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

June 10, 11, and 12, 2015

Agenda http://csrc.nist.gov/groups/SMA/ispab/documents/agenda/2015_agenda-ispab-june-meeting.pdf

National Cybersecurity Center of Excellence (NCCoE) [1]
9600 Gudelsky Drive, Room B-105, Rockville, MD 20850 (240) 314-6801

Board Members	Board Secretariat and NIST staff
Peter J. Weinberger, ISPAB Chair, Google Chris Boyer, AT&T John R. Centafont, NSA Dave Cullinane, TruStar Kevin Fu, University of Michigan Greg Garcia, FSSCC Toby Levin Edward Roback, US Department of Treasury Gale Stone, Social Security Administration J. Daniel Toler, US Department of Homeland Security	Donna Dodson, NCCoE, NIST Matt Scholl, Board Secretariat, NIST Annie Sokol, DFO, NIST Tatiana Laszczak, Exeter Government Services, LLC Robin Drake, Exeter Government Services, LLC

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

Wednesday, June 10, 2015

Welcome and Remarks

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

The ISPAB Chair, Dr. Peter Weinberger, called the meeting to order at 9:01 A.M. and welcomed the board members. He noted a board quorum of seven members present despite three existing vacancies on the board at this time. He also noted the terms of three board members, Dr. Kevin Fu, Greg Garcia and Toby Levin, will be ending in November 2015. While Dr. Fu had declined to serve another term, both Ms. Levin and Mr. Garcia agreed to serve a second term. It had been a tradition to invite retiring members to give a presentation of their choices at their final meeting. Each board member provided a brief update of their activities since the last meeting in February.

1 National Cybersecurity Center of Excellence http://nccoe.nist.gov/

Information Technology Laboratory (ITL) Realignment and Proposed Applied Cybersecurity Division

Donna Dodson, Chief Cybersecurity Advisor, Information Technology Laboratory (ITL), NIST, and Director, National Cybersecurity Center of Excellence (NCCoE) (PPT presentation provided)

The Chair welcomed Donna Dodson, Chief Cybersecurity Advisor, Information Technology Laboratory (ITL), NIST, and Director, NCCoE, to the board to discuss the ITL Realignment and Proposed Applied Cybersecurity Division.

Ms. Dodson described a number of activities occurring at NIST and NCCoE this week, including: the meeting of Visiting Committee on Advanced Technology (VCAT), National Research Council (NRC) Laboratory Assessment [2] of NIST divisions namely the Information Access Division and the Software and Systems Division; and a workshop on elliptic curve cryptography with visiting staff from Microsoft at NCCoE. A scheduled tour of NCCoE facility had been arranged for the ISPAB on Thursday afternoon.

Ms. Dodson mentioned that Ari Schwartz, the scheduled moderator for this presentation was called into a briefing at the White House and would not be attending the board meeting in person but may possibly be in attendance by phone.

Ms. Dodson began with general discussion and background on the proposed ITL realignment. Currently, there are six divisions within ITL[3]: Applied and Computational Mathematics, Advanced Network Technologies, Computer Security, Information Access, Software and Systems, and Statistical Engineering. The ITL front office is also part of the lab. Other resources include the NCCoE and National Strategy for Trusted Identities in Cyberspace (NSTIC).

Primary considerations for the lab expansion included considerable resource expansion in cybersecurity over the last five years with rapid growth in new programs. Ms. Dodson reported that the NSTIC began with one employee and had since increased to twelve full time employees. NCCoE began with three or four staff members, and today, there are approximately fifty full time employees. Other ways to align management and administrative spaces for these programs were considered. Last year, National Initiative for Cybersecurity Education (NICE) received federal funds for cybersecurity education. Mr. Rodney Peterson, NICE, who will be presenting to the board today, joined NICE earlier this year. Some programs initiated in the ITL front office and have since matured and need to be fostered to continue growth.

Several options were considered to accommodate the growth that has already occurred:

1. Move current cybersecurity programs at the lab level into the Computer Security Division (CSD). CSD is one of the largest divisions within NIST.
2. Create a new division focused on applied cybersecurity that complements CSD.
3. Disperse aspects of the cybersecurity level throughout ITL.
4. Make no changes to existing structures.

NIST believes in mentoring employees and the importance of strategic planning. CSD would continue resource growth to meet demands in computer security and cybersecurity. The scope of CSD and ITL would be challenging for the front office to maintain.

---

2 http://www.nist.gov/director/nrc/
3 http://www-i.nist.gov/itl/OrgChart.pdf

The proposed new division with focus on cybersecurity and will foster thinking about standards and best practices, and building upon the work that is already being done. There will be no changes to existing structures. There has not been a focus on a new lab in the process of determining how to proceed with realignment.

In considering option 2, creating a new division, the following positive points were discussed:

1. Existence of the new communications lab in Boulder, CO.
2. New applied cybersecurity division – Move extensive resources currently engaged in cybersecurity operations from the ITL front office rather than lab wide support functions.
3. Provide a framework for integrating external stakeholders into the lab's cybersecurity applications activities, to more effectively utilize resources, and
4. Achieve better alignment of management and resource structure

The proposed structure for Applied Cybersecurity Division (ACD) will have a division chief and the following three groups: the NSTIC, cybersecurity and privacy applications, and the NCCoE. Areas like public safety networks, security in voting, cyber-physical systems and others will also be considered under the new structure. The new structure will take effect in the new fiscal year i.e. October 1, 2015. The vacancy for a division chief will be opened this summer so that search will be in process when ACD officially begins operation. In the interim, Dr. Charles Romine, ITL Director, will be the Acting Division Chief.

Proposed functional statements for the new division:

1. Applied Cybersecurity Division (ACD) – Implement practical cybersecurity and privacy through outreach and effective application of standards and best practices
2. Trusted Identity Initiative Group – Integrate and apply identity management technologies, standards and guidelines information and cyber-physical systems
3. Cybersecurity and privacy applications group – develop, integrate and promote the mission specific application of Information security standards, guidelines, best practices, and technologies.

Most functions of the remaining in CSD will not change. Work with research and standards, best practices at technical level will continue. Critical work in security automation will also continue. Software assurance and basics of mobile applications will stay in the computer division. The testing program focused on crypto-module validation testing over the last three years will remain in CSD. In total, only about nine people will transfer from CSD to ACD. When the permanent division chief is in place, he/she will determine group structure.

Panel 1 - A look from the inside

Nat Lesser, Director, NCCoE, NIST

Tim McBride, Associate Director, NCCoE, NIST

Katerina Megas, Lead Communication Strategist, NSTIC, NIST

Dr. Ron Ross, NIST Fellow, Computer Security Division, ITL, NIST

Ms. Dodson introduced and moderated the first panel discussion from the internal perspective of the proposed realignment. Panel members introduced themselves and provided brief descriptions of their responsibilities.

The ITL realignment is an extremely important initiative, and the new structure will allow greater growth, and opportunities for strategically planning. It will also focus on developing the fundamentals such as cryptography and security controls, and on outreach with offering of guidance to companies for implementation. There is shortage skill in cybersecurity, and the new structure will allow time for mentoring staff and for strategic planning. Therefore, a new division is long overdue and it is a good change.

The new division should resemble NIST's cybersecurity program (involving research). The coordination of division chiefs will help industry to see the broad spectrum of areas involved. Strategically, the new structure will also provide a structure for NCCoE for outward interactions with industry, focusing on commercial organizations and promoting cybersecurity practices. This will enable better communications and sharing best practices.

