, National Cybersecurity and Communications Center
Will Burke, NCATS Team Member, DHS, National Cybersecurity and Communications Center

The Chair welcomed Ken Vrooman, Will Burke, and Krysta Coble from the US Department of Homeland Security to the meeting to update the Board on NCATS successes and challenges. NCATS is a hands-on testing organization. They do testing to identify problems on networks before they become incidents or issues. NCATS offers two services: a cyber hygiene program, and risk and vulnerability assessments. The group will also discuss its pilot programs.

They consider themselves a penetration testing team. There are government experts and respected contractors who work with them. There is a high level of capability within the program. The staff stays current with what's going on, and is very dynamic. They run risk and vulnerability assessments on-site and run external components of those assessments. The cyber hygiene program runs from the NCATS lab. The risk and vulnerability assessment has internal and onsite components. Services provided get tailored to the customer. Some customers only want basic cyber hygiene services. The team acts in a trusted advisor capacity where requested. Their work takes place in addition to regular audits that the organization may hold. NCATS simulates the bad guy, and determines what problems can be exploited by an attacker.

NCATS provides services to federal civilian branch agencies. They also work with state, local and private sector groups with a focus on critical infrastructure. The number of stakeholders is growing. Some services are available for a cyber hygiene program. The vulnerability testing is a full service program. There is no charge for these services. Once people use the service, they spread the word about their experience. NCATS works as part of reducing risk across the nation. There is a need to maintain expertise in these areas. Statistics on cyber security trends (clicks on phishing links for example), is the value from the program back to the government. NCATS operates under a rules of engagement agreement between the parties involved. The Board asked what is budget of the program. Vulnerability assessments cost approximately $55,000 each. Cyber hygiene is very inexpensive because it is automated. NCATS runs onsite assessments; other DHS assessments are comprised of desktop or voluntary sharing with DHS.

Risk and Vulnerability Assessment (RVA)[15] services include cyber hygiene and risk and vulnerability assessments. Systems with high vulnerability will scan on a daily basis. This provides new insights into changes in subject systems. Is cross site scripting done? Web scanning is not mature. There are many false positives. Everything is un-credentialed. RVA involves senior engineers assessing the network. Customers can choose from the set of available services. An assessment consists of one week of external testing, and one week of internal testing. Findings from the penetration test require manual testing.

[14] http://krebsonsecurity.com/wp-content/uploads/2015/11/DHS-NCATS-FY14-Annual-Report.pdf
[15] http://thehill.com/policy/cybersecurity/261658-dhs-hacks-businesses-for-free-to-test-cybersecurity

Web applications often require manual testing. It is often a cascade of lesser vulnerabilities that brings out the most extreme vulnerabilities during testing. They are able to send phishing emails and record the number of clicks on those emails. They do have the capability to send a malicious payload, and provide call backs to the lab for those workstations that contain malicious payloads.

The web application scanning service is one of the most popular. It is also the most labor intensive. Cross-site scripting involves manual testing and it is labor intensive. Database scanning and operating system testing is a set of tools that is used. Database scanning is useful in determining whether proper permissions exist and whether default passwords and missing patches exist.

NCATS was asked by the White House to test high value assets. They scanned multiple agencies in a two-week period. They were able to send payloads and be on the inside of the agency. They did a web application assessment, and found little advantage. Between the phishing campaign and the internal networks, they were able to act like an insider threat and acquire information. There were systems in place to stop the outflow of information.

Heartbleed scanning was done during the cyber hygiene program. The scan reduced the Heartbleed vulnerability by 98% in the government environment. DHS issued a binding operational directive to allow scanning by the cyber hygiene program and any vulnerabilities discovered must be fixed in thirty days. From a policy perspective, the binding operational directive dealt with critical vulnerabilities. When the critical vulnerabilities have been dealt with, attention then turns to non-mandated lower threats.

Offensive Security Assessment (OSA) pilots involve external testing only in the National Cybersecurity and Communications Integration Center (NCCIC) Lab and lasts 90 days. Working at the lab allows the team to undertake simultaneous engagements. The goal is to train agencies to identify breaches. RVA looks for types of vulnerability in a network. The OSA looks for targets and how to achieve those targets. Using a true red team capability, they measure response and sharing of indicators of compromise (IOC). They find their own way into the network and use social media. They start with open source information gathering (web, LinkedIn, etc.) to try to get a picture of the network and the individual involved. Targets are selected based on the open source information gathering, and the process starts "low and slow". The first attempts involve things network security personnel should see. Trusted agents on the inside monitor the response and what is done with the information. The OSA groups track everything the trusted agents do as well. As things continue, they track response times with the goals that response time decreases.

OSA is still in the first offensive security assessment with one customer. It is planned to become a formalized program in FY17, and fully in action by FY18. There are three teams working independently and sharing information across three modules. There is one federal employee lead in charge of every module, with individual team members being able to change out as needed. It is much more focused and streamlined. The first module involves the initial foothold and persistence team. They do the initial research with the goal to try to get the initial foothold in the network. The task then is to entrench in that system, then to hand off to the second module.

There is a 4-person team for the pilot. Teams may become larger depending on the growth of the program. They have been able to hire people with the right skills. While module 2 works, module 1 can start other customers or continue with the current. There is a mix of federal and contractor personnel.

Module 2 is the privilege escalation team. They take the initial foothold and try to expand that access until they have admin domain and enterprise admin access. If they discover systems that appear to contain vital information, they establish persistence on that system and pass that information to module 3, the data analysis team. The data analysis team will determine what "crown jewels" might be on that system. All modules work together while the entire process is going on. They are able to demonstrate what was done on the system without actually removing data or causing damage.

The modules use different tools. There is no work on any classified sites. They use 3 commercially available tools and custom scripting. Some of the newer tools were written by NCATS contractors to automate certain portions of the investigation process. The rapid response team was created out of a specific need. The team investigates suspected breaches upon request based on information provided by the company. The rapid response team responds within 2 days of getting a request. They had a rapid response in early 2016, found a problem did exist, and the company fixed the problem.

Phishing is the major means NCATS uses to get into stakeholder organizations. They are hoping to increase stakeholder education. The phishing campaign entails a 90-day engagement period with stakeholders. The stakeholder provides a list of target users. They monitor click rates only, with no payloads being used. The objective is to increase security awareness, decrease potential threat of successful attacks, and provide meaningful and actionable measures.

The phishing service is in the process of being piloted. There are two different issues involved, the user problem and the infrastructure problem. The user problem can generally be remedied with user training. The infrastructure problem is more complex. Payloads need to be stopped on the workstation, and outbound call backs need to be prevented. The primary focus at the present time is on the click rate.

NCATS is introducing complexity levels for calculating the difficulty to identify indicators of a crafted phishing email. There are ten levels ranging from 0-10, easy to difficult. There are four categories of indicators: appearance, sender relevancy, behavior, and emotion.

Agencies wishing to request services can email to the address in the presentation. NCATS will respond with an information pack. There is some need for legal review of the rules of engagement as NCATS is accessing agency networks. The rules of engagement document lives until someone in the agency dictates the document be cancelled. Business is very good. The cyber hygiene scans can be done in about a week. RVAs have a six month plus waiting list at the present time. Anyone, including private sector companies, can get in the queue to get RVAs. NCATS does not schedule an RVA until the signed paperwork is received.

Updates on Information Sharing and Analysis Organizations (ISAOs) Update (presentation provided)

Chris Boyer, (Moderator) Assistant Vice President, Global Public Policy, AT&T Services Inc. / Co-Chair, Cyber Policy Subcommittee, US Communications Sector, Coordinating Council (CSCC)

Kathryn Condello, Director, National Security, CenturyLink / Vice Chair, Executive Committee CSCC

Joe Viens, Time Warner Cable Inc. / Chair, Communications, Information Sharing and Analysis Centers (Comm-ISAC)

The Chair welcomed Chris Boyer from AT&T, Kathryn Condello from Century Link, and Joe Viens from Time Warner Cable to the meeting to update the Board on ISAOs. There are several activities going on at Communications Security, Reliability and Interoperability Council (CSRIC) currently relating to cybersecurity. The presentation today will focus on Working Group 5 (WG5): Cybersecurity Information Sharing, which is focused on information sharing. There are three working groups: information sharing, supply chain security, and work force development issues. There is also a new working group concentrating on wireless issues.

WG5 will be making recommendations to improve response to cyber-attacks and information sharing. There are approximately 100 people in the working group. Final recommendations will be made in March 2017. The cybersecurity working group is working to improve the ability to respond to cyberattacks by improving information sharing. WG5 consists of communications industry membership.

The notional diagram (Slide #5) provided in the presentation is intended to be industry centric, not ISP centric. The left of the diagram displays private-to-private and industry-based sharing relationships. It depicts formality of relationship and structure of data. Use cases for each type of relationship have been developed. The types of relationships are private-to-private and private-government-private. Private-to-private is intended to represent contractual relationships without being vendor-specific. Formality of relationships can be determined as "Formal Unstructured", "Formal Structured", "Informal Unstructured", and "Informal Structured".

There will be a use case to represent each case study. There is no one-size-fits-all model for the industry. Once all use cases are complete, the group will schedule another face-to-face meeting, slated to happen in the second quarter 2016 timeframe, to make recommendations. An interim report will be drafted in June 2016 to outline barriers/challenges and to provide periodic updates to the steering committee and the council. There is great sensitivity regarding sharing customer and enterprise data. The diagram is intended to illustrate the industry as it exists today.

The ISAO standards organization was started last year by an executive order. The President called for DHS to issue a grant to start a standards organization and provide guidance for groups wanting to start an ISAO. The initiative is trying to go after underserved communities that want to participate, but do not know how to go about it.

DHS awarded a multi-year grant to the University of Texas San Antonio (UTSA). There are six working groups on a range of topics. WG5 is offering its expertise to the sub-working groups that are involved. The timeline is somewhat aggressive with initial deliverable is due in May to provide basic guidance on ISAOs. The full standards guidance is currently due in September 2016.

WG5 would not refuse to assist smaller entities requesting aid. Information sharing is occurring outside the government. It is difficult to determine what is relevant to particular organizations. Much of the information being shared is not cyber-related. It is challenging for large organizations to sort through and make sense of all the information they receive. Smaller organizations can have a much more difficult time. The percentage of information that might really be actionable is very small compared to the whole.