The CSD has designers while the new Division will have implementers. In practice it is necessary to have divisions working seamlessly together as one organization. Its structures will enhance internal bureaucratic processes and functions and will enable greater speed and agility in function. There is a mandate to "Operate at the pace of business".

The new Division needs to promote a greater degree of collaboration and to minimize silos with little separation in function and relationships. Creating matrix teams where possible will encourages knowledge sharing between groups and teams. Management must exemplify keeping internal connections viable by cultivating a common management viewpoint.

NCCoE will be releasing in the next few months five practice guides containing "how-to" guidance for industry. These guides under Special Publication series 1800, NIST Cybersecurity Practice Guides, will provide guidance and examples on how to implement standards and best practices. The intention is to help organizations improve and reduce the cost of deploying security technologies. Mr. Lesser's office is in the process of developing new publications that will align with the current SP 800 series of NIST special publications. The new 1800 publication series can be used across NIST. NCCoE is the first user of Special Publication 1800 series. It contains practical application of cyber security. Current work must be continued while assisting with implementation of new guides. New work in security engineering can be undertaken to a greater degree. NIST Special Publication 800-53 can be considered as application to a particular problem (implementing security controls, and developing new ones as needed).

These are published guides:

- 1800-1 Health IT: Securing Electronic Health Records on Mobile Devices
- 1800-2 Energy: Identity and Access Management

Future publications include:

- Attribute Based Access Management
- Mobile Device Security
- Financial Services: IT Asset Management

Panel 2 – External stakeholder discussion

Dan Chenok, Executive Director, Center for the Business of Government at IBM
Alex Popowycz, CIO, Health First (via telephone)
Ed Roback, Deputy Director, Office of Critical Infrastructure Protection and Compliance Policy, U.S. Department of Treasury

Ms. Dodson introduced and moderated the second panel discussion. The panel brainstormed the opportunities and challenges in the proposed structure from external stakeholders' strategic perspective. Tactical considerations included budget, integrated governance and communications with industry, and clearly identifying unique functional characteristics so they stand out from existing capabilities.

NIST's growth has made management by one individual unwieldy at this level. Technology transfer needs to be improved – witness recent data breaches. There is a great need for real world practical sharing. The current organizational divisions will need solid mission statements that are distinct from each other.

National Initiative for Cybersecurity Education (NICE) [4] Updates

Rodney Petersen, Lead, NICE (PPT presentation provided)

Mr. Petersen opened with a brief overview of his professional background and his work before joining NIST earlier this year. His time at NIST thus far has been focus on observing and building relationship. His goal is to develop a structure and plan for national cybersecurity education. Earlier strategies had emphasis on national centers for excellence. There is a recognized need for workforce support and education initiatives. Discussions are ongoing among academics regarding cybersecurity degrees or certifications.

More recently, an emphasis has developed in three areas:

1. General public awareness,
2. Public education, and,
3. Workforce perspective.

NICE received funding for the first time last year. The Cybersecurity Enhancement Act of 2014 was enacted late last year. Mr. Petersen discussed the existence of Federal scholarships for service programs with the National Science Foundation (NSF), cyber security competitions and challenges going on across the country, and the National Cybersecurity Awareness and Education program [5] at NIST as existing vehicles to raise awareness of education opportunities in cybersecurity. There are ongoing discussions about cybersecurity degrees or inclusion in current computer science or information science courses.

4 http://csrc.nist.gov/nice/index.htm
5 http://csrc.nist.gov/nice/awareness.html

NICE will be submitting its strategic plan to Congress in December, 2015. The organization is in the process of re-envisioning its role through national initiatives for cybersecurity education and workforce development (seeking private perspectives on national initiatives), establishing public-private partnerships with, government, academia and the private sector. Historically, partnerships have been led by the government. NICE is now seeking to have the private sector lead in this partnership.

NICE's Strategic Directions include the following goals: Accelerating Learning and Skills Development by exploring programs and techniques to rapidly increase the supply of cybersecurity programs; reducing time and cost for obtaining knowledge, skills, and abilities; targeting displaced workers or underemployed individuals who are available and motivated; taking advantage of opportunities to play into current priorities of the President and the Secretary of Commerce to connect people with job driven training.

Employers may have challenges in determining what skills are needed to fill cybersecurity jobs. Currently, there don't seem to be skill levels in cybersecurity or computer workers/skills. Changing employer mindset on what is required for positions is part of the process. Human Resources writes job specifications for cybersecurity positions. Often, employers follow the field in specifying "degree required" or a number of certifications needed in job descriptions, not because the degree is required but because it is required by other companies. It is a priority to change how human resources process hiring decisions. The focus needs to be on skills rather than knowledge. Not all jobs require degrees. There is a need to develop general titles for types of work and what is required and accurate position descriptions.

Cybersecurity careers need to be promoted to under-represented groups. We need to consider reasons why women, veterans, and others are not retained in these types of programs, to understand why some start but don't seem to finish. Promoting cybersecurity careers in middle schools or even earlier will help raise awareness of opportunities as awareness of jobs starts in elementary school.

Many programs exist at colleges with the potential to form a diverse learning community. Workforce demand and supplies of qualified workers will determine future hiring trends. Individual skills and abilities need to be effectively measured and rated against knowledge levels. Effective recruiting and hiring practices, and correctly relating years of experience and actual knowledge will allow the right people to get hired for the right jobs. Retaining talented workers in government is also a challenge.

NICE key programs and activities include: the National Cybersecurity Workforce Framework; annual conferences; NICE 365 calendar events look to increase presence and dialog on an ongoing basis. Outreach and engagement with government, academia and industry is critical to having a capable and educated cyber security workforce. Industry has a key role in building the workforce as employers of cybersecurity workers and service providers. Many available resources are oriented to large business. Developing resources for small and medium sized business is a concern. Small business may only have one employee to handle security concerns. It is crucial to assist them with getting the right combination of skills to effectively deal with cybersecurity.

There is concern that the US will not have the type of workforce needed for the future. Other countries appear to be accelerating in technical education in cybersecurity. The amount of government investment in cybersecurity is not known at this time. Academia and industry will need to partner in investing in educational programs with the government. UMD invested money at the time they started the cybersecurity program.

Executive Order 13694 Block the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities [6]

Andrea Gacki, Deputy Director of the Office of Foreign Asset Control (OFAC),[7] U.S. Department of Treasury

Ms. Gacki opened with a background presentation on the Office of Foreign Asset Control. OFAC implements 20-30 different sanctions programs on behalf of the US government. Sanctions programs can take different forms depending on the particular threat involved. Sanctions can be implemented against foreign countries, individuals, or other entities. OFAC's goal is furthering US policy goals and to support national security objectives.

Foreign financial transactions, to the extent US dollars are involved, that use the US financial system are prohibited. Foreign financial transactions going through US banks will be blocked and are required to be reported to OFAC. Sanctions have a real impact in this arena. Banks can pay heavy fines for not complying.

Executive Order 13694 is a targeted executive order. If banks have questions, OFAC has a compliance division and hotline for questions on correct course of action in any situation. Banks then are obligated to take action and block transactions.

This executive order authorized the Secretary of Treasury to impose economic sanctions on the named individuals. The language in the executive order is deliberately intended to state significant and malicious cyber-enabled activity. Individuals are tagged worldwide that identifies why they are on blocked list. Identifying information must accompany names on the list.