Sometimes there is a tradeoff between reporting speed and credibility. An indicator may point to the possibility of a major issue that's coming. Waiting may provide clarity as to the scope. ISPs and vendors can work quietly to research and figure out a fix. Certain situations benefit from reacting to particular activity. It gives the capability to react quickly to provide a fix to the affected parties, followed by general information sharing if the level of severity warrants. The government is working on a cybersecurity incident response plan. It is complex, but is necessary. The focus is on industry-out, federal-down, and state-up.

Meeting Recessed

The meeting recessed at 5:37 P.M., Wednesday, March 23, 2016.

Thursday, March 24, 2016

The Chair called the meeting to order at 8:30 A.M.

Cryptographic Module Validation Program (CMVP) (presentation provided)
Michael J. Cooper, Group Manager, Security Test, Validation and Measurement Group (STVM), Computer Security Division (CSD), ITL, NIST
Melanie R. Cook, Operations Team Lead, STVM, CSD, ITL, NIST
Apostol Vassilev, Ph.D., Research Lead, STVM, CSD, ITL, NIST

The Chair welcomed Michael J. Cooper, Melanie R. Cook, and Apostol Vassilev, all from NIST, to the meeting to update the Board on the Cryptographic Module Validation Program (CMVP) program. Mr. Vassilev noted FIPS 140 (The Federal Information Processing Standard Publication) *Security Requirements for Cryptographic Modules* was issued in 1994. It was developed as a standard by government and industry working groups. Once the standard was established, NIST created the CMVP. The "clipper chip" controversy was occurring at the time. Cryptography took off following this controversy. It was developed in the context of great technological progress that has been ongoing since 1994.

FIPS 140 was updated in 2001 (FIPS 140-2),[16] the same year the Advanced Encryption Standards (AES) became a standard. The 2001 version made small changes compared to its predecessor. FISMA 2002 removed the statutory provision that allowed agencies to waive mandatory FIPS requirements. It meant FIPS 140 became mandatory. In effect, FIPS 140 became the acquisition gatekeeper to the federal government for cybersecurity.

It is hard for an essentially unchanged security standard and validation program to keep up with today's incredibly fast evolution in the domains of cryptography and cybersecurity. The mission is to improve the security and technical quality of cryptographic modules employed by federal agencies and industry by developing standards, researching developing test methods and validation criteria, and utilizing accredited independent third party testing labs. These labs produce test reports that are validated by NIST.

What is a cryptographic module? It is really a set of logical boundaries around cryptographic implementations within a computer system or hardware (a logical box that has cryptographic technology and some interfaces to perform services in it). CMVP has an international footprint and looking for the best technology around the world.

CMVP testing and validation is covered by four entities: the vendor who designs and produces, the CST Lab that tests for conformance, NIST validates the test results that are submitted, and the government user specifies products and purchases (if products are eligible for procurement).

There are four actors moving in different cybersecurity orbits: government agencies, CMVP, laboratories, and high technology industries. Industry perspectives on CMVP have revealed long review cycles that go well beyond product cycles, as well as cost and rigidity in the process. Updating validated modules is difficult. Patching is a way of life; patches continue to be necessary. Automating review

[16] http://csrc.nist.gov/groups/STM/cmvp/standards.html

workflow helps but not enough. Long validation cycles were acceptable in the '90s. The state of technology is different today; long review cycles are not feasible given today's pace of technology.

Cryptography is everywhere today. There are multiple cryptography environments. Industry is saying there is a great need for improvement in validating software. Hardware security testing has not kept up with the state of the art and low cost fault injection (hacking hardware). Fault injection is much less expensive to attempt today.

Other government programs such as the National Information Assurance Partnership (NIAP)[17] and the Common Computing Security Standards Forum (CCSS Forum)[18] are significant programs who are invested in the quality of cybersecurity in the government acquisition arena. Industry expects standards to be aligned at the broader level, so that only a single validation is required. Independent labs are often burdened with labor intensive and ineffective test methodologies. Code reviews for software today are often superficial. As a result, there are concerns with testing methods.

The same concern with ineffective test methodologies applies with in-depth hardware testing. "The English essay model" is often used to describe validation testing. Submitted validation reports often describe testing methods in the form of an essay. As one would expect, some reports are well written, others are not. Concerns exist with lab competency in challenging technical areas related to cryptography such as entropy estimation and physical security testing, with competency unevenly distributed among labs.

Randomness of cryptographic keys is critical, and estimating entropy measures the randomness or strength of keys. On normal Turing machines, these devices in effect become deterministic machines. Unpredictable behavior in these machines yields no useful result. Knowing the level of randomness is critically important. Testing for randomness can be challenging in certain instances. The results of expanding an irrational constant such as Pi will pass randomness tests; however, the sequence of digits that is generated when the value of Pi is expanded is not random. There must then be a justification of why a particular source is considered to be random.

The metamorphosis effect is defined as a living organism goes through significant change after birth (butterfly). In testing modules, it can be noted though the testing may not have produced any change, descriptions of the module may change greatly. The metamorphosis effect in labs exposes significant discrepancies particularly where the English essay model for describing testing is used. Following documentation-only certification, modules validate without a single implementation change, when in actual fact there have been changes to the modules being validated.

It creates a systemic problem casting doubts on security assurances due to lack of trust in laboratory testing. Long review cycles slow down adoption of the latest technology, as the technology must be certified prior to being acquired by government agencies. Security certificates are time consuming to produce and are generally expected to last for a few years. The reality is different, as the pace of technology is now much faster. Ongoing changes to operating system environments can also impact randomness of cryptography used to secure a particular system.

[17] https://www.niap-ccevs.org/
[18] http://www.ccssforum.org/

There is an inability to get FIPS 140-2 compliance assurance on platforms. Due to the length of the validation process, configurations do not match real platforms. Similar concerns exist with hardware. Changes to operating systems and hardware occur more quickly than software validations are issued. Awareness of what's happening in technology in general is necessary. Looking ahead, the economy of cybersecurity has been slow to emerge.

Dr. Weinberger asked what expectations can there be with respect to any cryptographic module? There are two parts to the answer. There are the security requirements that the standard defines. If the module has been certified, how do we know it's ok? The verification of the requirements of the standard can be examined. CMVS is working to improve confidence in whether the security requirements have been implemented properly. The question is whether or not the standard provides in practice what one would expect it to provide. Implementing against a standard ought to provide some assurance as opposed to merely checking a box.

Cybersecurity did not arrive in its present state by accident. Companies push technologies out sooner, expecting to patch later. The time cycle has shortened so much that vulnerabilities are discovered following distribution. Regulation seems to be the easy answer, but it stifles innovation. NIST would like to find solutions to problems based on common interests, rather than relying on heavy regulation. Common interests can be developed, but they take time. Car safety was once considered too expensive originally by manufacturers, until Volvo made car safety a competitive advantage. Volvo's name today is still synonymous with safety.

Putting it all together, the NIST proposed plan to adopt ISO/IEC 19790:2012[19] Information technology – Security techniques – Security requirements for cryptographic modules as FIPS 140-3 in a Federal Register notice[20] in August 2015. The comment period closed in September, 2015, and the comments received are currently being analyzed. It is an opportunity to re-organize the CMVP in a better way. NIST intends to continue to specify the cryptographic modules, modes, and key management schemas that are acceptable for use by the US government.

The main idea is to move away from the current schema of industry, laboratories and NIST, in favor of relying on industry experience for everyone to reach a better state. Instead of outsourcing testing to third party labs who may be limited in their ability to provide qualified staff to do the testing. Consideration is being given to leverage what technology companies do today to pass their products, instead of expecting laboratories to do all the testing of a module.

It may be better to utilize mature industrial security development processes like ISO/IEC 27034[21] Information technology – Security techniques – Application security, making use of a security development lifecycle. It covers design, development, and maintenance of security products. There is consideration of moving to security techniques such as application security and reuse of test evidence in

[19] http://www.iso.org/iso/catalogue_detail.htm?csnumber=52906

[20] Federal Register Notice issued on 08/15/2015, Government use of standards for security and conformance requirements for cryptographic algorithm and Cryptographic Module Testing and Validation Programs https://www.federalregister.gov/articles/2015/08/12/2015-19743/government-use-of-standards-for-security-and-conformance-requirements-for-cryptographic-algorithm

[21] ISO/IEC 27034 Part-1 Overview and concepts, Part-2 Organization normative framework http://www.iso.org/iso/home/search.htm?qt=27034&sort=rel&type=simple&published=on

government validations; requiring labs to verify evidence, and not independently recreate it one hundred percent; and refocusing labs on testing beyond what is already tested by vendors.

The Board asked what is being done to make sure that the labs are testing properly. Is it a NIST issue for teaching the labs to test properly? A number of measures have been implemented. Lab competency requirements have become more advanced. There is concern that the measures will not function beyond the current envelope. They are utilizing a "carrot and stick approach" to lab process improvement. Incentives exist for labs to do the best possible job. CMVP holds an annual managers meeting and quarterly calls with the labs. They also meet with NIAP monthly.

There is consideration of introducing a three tier model for testing labs. The main idea is to get away from the English essay validation model, move to complete automation for FIPS-140 testing and produce a verifiable artifact to document validation. The proposed model reduces the validation cycle, and enables just-in-time validations, with the upshot being it reduces cost and provides powerful economic incentives for the industry.

The three tier approach allows for meaningful risk management and adopting technologies. The three tier model is mainly relevant for companies with mature development cycles, but are not able or willing to automate for some reason. Tier 3 (highest) will be reserved for U.S. government and national security systems. Tier 1 and 2 will be used for other markets where FIPS 140-2 guidelines are voluntarily used today.

Instead of solving a hard testing problem (such as estimating entropy), can a simpler problem be solved in its place? If entropy cannot be estimated from various sources, what if known sources could be used? In this way, we can assist the industry to meet most difficult security requirements through technology innovation. There is consideration to introduce "EaaS" (Entropy as a Service) to be used as a web site that utilizes known good sources, eliminates complex estimation, in one research area.

Another difficult issue with some existing cryptographic algorithms is they are inherently asymmetric in the way they calculate when dealing with hardware. The device behaves differently when the value of the key bit is zero or non-zero, and that causes electro-magnetic emanations that make the key detectable and gives attackers the capability to break the key. Industry is attempting to obfuscate the effect of these calculations with other calculations to try to make the key value less detectible.