When Treasury designates a person (or entity) to be sanctioned, the name goes on a list. There must be identifying information for the individual including type of sanction. Scrutinized activities by entities must meet the "significant and malicious" criteria. Treasury takes steps to financially isolate actors. This makes it difficult for them to conduct financial activities. Treasury designations have global effect.

Ms. Gacki was asked to define "providing support" in the context of a sanction situation. The sanction is a strict liability regime. OFAC will examine the totality of circumstance. Witting engagement in these activities is a determining factor. OFAC in consultation with other government agencies will determine if support has been provided in violation of the sanction. Treasury has published FAQs for questions relating to this EO, along with a hotline.

Prohibitions are not limited to financial transactions. Knowledge of OFAC compliance is a goal for a greater number of companies. OFAC outreach to business is very developed. OFAC does not proscribe a compliance program. There is guidance on how to set up a compliance program. OFAC can provide consulting if needed. Blocked funds are frozen, and are kept in a blocked account at a financial institution. They do not become OFAC property. Sometimes real property is involved. Sanctions can have implications beyond the financial sector.

---

6 A) http://www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber_eo.pdf, B) FAQ related to E.O. 13694 Cyber-Related Sanctions page, C) posting on OFAC Recent Actions page that introduces the program. The White House Blog also posted some useful information about the program.

Additional information:

Cyber-Related Sanctions Page: http://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx
Public Notice: http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20150401.aspx
The White House Blog: https://www.whitehouse.gov/blog/2015/04/01/our-latest-tool-combat-cyber-attacks-what-you-need-know

7 http://www.treasury.gov/resource-center/sanctions/Pages/default.aspx

OFAC depends on the private sector for small or medium sized business participation. Sanctions very rarely target US persons, but it could happen. OFAC is not intended to replace US law enforcement action. OFAC has targeters who do the investigatory work to build cases. This work can involve other government agencies. The decision to impose sanctions is a government wide decision.

Some companies or individuals can work very hard to conceal illicit activities. Treasury is accustomed to dealing with these activities. Evasion or concealing activities goes on all the time. OFAC has its own investigatory capability and other agencies do bring leads. OFAC enlists experts when necessary. Currently, there is more work than the agency can keep up with.

There is an appeal process for being named on the list. There is also a de-listing process for those who change their behavior. OFAC is domestic authority; but also works internationally.

Financial transactions from other countries are not done in US dollars as a rule. Some foreign currencies will convert through the dollar for safety reasons. The percentage of international transactions done through the dollar is not really known at this time.

OFAC has civil enforcement authority. The US Department of Justice handles criminal enforcement. Depending on the circumstances, OFAC can opt to take no action on a case or issue a cautionary letter. There is no public reporting when these outcomes occur. When penalties are levied, amounts can be in the millions or billions of dollars. Sanctions take effect immediately. Public notice occurs when the sanctions appear on the website. However, publication in the Federal Register is the legal determinant of when sanctions start.

IG Reporting on FISMA

Gale Stone, Member, ISPAB, Deputy Inspector General, SSA (Moderator)
Brett M. Baker, Chair, Federal Audit Executive Council, Assistant Inspector General for Audit National Science Foundation (PPT Presentation provided)
Peter Sheridan – Senior Manager for IT Audits, Federal Reserve Board (PPT Presentation provided)

Ms. Stone provided an introduction for Dr. Baker and Mr. Sheridan. OIGs are required by FISMA to perform an annual evaluation to determine the effectiveness of the agency's information security program and practice. The presentation today is a discussion of a maturity model for government agencies. Dr. Baker and Mr. Sheridan will give an update to the work on, and the foundation with respect to the capability model.

Offices of Inspectors General (OIG) must perform annual assessments of agency information security programs and practices. These reviews cover technical aspects of security.

US Department of Homeland Security (DHS) has eleven areas of OIG guidance: Risk management, continuous management incident response and reporting, security training, plans of action and milestones, remote access management, identity and access management, configuration management, contingency planning, contractor systems, and security capital planning.

There are a variety of ways to protect networks in terms of architecture. Checks and balances must be in place to control security. Access control is critical. More can be done to incorporate architecture into FISMA practices. It is reviewed by the National Science Foundation board and others who provide oversight. The plan is to get past "yes/no" level checking for FISMA.

Other data calls such as CAP goals are covered under Plan of Action & Milestones (POA&M). TIC (trusted internet connection) and non-TIC connections re reviewed. IGs deal with all oversight related items for

agency compliance. FISMA manages IT security risk areas. Agencies should be using trusted internet connections.

FISMA framework provides views of narrative FISMA report important for reporting. It is one of the most important opportunities for FISMA to articulate unusual items that are occurring. It gives visibility and acts as status.

Audit tracking formalizes audit tracking responsibilities and status of those responsibilities. The capability maturity model will include the 11 areas and give a picture in the future. For other cybersecurity data calls, do inspectors general offices have oversight? They examine access ports, and what's coming from public internet. When assessments are done, these 11 areas are the drivers. Other drivers come from other agencies that may be audited. What else is used to measure agency security? All guidance becomes part of annual risk assessment.

Are we gaining or losing against threats? We get better at stopping existing threats but threats evolve. Many government agencies are paying attention to threats. It is constant work to keep up. Update guidance was given late last year. Agencies were required to submit a continuous monitoring information security strategy by November 2014.

In 2015, FISMA will require examining metrics in a different way. Reporting will include outcome oriented measures to better assess status of agency information security status. Capability maturity modeling makes sense in the government context. Annual scans by DHS will be useful. DHS has initiative for formalized process for regular and proactive scans of public agency networks.

FISMA 2015 Updates develop a format for updated DHS US-CERT incident notification guidelines for reporting information security incidents to DHS US-CERT. Agencies are required to report incidents within an hour of occurrence. New guidance clarifies what constitutes an incident that needs to be reported. OIG will assess the effectiveness of continuous monitoring programs by agencies.

The process of looking at a better way for OIGs to report FISMA work started four or five years ago. IGs put a lot of resources into doing the annual FISMA report. The Office of Management and Budget (OMB) developed questions for OIGs. Now DHS oversees the process. Recently there have been legislative changes striving to add consistency and transparency to OIG responses.

The FISMA Modernization Act was passed in December, 2014. It stipulated that each agency would have an independent evaluation to determine effectiveness of programs and practices. Under the old FISMA, there was an evaluation and demonstrated compliance of a subset of applications. Under the new FISMA, test compliance and effectiveness is determined as defined by NIST. Effectiveness is defined as ensuring controls are implemented correctly, operating as intended, and producing desired outcomes. Continuous monitoring work is now central. It includes a number of components.

Mr. Sheridan reviewed changes under FISMA Modernization Act. The old act checked for compliance only. The new reports whether controls are implemented correctly and producing the desired outcome with respect to meeting the security requirements. IGs are now providing guidance through technical assistance.

Proposed IG ISCM Capability Maturity Model:

- Level 1 – ad-hoc
- Level 2 – defined
- Level 3 – Consistently implemented
- Level 4 – Managed and Measurable

- Level 5 – Optimized

It gives a picture of what requirements still need to be met. The model will be an appendix to DHS OIG FISMA metrics. There is an 1-page bullet list. It is intended to demonstrate why an agency is at a particular level. It provides consistency across OIGs.

It is important to note that programs can be effective at lower levels. The object of the model is not to get to level 5. OIG FISMA metrics were issued in December. The document may be revised to include the capability maturity model as an appendix.

It is anticipated the model will be extended beyond continuous monitoring. Eventually, a dashboard will be provided to CIOs to document the maturity level. All reporting agencies will participate in the continuous monitoring evaluation in 2015.

FISMA will be working on the other ten areas over the course of 2015. They may be ready for review during FY2016. There will be a phased implementation. A lot of the measurements that are included in the maturity model still require agency staff people to document the measure of how to demonstrate evolution in the face of threats. Mr. Sheridan's office is presently looking at existing guidance to determine the role of documentation in demonstrating capability.

It is noteworthy that CMMI (Capability Maturity Model Integration) terminology is used in the maturity model. DHS was involved with Software Engineering Institute (SEI) in 2011. NIST was concerned about the use of SEI terms. Terminology used in this presentation is outcome of NIST and DHS editing. Work is beginning on the other areas, and evaluating if the existing areas are the right/best representations of maturity. Agencies are in the process of performing gap analysis to see where updated tools for continuous monitoring are needed.

Given the pace of gap analysis being done for government agencies, and that agencies are not being given money for tools to combat threats, it is not an unfair statement to say we are losing ground against the threat.

Vehicle infrastructure (auto-manufacturer communication and usability): Discussion on Data security and privacy

Andrew Lacher, Unmanned and Autonomous Systems Research Lead, MITRE (PPT presentation provided)

Mr. Lacher began his presentation with an explanation that a cyber-physical system is defined as a software-controlled system, or any software intensive system. His organization is striving for a trustworthy economy in terms of software assurance. This means there is safety, security, and efficiency in software.

Vehicles now are connected to the internet and that introduces vulnerabilities in a number of areas. The direction of society is toward increasingly autonomous systems. We have the potential to improve safety with software by:

- Improving safety – Reduce accidents and exposure to danger.
- Improving efficiency – Reduce manpower requirements and energy consumption.
- Enabling new capabilities – People become passengers in their own car.

Examples of increasingly autonomous systems –

- Unmanned aircraft - Have been around awhile. The FAA has oversight of unmanned aircraft.

- Flight deck automation - New developments happening on flight decks (iPADs on flight decks). FAA has oversight of developments in flight deck automation.
- Automated driving – There are newer developments in this field. There is no Federal oversight or certification authority with oversight on automated driving.
- Driverless vehicles – There are newer developments in this field. There is no Federal oversight or certification authority with oversight on driverless vehicles.

All these systems require increased dependence upon software, data, and command and control links in order to operate safely and securely. As has been stated, there is no certification authority for automated driving or driverless vehicles.

Lower-end cars today have 30-50 ECUs (inboard computers), made by different manufacturers. They are made to interface standards, but are not made by one entity. Some auto software is non-deterministic, and some is learning software. Consequences of failure can increase operational risks, idle fleets, and in some cases the vehicle itself becomes a threat. Phones know everything about users; cars collect data on drivers. We have no control where this data goes.

Deliberate attacks create safety problems such a denial or disruption of service, etc. Cars collect a lot of data that is transmitted to unknown entities without the driver being aware of what is being collected or who is receiving the data. There are no policies as to who has permission to use data, how it is protected or transmitted. Turning off the navigation system or other safety systems may be the only way to opt out of this data collection activity at the present time. Some data may be transmitted when car is in for service at the dealer particularly. Bluetooth signals can be used to collect data as well.

Unmanned aircraft are often connected to the public internet even when they are not flying (consumer grade unmanned aircraft). The primary manufacturer of unmanned aircraft is Chinese, and the manufacturer is collecting information on movement of these aircraft. Software updates and operations download occur over wireless connections when the aircraft is not operating. Wireless updates over the internet also occur in the automotive industry. EX: Tesla cars had a problem with gas tank vulnerability and uploaded an update over internet to change the suspension and the position of the gas tank.

Software updates are conducted wirelessly at any time. So when a car is not being used, there is potential for malicious updates. Research is ongoing in this area. Entertainment, GPS and engine monitoring systems all use the same display. There is connectivity that can be exploited.

The automotive industry is working to develop automotive privacy principles to clarify how they will work toward protecting information. These principles are not mandated at present. They are: Transparency, Choice; Respect for Context, Data minimization, de-Identification and retention (industry wide).

Data security, integrity and access, accountability are goals for the future. There is a movement to create an automotive information sharing and analysis Center (ISAC). A study is being done to determine the best way to create one. It will promote information sharing on attacks, and other areas.

The government is considering greater numbers of automated systems. Cybersecurity will be a big part of the implementation of these systems. Innovation leadership comes from industry and not from government. IT companies are now building cars as demonstrated in Google's self-driving car project.

What is the role of government in the oversight of regulation of technology? Studies show self-driving cars are safer. Automation does not have human failings that can occur in driving. But the car only

knows what it's programmed to do. It is difficult to anticipate every situation. This is where research is necessary. Driving behaviors learned in one area are not yet applicable to other areas.

What does it mean to say something "works"? Delays on implementation of this type of technology are applied because of caution on the part of manufacturers rather than government currently.

A clash of cultures exists between information technology and aviation as far as what the core goal is. Aviation is safety driven and founded on risk avoidance. IT culture is driven by innovation, and innovation is driven by risk. IT innovation rewards risk. Government oversight of automation is not keeping pace with technology development.

Trust of systems exists because of third party oversight of the consumer's relationship either to other individuals or systems. People have this trust because there is oversight of the relationship. Confidence in systems may be correct or may be incorrect. There are needs for an empirical measure of trustworthiness in systems.

Cyber resiliency has a number of areas: Cybersecurity, software assurance, and the ability to test. We need confidence that cars or aircraft are free of defects. Technology is progressing faster than laws or oversight. Government has been able to regulate after defects or safety failures have occurred, e.g., seat belts and anti-lock brakes.

FAA makes standards for aircraft. Others in the field do certifications of aircraft. There needs to be some set of standards for autonomous systems for automobiles.

In conclusion, cybersecurity cannot be thought of independently of other issues. We need confidence that our cyber-physical systems will function as intended despite: design defects, unanticipated data/situations and deliberate attacks. We need to think about system vulnerabilities while systems are operating and while not operating but connected.

The meeting recessed at 4:19 P.M., Wednesday, June 10, 2015.

Thursday, June 11, 2015

The Chair called the meeting to order at 8:37 A.M.

NIST Crypto Standards and Adoptions (PPT Presentation provided)
Quantum Cybersecurity (PPT Presentation provided)
Dr. Lily Chen, Acting Group Leader, Computer Security Division, ITL, NIST

Dr. Lily Chen began her presentation by explaining that she will be presenting two separate topics. Her first presentation addressed NIST Crypto Standards and Adoptions and concentrating on how crypto standards are adopted in the international community as well as industry. Dr. Chen gave an overview of the current types of cryptography standards referencing four areas:

1. Public Key Based (ex. FIPS (Federal Information Processing Standards) [8] 184, key establishment 800-65A/B/C)
2. Symmetric Key Based (ex. FIPS 197, 800-67, SHA 1/2/3, Randomized Hash etc.)
3. Tool Based (ex RNG, KDF)
4. Guidelines (ex. Hash usage / security, Transition, Key generation, etc.)

The first three areas are crypto standards and the fourth area details guidelines on how the standards can be used. The term "adoption" mainly refers to cryptographic algorithms (see slide 3) and the government accepting the standard bodies. Dr. Chen referenced NIST Crypto standards and major development examples that included: Advanced Encryption Standard (AES), Secure Hash Algorithm – 3 (SHA-3), organizational standards (SP 800-56A / 56B), and in-house developments (SP 800-56C).