An alternative is to create inherently symmetric algorithms, which would eliminate this sort of problem. It is difficult to determine how much assurance exists. Research to develop inherently symmetric algorithms is being done with several universities including the University of Maryland, KU Leaven, Belgium and the University of Florida. The overall approach is to be smart about the hard problems, and automate the easy ones.

The group is looking to establish bilateral relationships to encourage adoption of the ISO standard with other validation programs in Europe and Asia. If the US is successful in optimizing its module validation problem, it will make it easier for other parts of the world to use our module validation results. This will allow companies to choose the validation authorities they want to target, not like the mutual recognition in common criteria, and retain the independence of the US program.

In December 2015, an industry working group was started with government and industry participants, including 36 members, representing 17 companies and open source entities, and 2 government agencies organized in several working areas, and they are working well together. The group is moving the process toward desired goals, proof of concept development and demonstration.

A joint effort exists between NIST and CISCO. There is a demo at ICMC in May 2016. NIST/CISCO are working together to develop a web service to demonstrate the automated cryptographic validation system. This will show that systems can be tested and validated through automation to have the certificate created. Currently, there is no way of testing the module in the cloud. There needs to be a way to make the testing platform independent, but at the same time show test and provide assurances in the cloud. Microsoft, Amazon web-services and others are working as part of this effort on how to get this tested and assured in a cloud environment.

Federal Cybersecurity Research and Development Plan

Tim Polk, Assistant Director, Cybersecurity, National Security & International Affairs Division, Office of Science and Technology Policy (OSTP)

Dr. Greg Shannon, Assistant Director, Cybersecurity Strategy, National Security & International Affairs Division, OSTP

The Chair welcomed Tim Polk and Dr. Greg Shannon to the meeting to speak about the Federal Cybersecurity R&D Strategic Plan. In February 2016, in conjunction with the budget roll out, the Cybersecurity National Action Plan (CNAP) [22] was announced. There are between 50 and 75 parts to the plan. Most are meant to be effective in the near term. The Cybersecurity R&D Strategic Plan contains portions that will be implemented over the longer term. The Commission on Enhancing National Cybersecurity is also a longer term piece of the national action plan.

Key elements of the CNAP include establishing a commission on enhancing national cybersecurity; creating a Federal CISO position to lead on cybersecurity oversight policies and strategy; establishing an IT technology modernization fund; and working with industry to encourage broader use of security tools like multi-factor authentication.

The 3.1 billion dollar figure for the technology modernization fund is not intended to cover everything that needs to be done. The fund is intended to handle the highest priority items. The High Value Assets project has also been created to identify high value assets currently at risk. It represents progress, but is not a complete solution.

The Federal Cybersecurity Research and Development Strategic Plan[23] was requested by Congress in December 2014 and written in 2015 by a working group of the National Science and Technology Council (NSTC). An inter-agency group was formed to work with classified and unclassified aspects. The plan is

[22] https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan; https://www.whitehouse.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know; https://www.whitehouse.gov/the-press-office/2016/02/17/remarks-president-cybersecurity-national-action-plan

[23] https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf

an unclassified document. They worked with MITRE and others during the formulation of the plan. It was held until February 2016 as Congress was not in session in December 2015.

There was an earlier plan in 2011 that was created directly based on stated agency desires. The approach to developing the February 2016 plan was different. Congress had its own agenda for the plan that was adhered to. The OSTP thought very carefully about who the different players were, and what expectations were for them.

Mr. Polk noted users were once considered the "enemy" in the eyes of code producers because users never seemed to do what they were "supposed" to do. Users tend to make decisions that are rational for them. Cybersecurity must work for the users using the systems in order for it to be effective. The latest report takes the view that if end users would not use the tools provided, maybe the tools are not good technology.

The plan was requested by Congress and went through multiple inter-agency reviews. The fundamental challenge is to make cybersecurity less onerous for users while providing more effective defenses against threats. Feedback on efficacy is critical, especially in understanding impacts. Efficiency in actions relating to policy is also important. Efficiency considerations are crucial in getting the framework more widely deployed.

Congress asked for near and long term goals to be defined, goals have been effective in working with agencies. They set expectations for policy makers as well, in terms of what could realistically be accomplished. At a high level, near term goals include improving risk management; mid-term goals include eliminating software vulnerabilities by at least one or two orders of magnitude; in the long term, reaching a state of defensive deterrence created in part by prohibitive costs in resources for the effort expended in an attack and greatly increased rates of successful attribution. Science and technology will at some point be able to provide these capabilities.

The plan calls for four defensive elements aligned with the NIST framework; made to be comprehensive by a larger audience:

- **Deter** – Involves being able to measure how difficult it is to breach a system; what science and technology (S&T) will do a better job than red teams, as they are the standard but not without fault;
- **Protect** - Efficacy and efficiency in being able to demonstrate particular approaches will resist malicious cyber activities and ensure confidence and integrity;
- **Detection** – Research and development going on in this area. A light weight solution is the most desirable.
- **Adapt** – Solutions here are not about identifying, responding or recovering, but are about learning how to evolve infrastructure so that adversaries are not able to attack the systems in the same manner in the future.

If these defense mechanisms are pieced together, there is the beginning of what a solution may look like within the system. Challenges and objectives include deterring breaches and measuring how difficult it is to breach a system, making breaches more attributable. Measurements now are compliance or

behavior-based; however, there must be more to protection. Detection must be light weight. The requirement for the R&D plan is to update Congress in four years on each objective and measure progress. The expectation is the objectives will be a living list that will grow and change over time. MITRE is now reviewing the document to determine what, if anything, was missed.

Success depends on these critical areas: Scientific foundations, enhancements in risk management, human aspects, transitioning successful research into widespread use, as well as workforce development, enhancing the infrastructure for research. Discussion of long term investments includes the President's commission on enhancing cybersecurity.

Defensive elements are relevant in all cybersecurity contexts. The plan considers these emerging technologies and highlights: detailing specific R&D priorities for each area, prioritizing basic and long-term research in federal cybersecurity R&D, lowering barriers and strengthening incentives for public and private organizations, expanding diversity in the research community and in the cybersecurity workplace.

What does success look like? Being able to design secure systems, making cybersecurity easier for users, and deterring adversaries.

Updates on Federal Risk and Authorization Management Program (FedRAMP) [24] [25] [26]

Matthew Goodrich, FedRAMP Director, General Services Administration (GSA)

The Chair welcomed Matthew Goodrich from GSA to the meeting to provide updates on FedRAMP. Over the last six months, there has been a dramatic increase in Authority to Operate (ATO) and providers in FedRAMP. In December, GSA launched an online training program, including some cyber security-related topics. During the last six months, GSA has been looking at feedback for the program. There has been positive feedback about the program. Feedback involved desires for greater certainty of success, more transparency in the process, faster speed to authorization, predictability in timeframes for authorizations.

Redesign of the process involved faster time to authorization, with the same or less risk, and equal or better quality of the security authorization package, provide confidence that we are working with capable and impactful Cloud Service Providers (CSPs). There is a process to make sure vendors are ready to start the authorization process. The focus has been on capabilities up front based on a new capability assessment. They have redefined roles of Joint Application Board (JAB) teams and FedRAMP Program Management Office (PMO) roles, increased reliance on third party assessors (3PAO), and created clearer rules of engagement for testing, evidence, and documentation. The new process is being tested this month.

The website[27] has made it easier to search and compare vendors who are authorized, detail where vendors are in process, highlighting agency participation with FedRAMP. The draft baseline with

[24] https://fcw.com/articles/2016/02/12/cdm-fedramp-oped.aspx?s=fcwdaily_160216

[25] http://fcw.com/articles/2016/02/24/fedramp-overhaul-noble.aspx?s=fcwdaily_250216

[26] http://fcw.com/articles/2016/02/24/fedramp-overhaul-noble.aspx?s=fcwdaily_250216

[27] https://www.fedramp.gov/#

vendors, plans to authorize multiple providers with the JAB along with release of the baseline, and final stages of authorization efforts are planned to be released in spring 2016.

Public comments on high impact systems were received last year. Two rounds of public comments were received. The second round received minimal substantive feedback. The agency is now finalizing feedback and working to align with US Department of Defense (DOD) impact levels. The agency is now piloting the draft baseline with vendors, a plan to authorize multiple CSPs with the JAB with release of the baseline, and final stages of authorization efforts. All are planned to be released in spring 2016.

Updates on Information Sharing, CyberSecurity, and Continuous Diagnostics and Mitigation (CDM) [28]

Andy Ozment, Ph.D., Assistant Secretary for Cybersecurity & Communications, US Department of Homeland Security (DHS)

The Chair welcomed Dr. Andy Ozment from the DHS to the meeting to update the Board on information sharing (legislation passed in 2015), cybersecurity, and continuous diagnostics and mitigation at DHS. Information sharing at DHS is thought of in terms of three methods: in person, PDFs, and machine-to-machine. PDFs are how most forms of information are made real to people, including reviewable documents that someone opens to make sense of the information, but it is not the way to relay 20,000 malicious indicators. In 2012, DHS decided to automate the sharing of indicators and start to develop some standards. DHS has been shepherding those standards for a few years in collaboration with emerging partners and shipped them off to One Acquisition Solution for Integrated Services (OASIS) this past spring.

In 2014, DHS started a pilot program with the financial sector, which was very successful. The financial sector liked it enough that they took the server on their end of the pilot that communicated with DHS to share threat indicators to create a new product. The Cyber Security Act of 2015[29] legislation was passed that provides liability protection for companies to share information from company to company or a company sharing information with the government. The legislation changed the technical requirements for the system. New requirements were required for the system as well as updates to the system for interagency processing were required within 30 days. The system is now in place to share threat indicators.

The Board noted that this is about the privacy implications of sharing of information. Some have suggested that the website made it hard to put in the wrong kind of information. Is there any truth to that sort of observation? The goal was to have a privacy scrub on the site. Functionally it was divided up into three categories. As requested by Congress, we now share more than just indicators; information on defensive actions and other open ended types of information are also being shared. When an indicator is shared, it is versioned and pushed out. If a field can be reviewed, it will be reviewed, if the field needs human review, the review takes place and the field is updated and it is pushed out once the review takes place.