Additional examples of standard bodies recognized by industry and internationally such as ISO (International Standards Organization), and one particular group that NIST cryptography is submitted for development includes ISO/IEC JTC 1 Sub-Committee (SC) 27 – IT Security Techniques / Working Group (WG) 2 – Cryptography and security mechanisms. Some standard bodies provide protection more than serving to engender trust. International products that are sold in the United States require standard protections, e.g. blocking ciphers. For example, a company can develop a product and use one algorithm within the block cipher library in order to maintain a cryptography standard.

The cryptography standards may be lead people to believe that cryptography security components are embedded in the standards. The standards organizations do not develop algorithms but algorithms are contributed by country members to the standards organizations for standardization. This is not only a NIST problem; it is government-wide as well as global. From a NIST perspective, they are caught in the middle of creating a FIPS as a standard and creating something that is globally acceptable.

There is a perception that people prefer the global recognition of ISO standards as opposed to FIPS, which are issued by NIST after approval by the Secretary of Commerce pursuant to the FISMA of 2002. Recently, there have been more discussions about the general requirements of algorithms be included in the ISO standards in the public domain.

Dr. Chen proceeded to the second presentation on Cybersecurity in Quantum Time. There are two recognized tracks of thought: 1) the "I" track referencing the idea of quantum cryptography from a

8 http://csrc.nist.gov/publications/PubsFIPS.html

theoretical perspective, and, 2) the "R" track referencing the reality quantum cryptography from a practical perspective.

Each Public Key Cryptography (PKC) scheme is faced with hard problems such as factorization, RSA, and discrete logarithm around quantum cryptography because the outcome is unknown. Dr. Chen referenced an example on how PKC is used today to protect Internet Key Exchange (IKE) and Transport Layer Security (TLS). However, with quantum computing technology today, it changes our understanding and recognizes "the hardness" of the problem. For example, all the PKC deployed since the 1980s must be replaced with quantum-resistant counterparts. Dr. Chen mentioned the impact to a symmetric key cryptography system is to use a larger key / hash size. However, the initial steps are to research problems that are computationally infeasible to be solved by quantum computers.

Some challenges in this space are, it takes time for a cryptography idea(s) to become useable and backward security is needed for confidentiality while many cybersecurity applications rely on PKC. The major challenges are: 1) security analysis against conventional computers, 2) security analysis against quantum computers, and 3) new quantum algorithm will solve the underlying hard problem. Additional challenges are: performance assessment is unknown for practical use (ex. proper key size, cipher text size and signature size), and smooth transition is possible for existing applications (ref. the PPT slides). NIST is researching security analysis against attacks and is focusing on existing schemes as well as to understand the practical implications of various analyses. NIST is also hosting bi-weekly seminars to study the proposals and results and collaborate with academia. Dr. Chen mentioned that the plan for the future is to continue to work on the security and to engage in interagency education.

Data Breach and Supply Chain Security

David Cullinane, Member, ISPAB, Founder, TruSTAR (Moderator)
Jerry Archer, SVP & Chief Security Officer, SallieMae
Paul Kurtz, Chief Executive Officer (CEO), TruSTAR

Mr. Cullinane provided a brief background in what started their pursuit to create TruSTAR.[9] There were a lot of companies concerned with the criticality of what is happening within their supply chain. Companies are producing products faster and cheaper than ever before which is largely their motto with consumers. Today, this has caused the primary issue with small to medium businesses and why they are being targeted by attackers. The attack model trending as a result are small businesses that work with larger businesses, and do not have good security, or lower levels, or none at all. Cyber-attackers breach the smaller businesses and find the connections to the larger companies and work their way up the ladder to breach the larger companies. This is a significant problem as emphasized by Mr. Cullinane.

Mr. Archer continued the discussion by stating that in their companies risk assessment process they have noticed a lot of aggravated risks when reviewing their vendor base. One issue is that the vendor base is largely outsourced which means from a day-to-day basis, which encompasses 200+ vendors, that have some form of access to either sensitive transactions or data. The trend is significantly larger amongst 4th and 5th party vendors due to outsourcing.

Mr. Archer emphasized that in the future the direction of breaches and attacks could lean towards retailers, medical devices and ransomware. Criminals tend to target the easiest path / opportunity. Another issue that occurred a few years back was that the cost of hardware needed to be driven down

9 https://www.trustar.co/

by manufacturers. Although this provided cost effectiveness, manufacturers were not prepared for the vulnerabilities that it created in the supply chain space.

On a larger scale, another growing concern in this space is the Internet of Things (IOT) with the potential of having 50 billion devices connected to the internet – what happens to the devices that cannot be upgraded? Mr. Archer commented that, essentially, there will be vulnerable devices in the billions that are exploitable with no capability to upgrade or patch. Manufacturers either must be forced to build in upgrade capabilities and if they do not want to support a device another company must be able to take over and provide the service in the future. An alternative option would be to mandate that those devices that cannot be upgraded have an end of life (sunset) date rule which would remove them from the internet.

There seems to be two areas of concern in this space, vendors and external devices. In response to the board's question on how does the company exert controls, if any, or visibility within its customer base or vendors, at the basic level, there is an annual risk assessment of company clients (first party vendors). The vendors provide a list of all their partnered or outsourced vendors during the assessment and TruSTAR builds a list of vendors and perform analysis on those that are most at risk. They also examine customer trends and inform clients of any additional risks. TruSTAR performs all its own risk assessments and will do multi-day site visits if a client is deemed critical from a security standpoint. Mr. Archer pointed out a common thought among most industry groups, the thought that if they are not being attacked themselves they are immune.

Based on the breaches that have occurred, can it be determined that there has been less of a regulatory approach, and is it more of a public concern due to the news highlighting the breaches that bring more awareness to industry. There have been lawsuits that create a fear of how companies are liable. However, the House of Representatives passed a bill [10] that provides some relief for sharing cyber incidents although it is not a get out of jail free card for industry. In other words, if a company shares their cyber incident data "that's good", but it does not get an enterprise out of trouble.

The board asked if there was any impact to the insurance industry measuring the amount of malware coming out of each industry. The panel did not have insight into that data. It seems likely the insurance industry will unfold in time once information sharing occurs across sectors which will allow them to write better policies. The panel noted it was too early to tell if any improvement has been noted since the cybersecurity framework was released.

Another sector that people do not typically think about regarding supply chains is aviation. The aviation [11] industry is completely dependent on computers from the moment a passenger checks in online, baggage processing, flight monitoring etc. A 787 jet has a global supply chain that has physical and cyber related components. Planes are highly dependent on computer systems which make this an incredibly complex situation. Aviation is governed more by safety than cybersecurity. There has been some progress with the open group creating a framework and process.

There is a missing link regarding industry not sharing data around supply chain risks; especially in the counterfeit and fraud space. Every time there is a seizure of products a notice is generated to the provider but none of that data is being pooled together. There is incredible inefficiency in going after

---

10 http://www.nytimes.com/2015/04/23/us/politics/computer-attacks-spur-congress-to-act-on-cybersecurity-bill-years-in-making.html?_r=0

11 See GAO Report GAO-15-370 FAA needs a more comprehensive approach to address cybersecurity as agency transitions to NextGen http://www.gao.gov/products/GAO-15-370

counterfeit and fraud.[12] There is a risk of counterfeit parts inside IT equipment. How industries close the loop in supply chain and sharing the data associated with its risk needs to be determined in the near term in order to make progress in deterring counterfeit parts being used in IT equipment.