[28] https://www.dhs.gov/cdm
[29] https://www.congress.gov/bill/114th-congress/senate-bill/754

There are multiple ways in which we can think about sharing indicators; we can share the hundred indicators each day that we feel are the most important, or we can share the million indicators each day which everyone has seen. We have received feedback from the companies we talked to and we want it to be shared scale, shared rapidly, and provide the most immediate threat. In order to share these indicators in a timely fashion, we are not vetting each indicator. Some automated validation will take place, such as verifying a commonly used domain be added to the system, we will not push out that indicator.

The feedback indicated that companies will vet the information anyway, so there is no reason to withhold it by vetting it prior to pushing it out. All indicators vetted one time only to save time. Indicators are scored by the reputation of domain. Government will provide indicators as some private sector companies are sharing indicators now. It is hoped more will share in the future.

The Board asked if there is a field that publicizes the category on the indicator as to whether it is software based or something so as companies can know if they are affected? For instance, there could be a vulnerability within a piece of software, or it could involve a particular asset, such as a router. Depending on what it is, it might be more relevant to different parties.

If the indicator is taking advantage of a specific vulnerability, we will tie it to the common vulnerabilities and exposures (CVE)[30] and it will assess the relevancy for the user. If not, there are not different fields to determine a category for the indicator. This will be an evolving process:

- Phase 1, get the infrastructure available to be able to share the information and get users signed up.
- Phase 2, get information within the system by starting with government indicators and getting some private sector partners willing to put in indicators.

There is a degree to which this will be open for business now to the private sector, while awaiting companies to share and receive indicators at https://www.us-cert.gov/ais.

DHS had been given an operational role on government networks, according to NIST guidance, policy and procedure standard roles. At the beginning, there was no buy-in from other government agencies as they did not want anyone else in their business. We had a problem of trying to measure the security of agencies and provide a baseline of security, which applies to all agencies, with no cooperation from the agencies.

The team took the approach of starting from the perimeter, as it is easier to get access from the perimeter and a good way for validation. They started the Einstein[31] program, 1, 2, and 3 which started at the perimeter and worked those for a number of years. With some push within DHS, the program was expanded to improve the agency's ability to manage and secure the interior of their organizations. The approach was to purchase the tools for the agencies to deploy and run in their environment and provide the data. Instead of asking agencies how secure they are, and having them provide spreadsheets, we now have machines assessing things and providing more detailed and useful data.

[30] https://www.us-cert.gov/ncas/bulletins/SB15-026
[31] https://www.dhs.gov/einstein

The Einstein program was started and worked for a number of years. Work started for agencies to secure their network. Phase 1 focused on basic IT management and hygiene. It started with a measure things approach. Phase 2 was interrupted by the Office of Personnel Management (OPM) intrusion. It focuses on identity management, authorization, and access control. It is not yet complete. Phase 3 involves determining what is happening on networks, event management, etc. Phase 4 will focus on data security.

Phase 1 of the CDM program was to focus on basic IT management and hygiene; hardware and software asset management, configuration management, and vulnerability scanning. This started with a measurement approach instead of a change things approach.

The Board asked how much of this has been completed. The purchasing part of it was completed in the fall of 2015. The agencies were divided into buckets, an integrator leads that bucket and is helping the different agencies deploy the tools. No agency has finished the installation/deployments at this time. We are unsure of how long the installation process will take; the best guess is in the fall of 2016 or early winter. Depending on the resources and dedication from each agency will determine how fast these installations can be completed.

Phase 2 of the CDM program is designed to find out who is on the network. It focuses on identity management and authorization control and access. We want to know how users are logging in, what are their authorizations, and are those authorizations needed to do the job. We are still in the buying portion of phase 2; we will finish that in fiscal year 2016.

Phase 3 of the CDM program is looking into what's taking place on the network. We are still in the requirements specification phase of phase 3. Phase 3 is currently scheduled to be completed during fiscal year 2017.

Phase 4 of the CDM program is still in the definition phase, but is most likely to be looking into the data security within networks. Phase 4 is currently scheduled to be kicked off later in fiscal year 2018.

There are some things that the CDM program provides, including a new way of buying tools for the civilian government. Instead of each agency purchasing different tools at varying prices, the tools are purchased in bulk. The same tools are not being purchased for each agency, but different buckets provide the ability to choose different tools. This ensures they all speak the same language and report in a standardized fashion. CDM provides the ability to drive changes within the agencies. All these tools will be tied to dashboards, which will be shared with agency peers and highlight what actions need to be taken to most decrease the risk to individual organizations. Agencies are realizing that they cannot do it on their own, but need to work together.

The Chair asked, "If I am a bad guy, then I don't have to worry until fiscal year 2019 or fiscal year 2020 as the rollout is so slow?" Mr. Ozment noted that remark can be made about any government area that is lagging and needs to improve. We are not where we want to be, but we are held back by agencies not getting to where they need to be and by acquisitions. Nothing can be done due to procurement, but this is where we are now.

There are agencies that are still reluctant, but legislation and the OPM breach has done more to assist with increasing motivation to change and we have received more cooperation than ever before, but it is

still not 100%. The biggest risk seen government-wide is agencies being able to absorb and take advantage of these tools.

The Board noted that it is easy to state what the program wants to do, but it is hard, given the past, to see that the program is actually going to complete its objectives. Is there any worry about that? Is there something built in to make sure that after everything is installed and running, everything will actually work properly? Mr. Ozment noted it is his biggest worry as well. In terms of working properly at a mechanical level, as far as dashboards providing the information, things should work. At a strategic level, the major concern is the agencies being able to assimilate and take advantage of these tools, and feels that is the biggest risk.

Phase 1 will provide a much broader understanding of what is available on agency networks, as currently there is no visibility, and most of the data is self-reported data which may or may not be computationally achieved. It is hard to hold someone accountable when the data is questionable. Alternatively, getting more reliable data will not totally resolve the issue but provide assurance that we are progressing in the right direction.

The Board noted one way of putting pressure on people is to provide transparency to the dashboards and make them public. A lot has been done to make results more public as anyone can go to performance.gov to see agency scores. However, it does not apply as much pressure as expected. Dr. Ozment pushed hard to make a lot of data public, but that did not particularly lead to more pressure. At the same time, it does not mean it is the wrong approach although he was surprised at the result.

The Board asked is there any chance the information sharing will be part of the CDM program. Initially at DHS the CDM and Einstein programs were not as integrated as we thought they should be and the indicator sharing program did not exist at that time. One of the things Mr. Ozment did was put CDM and Einstein in the same organization for increased collaboration. They are not where they need to be as yet, but are moving in that direction.

DHS is currently looking to expanding its support capacity; looking to expand the red teams from the current one or two teams to 24 teams. We are looking to increase the current number of incident response teams from about six to ten to twenty-four teams. DHS is also looking into making them hunt teams as well as incident response teams to proactively look for vulnerabilities within agencies. Changing the capacity of the teams, will enable DHS to assist with a lot more agencies. We are building a design and engineering team to help assess and build tools and systems within other agencies.

Circular No. A-130 Revised [32] [33] (presentation provided)

Carol Bales, Senior Policy Analyst, Office of Management and Budget (OMB)

The Chair welcomed Carol Bales from the Office of Management and Budget to the meeting to update the Board on the A-130 Revised Circular. The A-130 circular has been under revision for almost 15 years, but it is nearing the end of the process. The Circular provides the underlying policy framework for federal information resource management. The revised Circular centralizes a wide-range of policy

[32] https://www.whitehouse.gov/omb/circulars_a130_a130pre

[33] https://www.whitehouse.gov/omb/circulars_a130_a130trans4/

updates on topics such as acquisitions, information governance, investment planning and control, workforce planning, records management, open data, privacy and security.

There were significant revisions as well as bringing it up to date with more recent policies and practices within the government. The Circular has been distributed for three rounds of interagency review as well as a 45-day period for public comments. Over 1,200 public comments were received in October, 2015 and all comments received have been adjudicated. Comments were received from several organizations, federal agencies, and individuals during the public commenting timeframe.

A lot of reorganizing took place leading revision of the outline and re-organization of the appendices. The appendix on electronic signatures was removed. The key requirements for Electric Signature was removed from the appendix and added to the main body of the Circular.

A variety of policy requirements in the main body were updated (slide #4):

- The circular requires the implementation of incremental and agile development, proactively enable accessibility to the public.
- It requires agencies to ensure the ability to access and receive records throughout the document lifecycle.
- It requires the Chief Information Officer and Senior Agency Official for Privacy to develop a set of competency requirements for IT leadership permissions
- It requires agencies to develop process for electronic signatures
- It requires agencies to leverage the evolving internet and elaborate the use of IPV6, and it also establish concepts to security, privacy, and personally identifiable information (PII).

There were also significant changes to Appendix 1 (see slide #5), which establishes new requirements for information security and privacy management and also incorporates and mandates from within FISMA. It provides the responsibility for protection and management of federal agent resources including minimal requirements for federal information security. It places ultimate and full responsibility with the head of agencies for ensuring that the information management practices are adequately addressed.

Appendix 2 focuses on the management of PII. Previous versions of Appendix 2 (see slide #6) revolved around the requirements of the Privacy Act of 1974. Those requirements have been removed, revised and instituted into OMB Circular-108 that was rescinded by this circular. The appendix establishes the requirements of senior official to establish policy for the handling of PII within the agencies. The definition of PII has not changed. The definition of "breach" has been removed. Agencies are being asked to reduce the use of social security numbers to the minimum possible.

The next steps include releasing the Circular for a final inter-agency review and adjudicating comments received. The current text is approximately 80 pages with the security appendix being just as long if not longer than the main body of the document.

American Council for Technology & Industry Advisory Council (ACT-IAC) report – Cybersecurity Ideation Initiation Report (presentation provided)

DHS Data Privacy and Integrity Advisory Committee – Cybersecurity [34] (presentation provided)
Dan Chenok, Executive Director of the IBM Center for the Business of Government
Michael Howell, Ph.D., Senior Director, Institute for Innovation and Special Projects, ACT-IAC

The Chair welcomed Dan Chenok from IBM and Michael Howell from the ACT-IAC to the meeting to provide an update on the American Council for Technology and Industry Advisory Council. The ACT-IAC is a joint task force between the government and the industry IAC. The American Council for Technology (ACT) is chaired by a government board of directors and the Industry Advisory Council (IAC) is chaired by an industry board of directors. ACT-IAC was put together to help government use technology in its mission performance in a number of different areas. It works through a series of professional development programs and a series of topic focused communities of interest that produce content worthy of cyber security. This group does not make any legislative recommendations.

The Cyber Innovation Ideation Initiative was produced to help improve federal government cybersecurity through innovative approaches. The ideation platform has gone public and allows for anyone to participate, whether from government, industry, or as individuals. There were eight challenges introduced with the ideation platform. Approximately 127 submissions were received with one too many details and ideas. Five to ten teams were created to assist with the compilation and vet through the submissions. There were some crosscutting themes in the submissions provided; much of what is required is known, but not implemented. Enhancements need to be made to training, and there needs to be a better way to perform information sharing.

The first challenge was trying to address the state of cyber security fundamentals. To do this we need to embrace cyber tips of the day, adopt a cyber investment management board, and we recommend an SEC-type self-assessment checklist, so that agencies can be their own inspector general in advance. Going through a personal internal assessment can help with being prepared for an actual inspector general audit.

Another challenge is limiting the vulnerabilities set by business users in their own networks. Some promising ideas for tackling this includes building a security maven approach similar to that of Wal-Mart. Embed cyber development into cyber teams and act as a support task force for the application development teams. Activities such as building security in the front-end of the application development processes, creating a cyber DevOps environment and a DMZ for developers as they are working. Adopting a risk based approach using quantifiable risk measures in Tech-Stat and similar sessions will also give benefits. Properly vetting for security risks within the internal environment, and not just talking about DevOps, but actually using security DevOps and making it integral to the development life cycle.

There is also the challenge of getting faster responses to data breaches on the network. It starts by looking for anomalies in the data patterns on the network. Creating a "hotline" reporting channel allows users to report incidents. DHS is to setup an industry and government reporting hotline that can be made available to users across different agencies. Feedback is essential for the hotline because if no feedback is received, the users will no longer use the hotline service. We also need to get to a better

[34] https://www.dhs.gov/sites/default/files/publications/dpiac-report-2016-01-algorithmic-analytics_0.pdf

centralized location for anyone to inform and receive information about risks. Along with the hotline, we need a way to triage and properly filter out non-issues. There is a need to broaden the incident/response awareness, training, and action planning to build cyber into a FEMA-like process within the agencies.

Adopting a threat-aware proactive defense through analytics is another challenge, but does present some encouraging ideas to address this issue. Creating blue team audits, followed by red team operations to get a team to work with agencies in advance to be prepared for threats and link them in with red team reviews. Having a Distributed Corroboration of Services (DCOS) to respond to threats by automated means and enable automated responses across agencies.

Pursuing an insider threat strategy will motivate creation of an insider threat action plan. It helps detect malicious cyber insiders that are not detectable by other means, finds cases of compromised credentials by spotting suspicious changes in employee behavior, and tracks risky behavior that puts the organization at risk. The use of security tools will also deliver other benefits to the business.

An additional challenge we face is sharing threat intelligence. Some ideas on sharing threat intelligence include endorsing and expanding the STIX/TAXII to make data breach reporting more robust and shared more widely. This will also embrace operations similar to that used by the North American network operators group. Secondly, establishing an environment that facilitates threat data information sharing will foster continued sharing.

We also must address the challenge with the talent search within the workforce which is considered to be the highest priority to get results in all areas. The creation of a Cyber Corps that will create an elite cyber security reserve corps of individuals that has passed all necessary competency screenings. We need to augment the CISO with tools to be able to recruit better talent more aggressively. Talent searches need to start locating talent in different areas within organizations. The entire workforce can be used instead of just the cyber security staff. Providing an environment of skills-based and performance-based training on how and where cyber supports the mission. Functional assessments and exercise events can occur that will benefit cyber talent within organizations.

Another challenge that needs addressing is executive leadership-led risk management by adopting a private sector board of director's oversight model. Creating a cyber responsibility assignment matrix (RACI) will provide more accountability and disciplined responses to executives, and a structured approach for agencies to report issues. Federal Information Technology Acquisition Reform Act (FITARA) governance can give CIOs more specific reach over agencies security to have cyber risks built into program and budgeting evaluations.

Lastly, another challenge area to be addressed is building effective security into acquisitions. Agencies must determine the viability of requiring federal contractors to have cyber insurance. Increase the pace of placing R&D activities in cyber being done in government and quasi-government labs into acquisition faster. Certifications similar to FedRAMP can be used to standardize baseline assessment for all acquisitions, not just those that are cloud-based. Develop and propagate model cyber contract requirements language. If the requirements are more consistent and complete, they can be followed and completed more easily.

The next steps we are to take will be to develop action plans about cyber workforce and integrating cyber into acquisitions. We will also be addressing risk management and incident response following the new OMB Guidance.

DHS Data Privacy and Integrity Advisory Committee – Cybersecurity

DHS NPPD has a pilot program underway to develop techniques and assess effectiveness of algorithmic analytics. The privacy office and NPPD worked together on potential privacy issues raised by these pilot programs. Work was done in three areas; general considerations, addressing key considerations affecting the program, and identifying potential privacy programs. The subcommittee changed the term "behavior analytics" to "algorithmic analytics" to avoid confusion about whether people's behavior is being analyzed. This change was made based on the feedback received from an actual pilot being run at DHS.

Algorithmic analytics is done by looking at patterns of traffic using machine algorithms to detect anomalies. It's not signature based assessment but can work as a portfolio with signature based traffic and an analyst is used to reviewing the anomalies. Commercial companies use Algorithmic Analytics today in front end authentication, transaction monitoring between data on the network, transaction monitoring real time queries, risk scoring matrices, and egress tracking; although the government does not have a good understanding of the egress data.

DHS has another pilot program, Logical Response Aperture (LRA), which is concerned with the data in transit between systems across the network. This pilot program is not concerned with data when at rest nor is it concerned with data once it is in the system. These analytics can be used to spot patterns once the data is in the system. The program looks at patterns of traffic, users, time periods, and all types of data coming in and going out of the system.

Mobile devices were not addressed, but the DHS may want to expand into this area as it presents special issues. No recommendations have been made, but we have suggested DHS go back and look to see if special issues and consideration should be made for PII on mobile devices. The risk of PII getting into the hands of analysts was minimal during the LRA program. Accountability is key within this program, therefore, human oversight is vital and allows for ongoing reviews and redress. Within this program there is potential privacy protection at each stage.

During the collection stage, the data, where feasible, should be encrypted and de-identified. Data collection should take place when data is in transit and at rest, provide notice to the public as to what's happening, and there should be transparency for what is collected. In the usage stage, we are clarifying the use cases for the program. It defines multiple uses; establishes processes for each use and limitations, and protocols for follow up analysis.

The sharing stage determines how the information is shared across the government and its partner entities. Rules must be defined for sharing within the government and outside agencies such as law enforcement, private sector, ISACs/ISAOs, etc. The access stage limits the personnel who can access data within the program. This should not be a public database. It develops the rules for when users access the data and how they gain the access to the data. It has volume limits on how much can be downloaded from the algorithmic analytics database and control logs are created for access.

The retention and disposal phase determines how long to retain data and the proper way to phase the data out. The timelines should be transparent so all are aware and get reviewed over the course of the program. The analytics must be separate from the analysis and they should have different retention periods. There is a need for security through the lifecycle and the process itself should be auditable.

Final Words from the Chair, Dr. Peter Weinberger

Peter Weinberger, Ph.D., Chair and member, ISPAB, and Computer Scientist, Google

Dr. Weinberger noted there is a tradition that outgoing members get an hour to speak on any topic they wish within reason. There are a few topics for the ISPAB to consider going forward. The first topic is cyber security. There are a few points to touch on including the Estonian e-government experience to see what can be gained from such examination. There may be lessons worth learning from what they have done.

On the topic of passwords and two-factor authentication, everyone agrees there are multiple problems with passwords. The workflow involved with separate passwords involves changing them from time to time. There are two stories with passwords; the single sign on story, and the other way of logging into each service every time. The HSPD12 and second factor authentication have gone down an unfortunate path in that the second factor does not involve the identity of the individual but relates to the server. In fact, the same security potentially could be used for multiple websites. Also, second factors are not convenient to use. Two factor identification must be managed. However, it is not user friendly. The whole process is not quite right yet. It would make more sense to have one password for all sites, and a different authentication for each.

Patches are almost completely satisfactory. Generally, patches occur automatically, without participation from the user.

The theory with anti-virus programs is that systems should be more secure after installation than before installation. Often the programs themselves are quite unsafe. ISPAB should look into the properties of things widely used by the government. The question asked by ISPAB should be, do these things add to the security of the government? In effect, it is almost the opposite of a certification process. Anti-virus programs should stand up to a reasonable attack. Is anti-virus a failure because there are so many zero days? Patching should be the first round of defense. Most attacks can be foiled by existing patches. Anti-virus is not useful if the computer is not patched.

Updates seem to be difficult to work with. It appears to be hard because people with knowledge of these things think it is very hard. There is a worry that the whole structure of cryptography is based on ignorance. It may be, or it may not. As stated from Psalm 146, "Put not your faith in the works of princes…"

In Dr. Weinberger's view, in the future there will be two possibilities: cryptography may well turn out to be like cigarettes. At first it is good, but then we will discover it would not work and we will have to use something else. Or we will use DES, which has had no attacks except brute force. In fact, we do not know whether these things are truly strong. Mr. Scholl noted we are one smart guy away from discovering the entire e-commerce infrastructure is a house of sand.

Mr. Scholl presented Dr. Weinberger with a picture of ISPAB from different years.

Meeting Recessed

The meeting recessed at 4:45 P.M., Thursday, March 24, 2016.

Friday, March 25, 2016

The Chair called the meeting to order at 8:30 A.M.

Dr. Weinberger opened the session by presenting a token of the Board's appreciation to Ms. Annie Sokol for her service as the Designated Federal Officer and the many other tasks she performed that contributed to many successful meetings. Mr. Scholl expressed his personal thanks and appreciation for the work and professionalism that Ms. Sokol has offered to the ISPAB effort.