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, A Proposed Rule by the Industry and Security Bureau [13] (PPT Presentation provided)

Bob Rarog, Senior Advisor to the Assistant Secretary for Export Administration, Bureau of Industry and Security (BIS) (Dual Use Export Control), US Department of Commerce

Overview: The Wassenaar Arrangement consists of a 41 member multilateral export control regime. Notice of US implementation of the technical language being discussed today was agreed 2.5 years ago. The language involves network intrusion and network surveillance, and involves products and technology related to those areas. Controls for these products have existed for a while outside the US.

Export control systems are different in different countries. However, the US is unique in that it has a process known as "Deemed Export"[14] which essentially means the release of technical data to a non-US national to another country is considered the same as giving them the technology. The Federal Register notice [15] was published on May 20, 2015 with a 60-day comment period ending on July 20, 2015. It is unrelated to other administration initiatives in cybersecurity. The commentary process is to obtain feedback that may influence the specific language. BIS is looking for technologists and product development personnel specifically to provide feedback. Regulatory language will not apply precisely to technological products. Some level of interpretation will always be involved.

Countries may propose changes, but the process is long. There is some flexibility in interpreting technical language. Q&As are done on the government site. Wassenaar controls apply to software and technology for command and delivery platforms, but would not apply to the intrusion software itself. Controls only apply to systems that generate, operate, deliver and communicate with intrusion software.

There are ambiguities in the language that will need to be clarified. The language does not apply to open source code. Technology controls apply to release of intrusion technology. Commonly used software sharing some of the functions of command, and delivery platforms are explicitly excluded. Penetration testing products are included.

Will this help companies in the US obtain sharp tools? Mr. Rarog believes it will complicate the environment. Technology controls apply both to technology for development and production of command and delivery platforms and to technology required for development of intrusion software.

Intrusion software is defined to be specially designed to avoid detection by monitoring tools or to defeat protective countermeasures; and that is capable of extracting or modifying data or modifying the standard execution path of software in order to allow execution of externally provided instructions. It is about information on how to discover vulnerability in a system, information about the vulnerability, etc.

---

12 See US DHS Fraud and Counterfeiting http://www.dhs.gov/topic/fraud-and-counterfeiting
13 Wassenaar FAQs https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports/related-regulatory-information-faqs?view=category&id=33#subcat68
14 https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports
15 https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items

The Export Administration Regulations (EAR) [16] does not control: Fundamental research, publicly available data or open source software. The proposal includes controls on IP surveillance systems. Such systems act at the carrier level to intercept and analyze messages to produce personal and social information from internet traffic. It can be used for intelligence purposes or to maintain surveillance on individuals or groups.

With a narrow license exception for shipments or transmissions to US agencies and allied governments, a validated license will be required for all destinations except Canada. Licenses will be reviewed favorably if destined for US companies or subsidiaries. Industry impact and comments – most items caught by this proposal are already subject to controls due to encryption functionality; as a result, we already have some impact data from major vendors. BIS needs more information on the impact of proposed controls on internal corporate activity, and on the research community.

Mr. Rarog emphasized that BIS needs more information on the impact of proposed controls on internal corporate activity, and within the research community and welcomes the feedback from the board and public.

The Communications Security, Reliability and Interoperability Council (CSRIC) Report on Cybersecurity Framework [17] [18] (PPT Presentation provided)

Chris Boyer, Member, ISPAB, Assistant Vice President, Global Public Policy, AT&T, (Moderator)
Brian Allen, Esq., GVP, Chief Security Officer, Time Warner Cable
Robert H. Mayer, Vice President, Industry and State Affairs, USTelecom Association

Mr. Boyer opened the session with a brief background of work regarding the NIST Cybersecurity Framework conducted by Communications Security Reliability and Interoperability Council (CSRIC) Working Group 4 [19] (WG4).[20]

The group worked on a multitude of issues dealing primarily with conformity of the framework to the communications industry. In the fall of 2014, the board was presented with a summary of work performed to date. In March 2015, the final CSRIC report was published and has since been released. On June 11 of this year, the CSRIC was presented with an update.

Based on the direction given to the working group by the policy roadmap, Mr. Mayer spoke of providing assurances and guidelines to the FCC (consistent with the Federal Advisory Committee Act (FACA)), as well as to industry and to the public regarding cybersecurity (CS) risk management.

When Congress failed to enact legislation regarding cybersecurity risk, the President issued Executive Order (EO) 13636, providing NIST with clear guidance to develop the CS Framework. NIST was given one year to develop the framework and NIST met the deadline.

The framework produced in February 2014 became the model of the partnership between industry and government to address cybersecurity risk management, NIST was required to produce the final report no later than March 18, 2015. In short, the substantive effort ended in December, 2014. WG4 was given

16 https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear
17 http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf
18 http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_WG4_PresentationFinal_31715.pdf
19 https://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iv
20 See presentations and discussion from ISPAB meeting, October 2014
http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-10/october-2014.html

a free hand to develop the framework and to report on ongoing work. Because companies differ regarding risk profiles and risk tolerance, the framework is not a one-size-fits-all solution, but does provide meaningful indicators to achieve success. Mr. Mayer acknowledged WG4's efforts to suggest a series of metrics.

Work on metrics began in August 2014, at which time the case made that the CS Framework should have the flexibility to evolve and to remain useful, no matter what threat might develop. NIST offered guidance to the FCC on how to communicate the framework internally as well as externally, because the latter is predicated on the risks others bring into the picture.

WG4 was able to provide the FCC with three assurances, one of which was that, on a periodic basis, NIST would provide the FCC with ways to monitor cybersecurity risk status with individual companies, through private conversations and meetings. Mr. Mayer cited the Protected Critical Infrastructure Information (PCII) [21] Program of 2002, designed specifically for the purpose of encouraging companies to come forward and enter into private discussions with the government on cybersecurity issues.

By following the CS Framework, NIST assured the FCC of protection against civil liabilities, FOIA, state actions, and regulations. Without these assurances, organizations would never divulge information critical to maintaining the framework. Specifics on framework deployment, such as operational requirements, will be presented in a series of webinars, the next of which is scheduled for June 18.

WG4 provided the tools to determine the impact of cyber security incidents on communication networks and the amount of time required to restore the network backbone to its operating condition. However, WG4 assured the FCC that information specific to individual companies or specific incidents will not be published because of the threat the information could be hacked. WG4 also presented advice to companies and organizations on what they can do to develop metrics unique to them. To that end, NIST provided a tool in the form of Frequently-Asked Questions (FAQs) regarding CS risk management, published in February 2015.

While WG4 was directed to study network infrastructure and provide suggestions to keep networks in operating condition, timely feedback from interdependent agencies and industry is essential to the relevance and utility of the framework.

Updates on NTIA Cybersecurity Request for Comment (RFC) Stakeholder Engagement on Cybersecurity in the Digital Ecosystem [22]

Allan Friedman, PhD, Director of Cybersecurity Initiatives, National Telecommunications and Information Administration (NTIA), US Department of Commerce
Evelyn Remaley, Deputy Associate Administrator, NTIA

Ms. Remaley began by describing the purpose of the National Telecommunications and Information Administration (NTIA) as an agency within the Executive Branch of the government, and is responsible for advising the President on telecommunications and information policy issues.