NIST Updates

- ***Cryptography (Quantum)*** [35]
- ***Code Signing***
- ***EO Cybersecurity Framework***

Matt Scholl, Chief, Computer Security Division, ITL, NIST
Donna Dodson, Associate Director and Chief Cybersecurity Advisor, NIST
Kevin Stine, Chief, Applied Cybersecurity Division, ITL, NIST

The Chair welcomed Matt Scholl, Kevin Stine, and Donna Dodson, all from NIST to the meeting.
Ms. Dodson began with an update on activities at NIST. The NIST cyber security program has grown a lot in the last six years, and the technical capabilities have increased. Research related to standards and best practices has taken off, and NIST has been asked to take on additional effort by working with federal agencies across the nation.

The decision was made a year ago to start a new division, and last fall the search was ongoing for a new division chief. Mr. Kevin Stine has been appointed to be the Division Chief of the new Applied Cybersecurity Division. Ms. Dodson, Mr. Stine, and Mr. Scholl will be focusing on bringing NIST expertise to bear on cybersecurity, and maximizing resources available across NIST and building upon the work being developed. The engineering laboratory does a lot of work in cyber-physical systems, work that relates not just to ITL and CSD, but also across other labs at NIST.

Mr. Scholl noted he and Mr. Stine have worked for a long time together, and consequently are not worried about information getting out of sync. Mr. Scholl is not too worried about coordination and sharing in the short term since many shared resources are already working well, but wants to make sure that management controls and communication are sound so that ten years from now CSD and ACD continue to operate effectively.

[35] http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/0906_001.pdf; http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/0458_001.pdf; https://www.bbvaopenmind.com/en/quantum-computing/?utm_source=facebook&utm_medium=techreview&utm_campaign=MITcompany&utm_content=QuantumComputing

Within the CSD, progress is being made on a number of publications. In particular, Draft SP800-90b Deterministic Random Bit Generator[36] has been finalized and released for comments. Two other recently released documents[37] on cryptographic development processes policies; which address how NIST looks at, collaborates, and designs cryptographic algorithms, modes, and key management. NIST has received very good feedback and is planning on final publication in the next two weeks. Other agencies including NSA have been supportive of the document. NIST IR 8105, Report on Post-Quantum Cryptography will be published as final soon. NIST had received comments on that draft document, and had discussions with industry, internationally, and internally to complete the document.

CSD is investigating new strategic areas, including the National Strategic Computing Initiative (NSCI) in which NIST is working jointly with NSA, OSTP (Office of Science and Technology Policy), and the NSF working on public and private partnerships, and next generation computer models. CSD's role is to look at two things: (1) securing high performance computers, and, (2) using high performance computers for security. A two-day workshop, Random Bit Generation Workshop 2016,[38] is scheduled in May 2-3, 2016, to bring in experts in this field to determine how to scope the work and begin the requirements for high performance computer security. Work will include identifying common definitions, common languages and establishing initial use cases.

The Board asked if there is any idea how this new model will look. Mr. Scholl responded they are unsure at this point, but they feel confident there will hybrid models utilizing public clouds, and internal grids, and they are looking for ways to make use of these highly connected and highly powered services. It will be important to consider and evaluate the security requirements as NIST is encouraging partnerships with industry, and NIST's current work becomes an opportunity to make an early start in this endeavor.

The Board asked what's new in this respect. With respect to toolchains, CSD is looking for mechanisms that are better to employ with software tools, especially as they are used in the software development lifecycle. The hope then is to work with software tool vendors to improve their products. Other areas where software assurance can be improved includes identifying efficacy of formal methods, automation of formal methods, statistical analysis, combinatorial testing, and different test methods.

The value of NIST is to publish PDFs – the 800 series for example, but to also develop reference materials. NIST collaborates with NASA, Air Force, LMIT, other commercial vendors, to get feedback on tools. So NIST's role is primarily research, publishing reference materials from that research. The end product of all of this will be a series of publications as PDFs, and other reference materials, in other words, "A library of things".

Ms. Dodson made a request for help to the Board, to identify cryptographers and individuals that can support the effort. NIST has been asked to increase the funding within cryptography and will be hiring cryptographers and mathematicians; looking to hire the best and the brightest. NIST will be engaging

[36] http://nist.gov/itl/csd/nist-requests-comments-on-computer-security-publication-on-randomness.cfm
[37] See Annex B – Draft SP 800-175A DRAFT Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies; Draft SP 800-175B DRAFT Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
[38] http://www.nist.gov/itl/csd/ct/rbg_workshop2016.cfm

schools and will be talking about current research. NIST is also reaching out to schools that have strong background in the field of cryptology. Engagement mechanisms are not just direct hires, there will be opportunities for summer research fellowships, guest researchers, and foreign guest researchers. The Board asked if it posted on www.CRA.org. The Board has not done so in the past, but intends to do so going forward.

The ACD's mission involves working with organizations and industries to identify and effectively apply cybersecurity standards and best practices in response to the stated mission and need. The work will be a result of partnerships and collaborations bringing technical expertise into NIST as much as possible. The National Cybersecurity Center of Excellence (NCCoE)[39] is an example of active partnerships and collaboration increasing expertise.

ACD as a whole is made up of three groups: 1) The Trusted Identity Initiatives Group, which includes the use of the National Strategy for Trusted Identities in Cyberspace (NSTIC)[40] program, 2) the Cybersecurity and Privacy Applications Group, which includes a significant list of efforts working with various verticals and sectors such as Health IT and HHS. The Cybersecurity Framework and smart grid work are included in this group, as well as a collection of activities related to small business outreach and other outreach programs including Federal Information Systems Security Educators' Associations (FISSEA),[41] and, 3) the NCCoE, along with the National Initiative for Cybersecurity Education (NICE) program.

The NICE program headed by Rodney Petersen, is a National endeavor. The focus is to review tools, programs, strategies, and activities from industry and associations that work with academic community to further cybersecurity education. The NICE strategic plan is scheduled to be published in the coming month where the focus will be on 3 strategic goals; accelerating learning and skills development, nurturing diverse learning environments, and guiding career development and workforce planning.

The seventh annual NICE Conference & Expo[42] was held in November 2016 in Kansas City. The prior year's event was held in San Diego, with phenomenal attendance. Last year was the first year it was held outside of the Washington DC region.

The NSTIC is part of the Trusted Identities Group. It includes a heavy coordination between CSD and ACD as well as other parts of ITL. NSTIC involves a strong emphasis on technical research and implementation such as with PIV.

The Board asked how the NSTIC program is going. This is the fifth year that NIST is engaged with the NSTIC program. NIST has learned a lot from the positive and negative outcomes of its pilots. What comes from it is the ability to take some of the core capability of NIST such as measurement science, and apply it to identities within NSTIC.

The Board stated the most trivial component of "identities" is determining whether there is a human being at the other end or not. The Board understands that a lot of problems exist with usability.

[39] http://csrc.nist.gov/nice/
[40] http://www.nist.gov/nstic/
[41] http://csrc.nist.gov/organizations/fissea/home/index.shtml
[42] https://www.fbcinc.com/e/nice/default.aspx

Usability is a core NSTIC element. A lot of the work in usability has been focused on the individual. We are also taking a broader view to identify the device as well. NIST had recently issued a draft NIST internal report (IR) 8103 Draft Advanced Identity Workshop on Applying Measurement Science in the Identity Ecosystem: Summary and Next Steps, that documents detailed results from NSTIC workshop,[43] January 12-13, 2016.

In the Cybersecurity and Applications Group, many programs and projects make up that portfolio including the Cybersecurity Framework (CSF).[44] The CSF continues to be a positive spotlight on that program. The Board stated that the CSF has been widely received and widely used, but identified this working worry that it is on the edge of some sort of regulation or requirement. Has NIST identifies that concern, and if so, has there has been any activity to try to address that concern. NIST understood that concern early on. In December 2015, NIST issued a request for information (RFI)[45] and asked a lot of specific questions regarding the use of the framework and areas for improvement. The theme that NIST received from the RFI response was to keep compliance voluntary. The international aspect is important to note as well, since there has been significant use and positive response domestically, and tremendous interest and updates globally. It provides a foundation for a global cyber dialogue. In the CSF workshop,[46] April 6-7, 2016, there will be representatives from the Italian government as well as a representative from Nippon Telegraph and Telephone (NTT) on a panel. The workshop is quickly reaching capacity. It has registered well over 700 attendees to this free event at the NIST campus.

A few other programs in collaboration with the engineering lab include taking the results and output of the cybersecurity framework and applying it in a lab setting to evaluate the impact of security on the performance of these technologies but also review security capabilities

The NCCoE ribbon cutting was held on February 8, 2016. It was very well attended. The event had significant industry attendance, including Secretary Pritzker from the US Department of Commerce, and was attended by many individuals from Maryland's Congressional delegation including Senator Barbara Mikulski. Senator Mikulski gave the keynote address and cut the ribbon. A highlight from the event was the demonstration held at the Birmingham Point of Sale (PoS) workshop. The PoS workshop had wide attendance including many individuals from the financial services sector.

The outputs of the NCCoE also include *NIST Cybersecurity Practice Guides* (SP 1800 series) which is a new subseries created to complement the SP 800s; targets specific cybersecurity challenges in the public and private sectors; practical, user-friendly guides to facilitate adoption of standards-based approaches to cybersecurity.

The Cybersecurity National Action Plan (CNAP) consisted of a series of activities that were conducted by OMB after the 60-day cybersecurity review. It included a number of requests for NIST to help federal agencies. One was a whitepaper issuing guidance on best practices in authentication of user accounts, for example utilizing a PIV card. Another document was guidance in helping federal agencies in recovery

[43] http://www.nist.gov/nstic/events.html
[44] http://www.nist.gov/cyberframework/
[45] http://www.nist.gov/cyberframework/upload/RFI3_Response_Analysis_final.pdf
[46] http://www.nist.gov/itl/acd/cybersecurity-framework-workshop-2016.cfm

operations, not just security controls, or limited to protective mechanisms or identification, but also addressing contingency planning. This identifies what an organization should do after an incident to restore operations.

The Board asked how that is developed – are there workshops? The workshops started at RSA, where an industry meeting was held. NIST requested from industry experiences in this space including use of tools, technologies, and practices that could form best practices. NIST's timeline on this is aggressive and is focusing at the technical capability for an organization to restore business practices and business recovery operations.

The Board stated it would be good to have outreach with regulatory agencies to share this information so that they can understand recovery lessons and alignment with regulation. There will be a recovery focus in two sessions at the CSF Workshop[47] on April 6-7, 2016.