The NTIA's involvement in developing next steps in the form of cybersecurity codes of conduct and best practices related to copyright and intellectual property issues based on a NTIA's Internet Policy Task Force (IPTF)23 green paper entitled, "Cybersecurity Innovation and the Internet Economy", June 2011.[24]

21 http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program
22 http://www.ntia.doc.gov/files/ntia/publications/cybersecurity_rfc_03132015.pdf
23 http://www.ntia.doc.gov/category/internet-policy-task-force

The NTIA examines risks spanning independent organizations and sectors, addressing cybersecurity risk issues resistant to unilateral solutions. For that reason, NTIA is working to bring stakeholders together to focus on the broader digital ecosystem, starting with the nuts-and-bolts of internet infrastructure and expanding to include the consumer space and web security. NTIA's goal is to offer help in addressing the fundamental challenges of securing the digital economy from a business process perspective. To attain that goal, NTIA has not, initially, tried to address "giant issues," but to study issues from a narrow perspective, in an attempt to identify issues that are self-contained and amenable to collective consensus and action. NTIA's efforts are directed toward precluding regulatory enforcement.

NTIA's goal is to bring industries, and groups of industries, together as fellow stakeholders. NTIA requested stakeholder comments in late March 2015, which listed several potential discussion points. The effort generated approximately 35 comments and spawned additional discussions. Currently, the effort is in the inter-review stage. NTIA is currently preparing a set of recommendations to share with the Internet Engineering Task Force (IETF).[25] The recommendations will not focus on "giant" issues, but rather on measurable impact. Once determined, the NTIA will announce the topic for discussion and locate a venue for the first meeting.

Stakeholders include participants from the telecommunications industry, the content industry, and researchers based in Silicon Valley. Issues under consideration included three broad areas: (1) The Internet of Things, (2) vulnerability disclosure, and (3) examining issues presently side-lined from active investigation.

Discussion on the internet of things will be useful in bringing people together in a non-regulatory environment and acknowledged that a significant amount of work has already been done, citing work in the automobile industry and work related to medical devices.

The issue of vulnerability disclosure is not new and includes existing documentation published by the Department of Homeland Security (DHS) and the International Organization for Standardization (ISO).

Some issues, like botnet identification and mitigation, have been sidelined. Spyware and malicious downloads have blurred the boundary between certain aspects of the consumer advertising industry and artifacts which might be injurious to the consumer security industry.

Topics already being addressed by Subject Matter Experts (SMEs) in a company, industry, or other organization are removed from consideration. NTIA does not attempt to develop new technical standards, but rather to help identify reduce large issues into well-defined areas subject to guiding principles. NTIA can then recommend specific points-of-contact to best address issues under discussion.

Updates on OMB Circular No. A-130 Revised[26]

Carol Bales, Senior Policy Analyst, OMB E-Gov Cyber and National Security Unit, Office of Management and Budget (OMB)

Ms. Bales enumerated specifics related to revisions to the OMB Circular No. A-130 Revised. The Circular is the overarching Information Technology (IT) policy regarding acquisition, management, staffing, and funding. OMB Circular No. A-130, which was last updated in 2000, is one of approximately 45 circulars, providing high-level policy on various topics, including federal resource management. A final update of

---

24 http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf
25 https://www.ietf.org/
26 https://www.whitehouse.gov/omb/circulars_a130_a130trans4/

Circular A-130 is set for December 2015, as mandated by the Federal Information Security Management Act (FISMA).

In April 2015, a draft of the A-130 Revised was disseminated to agencies for comments. The comments, received in early May, are currently being addressed. One significant change requires agencies to coordinate regarding information security and privacy as applied to federal information resources.

Today's presentation is focused on describing the content of Appendix III,27 which was previously titled Security of Federal Automated and Information Resources, known as Responsibilities for Protecting Federal Information Resources. Based on a new FISMA statute, Appendix III is a compulsory direction given to an agency for the purposes of safeguarding federal information from known or suspected information security threats. The A-130 team was organized to focus on cybersecurity policy and oversight.

In May 2015, DHS issued an unpublished binding operational directive, entitled, "Critical Vulnerability Mitigation Requirements for Federal, Civilian, and Executive Branch Departments, and Agencies' Internet Accessible Systems".

The board asked if "compulsory" meant instantaneous compliance in this instance. Compliance timelines are spelled-out in the OMB memoranda. As an example, the OMB under discussion directs which agencies must patch critical vulnerabilities within 30 days. It is also an ongoing requirement. Asked about the consequences of non-compliance, Ms. Bales said that the team has been given increased bandwidth to follow-up with those agencies.

Ms. Bales' team conducted eight sessions out of a planned twelve sessions. These sessions were to facilitate communication regarding revisions to the A-130, and were scheduled for completion by the end of fiscal year (FY) 2015.

Though the newly-revised Circular A-130 holds personnel accountable for following security policies and practices and for incident response and management, the circular omits specifics as to which agencies should report and when. Those details can be found in OMB memoranda, FISMA business guidance,[28] and NIST SP 800-61 Rev.2, Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology.[29]

The circular prohibits the use of unsupported system components, unless validated by the US Secretary of the Treasury, or an equivalent authority. It also mandates an audit regarding access rights granted to privileged users to help mitigate the risk of insider threats, and authorizes the oversight that non-federal entities hosting federal information comply with guidelines as published in NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (June 2015).[30]

The team is in the process of reviewing over 500 comments submitted in reference to A-130 as next steps" in the process. Once adjudicated, the circular will be prepared for internal OMB clearance with a 30-day period for public comment. It will then be circulated for additional agency review, with a goal to deliver the final version by December, 2015. The goal is not to add to precautions already in place, but to help clarify the process.

---

27 https://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii
28 http://www.dhs.gov/federal-information-security-management-act-fisma
29 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
30 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

NIST Computer Security Division Updates

Matt Scholl, Chief, Computer Security Division, ITL, NIST

Mr. Scholl began by referring to Ms. Dodson's June 10 presentation on ITL realignment, then reiterated his logistical challenges: managing 92 full-time government employees (not including guest researchers, students, and post-doctorates) as playing a key motivation for the realignment.

The easy task is defining an organization chart. But the difficult tasks are realigning budgets, property inventories, administrative support, travel allocations, website presence, and other critical concerns. The task was made easier because of the minimal impact on physical logistics (room location, access to print servers, phone, email account, and related concerns), which provided staff with the least amount of disruption. Mr. Scholl acknowledged Mr. Kevin Stine (currently a group manager), as acting manager overseeing the realignment effort.

In late May, additional funding (base money) was allocated for cryptographic work to cover staff, grants, contracts, and related support vehicles. Currently, talks are in progress with a number of academic institutions regarding expanding NIST's cryptographic capabilities. Next year's efforts will include research into several areas of post quantum cryptography, including issues such as crypto-utility, providing something resistant to an environment we don't yet understand, and something that will have to live in the quantum and classic arenas at the same time.

NIST organized the Workshop on Elliptic Curve Cryptography Standards on June 11 and 12,[31] considering whether more efficient and powerful curves are needed in NIST's elliptic curve cryptography or are the present curves adequate to address confidence in those curves. Discussion is just getting underway. Additionally, Lightweight Cryptography Workshop 2015 [32] is scheduled on July 20-21, 2015, at NIST campus to discuss lightweight vs. constrained cryptography.

There will be a need to deal with the requirements to write a new risk management document following the release of Circular A-130 Revised; examining how the framework can be implemented within Federal systems, and how to use the existing suite of NIST documents as references. Provision has already been made to delegate the work required to comply with the update. Resources have also been allocated in efforts related to broadband and communication technologies, as well as in public safety networks.