Mr. Charles Romine, Director, Information Technology Laboratory, NIST, joined the meeting briefly to discuss how to engage the Board with NIST at a larger level. He talked about larger research areas in which he is concerned, and where he would like to get input. He hopes to have the next ISPAB session at NIST, to provide a mental reset and introduce the Board to other members of the lab and NIST leadership. Mr. Romine is very interested in having other divisions of NIST, for example, the software and systems division, advanced network division, mathematics division, and laboratory metrology, to have opportunities to discuss specific security practices such as PGP, networking, and some of the vertical spaces.

Legislative Updates relating to security and privacy

Matt Grote, Senate Homeland Security and Governmental Affairs Committee

The Chair welcomed Matt Grote from the Senate Homeland Security and Governmental Affairs Committee to the meeting to update the Board on legislative updates relating to security and privacy. Matt Grote noted that as it is an election year, there is not much pending.

The following bills were at various stages of activity during the last year:

- A bill requiring trading companies to disclose the types of expertise of their boards of directors. The SEC gave out guidance on cyber incidents, and the feeling is the bill will not likely go this year.
- A bill regarding a dispute between an agency and its union where access to agency webmail was turned off to deny union access because it was a security threat. The CISO and/or agency head has the final say on the security controls to pre-empt this decision at a particular agency. It was referred to the Senate Homeland Security Affairs committee. The agency head will have the final decision for the agency. The bill passed the House.
- A bill to codify DHS outreach passed the House that focuses on local/state governments regarding federal assistance to state/local governments from DHS. This is the bill that is most likely to pass this year.

[47] http://www.nist.gov/itl/acd/cybersecurity-framework-workshop-2016.cfm

- In addition, there are two bills in discussion now on encryption: The McCaul - Warner Commission bill was not sent to Chairman McCaul's committee in the House. In the Senate, it was referred to the Homeland Security Government Affairs committee. Chairman Johnson supports it, but it is not clear when further action may take place.
- A vote is expected on the Burr-Feinstein encryption bill. This is the first time there may be an actual policy proposal on how to deal with the issue. Currently, the Communications Assistance for Law Enforcement Act (CALEA) is the baseline for this bill. The question is whether to extend CALEA to other types of devices or software applications. An alternate approach not based on CALEA may also be developed. It will serve as a baseline for public debate on the topic.
- A bill on FedRAMP cloud enhancement. There are different ideas about how well FedRAMP is working. It seeks to redefine the JAB as a clearinghouse for certification documentation. There is a bill for re-organization of the National Protection Program Directorate (NPPS). The bill may change the name, require an internal re-organization, or other conditions. The issue with this bill is, can Congress tell an executive agency how to organize itself? There are two schools of thought; there are those with strong feelings on all these areas and are skeptical that reconstruction will improve matters all that much, and those that believe Congress should defer to agencies to organize themselves. There may be some action this spring.
- Draft bill sponsored by Sens. Richard Burr and Dianne Feinstein is not having any success. Mr. Grote expects it to be a challenge this year, but it may act as the start up for conversation. There may be a markup of an existing bill, but there are procedures associated with that process. Currently, there is no interest in the House for a policy solution. There may be some CALEA related activity, but that is not certain at this point. It will be a tough road to get the bills passed into law.
- One of the major priorities last year was to turbocharge EINSTEIN. A bill was passed to broaden and deepen its capabilities. Einstein 3A is the model that will stick the longest. Defense has host based agents, and so has a better window into what is happening. It is still a long road, but are on the right path. Worked with Senator Johnson, a few controls highlighted in the Einstein bill (the Federal Cybersecurity Enhancement Act) would have helped to deter the OPM attack. The Einstein bill gives priorities and oversight capabilities. The FISMA report[48] was released on March 18, 2016, and the scores were somewhat disappointing, but there is better visibility into the state of federal agency security.
- Some senators are working on data breach legislation to move the government forward. It may not come to pass this year, but it is in the works. Are there cyber controls? It is likely, but Matt Grote is not included in the internal discussions. He anticipates that industry will want to weigh in on that issues.

The Board asked about the NPPD relating to the Federal Protective Service. Is there a physical protection counterpart to cyber? They should be integrated with NPPD. They assess every Federal building in the country. They have a mature process, and includes standards and processes. They are getting involved in cybersecurity relating to buildings (to combat threats to HVAC), etc. It is an area that requires attention.

[48] Annual report to Congress: Federal Information Security Modernization Act https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf March 18, 2016

The Board asked about the Congressional working group. The Judiciary and Commerce committees are gearing up to study policy. They work together from time to time to draft legislation. Is there other legislative oversight when there is not much legislative activity going on? There are many other bills in process to catch up on. There is a push to have a hearing on federal network security and network security in general.

There was hearing last year on the IRS data compromise. But IRS is not directly in the jurisdiction of the committee. Is there any letter or further action? IRS is a more of an independent agency, however, they are beginning to see the handwriting on the wall. The Cybersecurity Enhancement act called out MFA as well. Agencies must notify Congress within 7 days of a major breach, and follow with updates.

Public Participation

There was no public participation.

Presentation on the Auto-ISAC and Vehicle Cybersecurity Best Practices [49]

Michael Spierto, Director, Federal Affairs, Auto Alliance
Pranav Saha, Lead Associate, Booz Allen Hamilton

The Chair welcomed Michael Spierto from the Auto-ISAC and Pranav Saha from Booz Allen Hamilton to the meeting to update the Board on the Auto-ISAC and vehicle cybersecurity best practices. The Auto Alliance is an association representing 12 automakers covering 77% of cars and light trucks on the road today.

There are a variety of new innovations being developed that enhance driver safety, fuel economy, reducing emissions, and others. Recent focus on automated vehicles which are the future of driving. Automated vehicles still represent the unknown, which causes many questions to be raised. Connectivity of vehicles is increasing every day, along with cybersecurity and privacy questions. The Auto Alliance is working to make sure security is "baked in". Consumer privacy principles have been developed to cover what automakers do with consumer driving data. They contain a set of promises to cover that data. The consumer must make an actual choice to opt-in and sharing information will require an active decision. It does not mean sharing with marketers for advertising purposes, or the government, and will not include sharing geolocation.

Consumers may feel pushed into sharing more information than they wish to because they believe they may not be able to operate their cars otherwise. Do automakers understand the sharing dilemma as perceived by consumers? Consumers should understand that only personally identifiable information (PII) is involved in the information sharing request. The privacy principles were released in 2014. In 2015, automakers started the auto-ISAC and majority of automakers participate. There is a board with a chairman and an acting executive director. Most other ISACS were formed following breaches. The auto industry has formed its ISAC before a hostile breach occurs.

[49] https://www.transportation.gov/briefing-room/secretary-foxx-unveils-president-obama%E2%80%99s-fy17-budget-proposal-nearly-4-billion

In January 2016, a framework for best practices was released. This was done in coordination with NIST and Carnegie Mellon. It is a work in process. The auto-ISAC is examining five areas: vehicle security by design, risk assessment and management, threat detection and protection, incident response, and collaboration and engagement with appropriate third parties. It's focused on the consumer and the vehicle; but to focus on the vehicle the focus must be on peripherals to the vehicles and things that interact with the vehicle. Manufacturing security is in scope for the group.

Is vulnerability disclosure included? It is included in the best practice development effort. They will be developing best practices for each OEM to be able to explore, invent, and create key differentiators in the market; to explore the best way to do cybersecurity for automobiles and develop guiding statements for cybersecurity.

Booz Allen is supporting best practice development, including a comprehensive reference model for vehicle cybersecurity and risk perspectives. There are two main work products: a reference model for vehicle cyber security and best practice guides. Each automaker must decide what will be implemented based on individual risk assessments. The reference model will be comprehensive. It includes identifying who/what communicates with a vehicle and in return, who/what the vehicle talks to.

The second work product will be best practice guides. They will go into detail on reference model topics. Development of the reference model and reference guides are in progress. They anticipate the model and guides to be in near final form within the next 2 months.

The Board asked what is the external facing mechanism or is it internal to industry. It is internal to industry for now. There is no certification process. The privacy principles have been submitted to the FCC, and are now available to the public. Is it anticipated the framework will talk about over-the-air updates? Over the air updates will be included in the model. They will attempt to be implementation neutral, if that is possible.

Mr. Spierto noted that the two most important things government can do to help is to promote cyber hygiene and develop a knowledgeable work force. Cars have become complex. Owners must figure things out on their own. Manufacturers are assembling components from their supply chain. The collection of suppliers of components is changing. The relationship to software suppliers is not dependent on a particular customer. The supply chain is included in the best practice model. They are looking at supplier management relationships and requirements for cybersecurity, they are also adding best practices, and in-house testing for software, as well as the service provider portion of the supply chain.

These technologies have huge benefit in that they reduce traffic, congestion and costs, and that story needs to be balanced with the potential to do harm. Education still needs to happen with the public and the government. Fear of the unknown draws the headlines. Studies have shown most accidents are caused by human error. Automating vehicles has the potential to drastically lower the numbers of accidents.

Board – Wrap-up

Dr. Weinberger brought the following items to the attention of the Board:

1. Reminder to NIST management that the board is not at full membership. Currently, there are two vacancies. Members representing "Non-Fed producers" are needed. The website has been updated with information regarding the Board vacancies. The Board is now reporting to the Secretary of DHS.
2. Mr. Boyer and Dr. Weinberger owe drafts of letters to the Board, to be forwarded to Mr. Scholl for the review process. Letters on - Vulnerability reporting status and use of ISO standards.
3. Meeting dates for 2017 – NIST will propose dates via email to Mr. Scholl. Board members should advise Mr. Scholl if there are known conflicts with dates. Availability of space at the Access Board is also a factor in selecting dates.
4. Dr. Weinberger is stepping down from his position as Chair. Mr. Boyer is the incoming Chair.

Response to ISPAB recommendation letter on quantum computing

The Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology, had responded to a recommendation letter that the Board submitted regarding quantum resistant cryptography. This the first time a response has been sent to ISPAB at least since 2007.What is the Board's intended action in terms of the timelines involved as stated in the letter? The response depends on the pace of progress. The Board would look for additional information in the fall, respond accordingly at that time, and annually thereafter as warranted by developments.

The Board is able to provide a response regarding, "whether NIST has made the necessary investments in human capital…" as cited in the letter and agreed to respond on that basis.

Review of Meeting

- Wassenaar – Follow up on the plenary in December 2016
- Commission on Enhancing National Cybersecurity - The Board heard comments from Ms. Todt on the commission, which sounds promising. The Board will work on a letter in June. – The Board may draft a letter to the Commission on Enhancing National Cybersecurity noting audience knowledge will be critical to the commissioners. Short and long term audiences need to be included in the recommendations.
    - Volunteer(s) are requested to draft the final recommendations. It will be a collaborative effort. The commissioners will contribute. Everyone involved will have some input. The collaboration software to be used by the commission will be determined by the commissioners. Meetings around the country are anticipated, with the number of meetings and logistics have yet to be determined. The Board's continuing input is appreciated.
    - Dr. Weinberger asked the Board's opinion of a possible letter to the commission now? There is no clear idea on the content at this time or wait until the next meeting of the Board in June and possibly think more about what should be in a letter and discuss at

the June meeting. June will be following official announcement of commissioners.

- Ideas for letter topics include defining success, avoiding duplication, the pyramid theme. Mr. Garcia noted the Board is concerned with the progress of federal information security, and should deal with the letter from that position. The Board determined to wait until June.

- The Board to discuss on a possible response to a letter it received from the Department of Commerce weighing in on one aspect mentioned in the letter.
- Cryptographic Module Validation Program (CMVP) - The Chair noted accessing the ISO standard costs $200. The government is proposing adoption of the standard and charging money for interested parties to have access to read it. ISO has stated it has a plan to make the standard more widely available to vendors. The Chair is proposing the board write a letter to urge a more flexible solution to making the standard available to vendors. Ms. Anton noted the cost is a burden to researchers as well. The Board passes the motion to write a letter. (No formal motion, no second). Quorum of 8 members present. The Chair proposes a letter to the effect that if the government goes the route of charging for access to the ISO standards, NIST should make it more accessible by not charging so much money. Most ISO standards cost money to access. Some are free. Not all can afford the $200 cost. Dr. Weinberger proposes NIST negotiate with ISO to get more favorable pricing. (Post meeting note: A recommendation letter was submitted to the Director, NIST in April 2016)
- Letter on the CVE process for Open Source Mr. Boyer will draft the initial version for the Board to review. Topic: Expanding CVE process to accommodate open source. The board passes the motion to write a letter.
- Future meeting topic for June 2016 on the commission.

Appreciation

Mr. Romine expressed appreciation for Dr. Weinberger's service on behalf of the leadership at NIST, and looked forward to Mr. Boyer's chairmanship. Dr. Weinberger also expressed appreciation for Ms. Sokol's work with the Board.

Adjournment

The Board did not discuss the future agenda as Mr. Boyer is not present. Mr. Garcia moved the meeting be adjourned. The meeting adjourned at 11:15 A.M., Friday, March 25, 2016.

ANNEX A

List of Participants

Last Name	First Name	Affiliation	Role
Annie	Sokol	NIST	DFO
Bales	Carol	OMB	Presenter
Blauvelt	Tom	Symantec	Presenter
Burke	Will	DHS	Presenter
Chenok	Dan	IBM	Presenter
Coble	Krysta	DHS	Presenter
Condello	Kathryn	Centurylink	Presenter
Cook	Melanie	NIST	Presenter
Cooper	Michael J.	NIST	Presenter
Dodson	Donna	NIST	Presenter
Goodrich	Matt	GSA	Presenter
Goodrich	Matt	GSA / FedRAMP	Presenter
Grandison	Tyrone	DOC	Presenter
Grote	Matt	Senate Homeland Security and Governmental Affairs Committee	Presenter
Howell	Michael	ACT-IAC	Presenter
Landfield	Kent	Intel	Presenter
Olcott	Jacob	BitSight	Presenter
Ozment	Andy	DHS	Presenter
Polk	Tim	OSTP, White House	Presenter
Porter	Christopher	FireEye	Presenter
Rarog	Bob	DOC	Presenter
Saha	Pranav	Booz Allen Hamilton	Presenter
Scholl	Matt	NIST	Presenter
Shannon	Greg	OSTP, White House	Presenter
Spierto	Michael	Auto Alliance	Presenter
Stine	Kevin	NIST	Presenter
Stine	Kevin	NIST	Presenter
Todt	Kiersten	NIST	Presenter
Vassilev	Apostol	NIST	Presenter
Viens	Joe	Time Warner Cable Inc.	Presenter
Vrooman	Ken	DHS	Presenter

Last Name	First Name	Affiliation	Role
Drake	Robin	Exetergov	Staff
Salisbury	Warren	Exetergov	Staff
Boyens	Jon	NIST	Visitor
Brosnihan	Carolyn	DHS	Visitor
Butkiewicz	Daniel	SAIC	Visitor
Conway	Tom	FireEye	Visitor
Dillon	Caroline	DHS / USCIS	Visitor
Dodson	Donna	NIST	Visitor
Galloway	Gary	Galloway Consulting, LLC	Visitor
Kans	Michael	Williams & Jensen	Visitor
Morgan	Sean	Palo Alto Networks	Visitor
Romine	Charles	NIST	Visitor
Sedgewick	Adam	NIST	Visitor
Souppaya	Murugiah	NIST	Visitor
Suh	Paul	DHS	Visitor
Taylor Moore	Debbie	Cyberzephyr, LLC	Visitor
Witte	Greg	G2 Inc.	Visitor
Chowdhry	Aisha	Federal Computer Week	Visitor/media
Curran	John	Telecom Reports	Visitor/media
Gunter	Chase	Federal Computer Week	Visitor/media
Higgins	Joshua	Inside Cybersecurity	Visitor/media
Lyngaas	Sean	Federal Computer Week	Visitor/media
Mitchell	Charlie	Inside Cybersecurity	Visitor/media
Noble	Zach	Federal Computer Week	Visitor/media
Otto	Greg	Fedscoop	Visitor/media
Rockwell	Mark	Federal Computer Week	Visitor/media

ANNEX B

NIST / Computer Security Division
DRAFT PUBLICATIONS
(November 2015 – March 2016)

Draft Special Publications

March 2016
Draft Special Publication (SP) 800-46 Rev.2**, DRAFT Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security**
Deadline to Submit Comments: April 15, 2016

Draft Special Publication (SP) 800-114 Rev. 1**, DRAFT User's Guide to Telework and Bring Your Own Device (BYOD) Security**
Deadline to Submit Comments: April 15, 2016

Draft Special Publication (SP) 800-154**, DRAFT Guide to Data-Centric System Threat Modeling**
Deadline to Submit Comments: April 15, 2016

Draft Special Publication (SP) 800-175 B**, DRAFT Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms**
Deadline to Submit Comments: April 29, 2016

February 2016
Draft Special Publication (SP) 800-166, Derived PIV Application and Data Model Test Guidelines
Deadline to Submit Comments: *March 14, 2016*

Draft Special Publication (SP) 800-180**, DRAFT NIST Definition of Microservices, Application Containers and System Virtual Machines**
Deadline to Submit Comments: March 18, 2016

January 2016
Draft Special Publication (SP) 800-90 B, Draft SP 800-90 Series: Random Bit Generators Recommendation for the Entropy Sources Used for Random Bit Generation
Deadline to Submit Comments: ***May 9, 2016***

December 2015
Draft Special Publication (SP) 800-116 Rev.1, Draft A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)
Comments submission closed February 1, 2016

Draft Special Publication (SP) 800-156, Draft Representation of PIV Chain-of-Trust for Import and Export

Comments submission closed *January 28, 2016*

Draft Special Publication (SP) 800-178**, Draft A Comparison of Attribute Based Access Control (ABAC) Standards for Data Services: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)**
Comments submission closed January 15, 2016

November 2015

Draft 1800-4, Draft Mobile Device Security: Cloud & Hybrid Builds
Comments submission closed January 8, 2016

Draft 1800-5, Draft IT Asset Management
Comments submission closed January 8, 2016

PRE-DRAFT CALL FOR COMMENTS
Special Publication (SP) 800-53 Rev.5, Security and Privacy Controls for Federal Information Systems and Organizations
Deadline to Submit Comments: April 1, 2016

DRAFT NISTIR

February 2016

DRAFT NISTIR 8105, Report on Post-Quantum Cryptography
Deadline to Submit Comments: *March 9, 2016*

DRAFT NISTIR 8103**, Draft Advanced Identity Workshop on Applying Measurement Science in the Identity Ecosystem: Summary and Next Steps**
Deadline to submit comments: ***March 31, 2016***

DRAFT NISTIR 8063, Draft Primitives and Elements of Internet of Things (IoT) Trustworthiness
Deadline to Submit Comments: *March 17, 2016*

Draft NISTIR 8011, Draft Automation Support for Security Control Assessments - Volume 1: Overview and Volume 2: Hardware Asset Management
Deadline to Submit Comments: *March 18, 2016*

A NIST Draft Whitepaper titled "Best Practices for Privileged User PIV Authentication"
Deadline to Submit Comments: *March 4, 2016*

December 2015

Draft NISTIR 8060, Draft (Fourth & Final Draft) Guidelines for the Creation of Interoperable Software Identification (SWID) Tags
Comments submission closed on January 8, 2016

Draft NISTIR 8085, DRAFT Forming Common Platform Enumeration (CPE) Names from Software Identification (SWID) Tags
Comments submission closed on *January 8, 2016*

November 2015

Draft NISTIR 8080, Draft Usability and Security Considerations for Public Safety Mobile Authentication
Comments submission closed on December 28, 2015

NIST / Computer Security Division
FINAL PUBLISHED PUBLICATIONS
(November 2015 – March 2016)

Special Publication 800-131 A Rev.1, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, November 2015

Special Publication 800-125 B, Secure Virtual Network Configuration for Virtual Machine (VM) Protection, March 2016

Special Publication 800-70 Rev. 3, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers, December 2015

Special Publication 800-57 Part 1-Rev.4, Recommendation for Key Management, Part 1: General, January 2016

NIST IR 7511 Rev. 4, Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements, January 2016

NIST IR 7904, Trusted Geolocation in the Cloud: Proof of Concept Implementation, December 2015

NIST IR 8074 Vol. 1, Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity, December 2015

NIST IR 8074 Vol. 2, Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity, December 2015

NIST IR 8055, Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research, January 2016