Efforts to increase awareness of the framework through training and other outreach mechanisms include Mr. Stine's team collaborating with the Small Business Administration (SBA) and the Federal Bureau of Investigation (FBI) in establishing InfraGuard chapters nationwide.[33] InfraGuard sites have been designated to host meetings between the SBA, local chambers of commerce, and local small businesses.

Research is also being conducted on cryptographic test and validation in accordance with FIPS 140, and SP 800-90A Rev.1[34] Recommendation for Random Number Generation Using Deterministic Random Bit Generators is due to be finalized probably during the week of June 21-25, after which NIST will test validation that entropy is not negative (which is different from saying that entropy is good).

NIST is also beginning to research mobile devices and applications, outside the context of a testing strategy, but to examine properties and qualities, as well as using mobile applications in specific

31 http://www.nist.gov/itl/csd/ct/upload/CFP-Elliptic-Curve-Crypto-June2015.pdf
32 http://www.nist.gov/itl/csd/ct/lwc_workshop2015.cfm
33 http://csrc.nist.gov/groups/SMA/sbc/overview.html
34 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

environments, actions which should be transparent. Tests will follow to determine the claim of transparency as compared to what is actually being done. Users should be able to tell if an application they're using is tracking information or transmitting information.

In May, NIST released DRAFT NIST Internal Report (IR) 8060 Guidelines for the Creation of Interoperable Software Identification (SWID) Tags [35], which is also an ISO standard used to uniquely identify software for forensic purposes, it is to be added to the National Software Reference Library (NSRL).

NIST is considering extending the utility of the National Vulnerability Database[36] (NVD) next year, to make it cloud-based, and to deploy as an AWS solution.

National Cybersecurity Center of Excellence (NCCoE) Demo/tour

Donna Dodson, Chief Cybersecurity Advisor, ITL, NIST, and Director, NCCoE

Ms. Dodson led the board in a walking tour of the NCCoE. The center, started two years ago, is a federally funded research and development center (FFRDC) operated with MITRE. NIST directs the work done at the center. The plan of new 1600 sf office space is being rolled out in the fall with 16 thousand square feet.

During the tour, the board saw the following two demos:

1. Attribute based access demo: The demo used a fictional merger example for access rights management. It uses TFA to identify users. It demonstrated how user permissions change as attributes for users are added. The business has the ability to change attributes. Ex: Receiving clearance information for users increased access to documents according to the level of clearance.

2. Health IT demo: Demonstration of security for electronic health records by Demonstrating certificate validation and blocked against attempts by unauthorized users.

The meeting recessed at 5:25 P.M., Thursday, June 11, 2015.

35 http://csrc.nist.gov/publications/drafts/nistir-8060/nistir_8060_draft.pdf
36 https://nvd.nist.gov/

Friday, June 12, 2015

The Chair opened the meeting at 8:05 A.M.

NIST Strategic Directions and Plans (PPT Presentation provided)
Dr. Richard Cavanagh, Acting Associate Director of Laboratory Programs, NIST

Dr. Cavanaugh opened his presentation with historical information on how NIST was founded in the early twentieth century and its mission, noting that NIST exists to work for commerce, not government.

The US has an increasing role in solving problems today. Areas include: Advanced manufacturing, Cybersecurity and advanced communications, Healthcare and bioscience, Climate change and clean energy, and forensic science. NIST is now in a partnership with the Department of Justice and co-chairing a Federal Advisory Committee Act (FACA) of thirty voting members.

Improving Critical Infrastructure Cyber security/ Cybersecurity Executive order: "America must also face the rapidly growing threat from cyber-attacks" (President Obama). Developed the Cyber Standards Framework (CSF) based on existing standards. Cryptography provides the basis for many security and privacy technologies used to support e-commerce. The CSF was released 12 months following the president's speech.

NIST is committed to increasing its resources and expertise in creating and maintaining cryptographic standards and guidelines. Commerce will have worldwide market places, so the United States must have standards to match. It focuses on advanced communications, global internet provider traffic, and advanced communications research. NIST created FirstNet (First Responder Network Authority) to provide an emergency responders nationwide network. The NIST research plan includes activities such as mission critical voice over LTE, and research in NetZero Energy (demonstrates net-zero energy used in home consumption).

NIST has involvement in healthcare; health IT, etc. Genomic Quality Assurance was a NIST led consortium with more than 75 public, private, and academic partners. NIST RNA controls played a role in key Ebola genetics study. NIST work was mentioned in published news reports at the time, but not the name. NIST is involved in critical efforts in medicine and other fields including nano-manufacturing, sustainable manufacturing, smart manufacturing, and robotics.

Conclusion –

NIST is involved in many programs in a nonvisible way. NIST needs input from FACAs.

There are many ways to prepare for the future. There is no formal method for preparing or determining what the future will hold. Forensics as a field has a lot of scientific activity.

Building blocks for determining work come from many places. Previously, NIST was self-contained in two campuses. Now there are nine Centers of Excellence and NIST is partnering with people doing the work to get up to speed more quickly. Those efforts are funded for five years. Applies to high visibility areas where learning is needed quickly.

Federal Chief Technology Officer's Priorities

Alex McGillivray, Deputy Chief Technology Officer, The White House Office of Science and Technology Policy (OSTP) (PPT Presentation provided – one slide[37])

Mr. McGillivray reviewed the makeup and mission of the Office of Science and Technology. There are four divisions in OSTP: Science group, environment group, tech and innovation, and national security/ national affairs. The CTO sits within those four groups, and the current team is the third CTO Team. The CTO position was created by President Obama.

The CTO is a very small team. Meghan Smith is the Chief Technology Officer. She joined CTO in 2014. Ms. Smith came from Google where she worked in various capacities. Mr. McGillivray was Twitter's general council. He now is lawyer and coder.

CTO Priorities –

1. Ensure America continues to be the best place in the world for science, technology, and innovation.
2. Innovate to make government more efficient for and with the public.
3. Make better use of America's most important asset – all of its people.

The CTO mandate is very broad: "Team CTO advises on how to unleash the power of technology, data, and innovation to advance the future of our nation." The broad mandate allows the team to act in many capacities. CTO focus is in three areas: Policy, Government, rest of US. Policy includes student privacy, and the Precision Medicine Initiative: Medicine is transitioning to having data security components. The challenge is how to think about that transition and how to support it as much as possible. Privacy is an issue. CTO is hoping to enable very large cohort studies in the future possibly with a million people.

Data coming in stovepipes is very tricky at the moment, and it is not easily shareable. It is also not clear of how the law corresponds to what people think about privacy. Consents will be necessary to distribute data to researchers. Precision medical initiative will help to determine which hypotheses are worth exploring. Data science becomes an additional tool to use. The team is still determining how approaches or policies will articulate goals. Principals within studies or regulatory contexts can assist in this area. There is no determining thought to revising HIPAA with regard to research on big data.

Patent/copyright protections are of concern. The CTO's office will be considering how changes in technology are related to policy. It is more prevalent for small companies to be caught in regulatory, and regulatory relationships are difficult with very small companies. It is a challenge for regulators to determine what is relevant or what should be looked at. The board suggested that compliance as a service as one approach.

Companies providing data to the government are concerned that the government cannot protect information. Victims of cyberattacks are worried about more breaches. Companies are deliberating whether to involve law enforcement and the concerns on compliance issues. Businesses in general believe the government is not a safe place for business information.

There is an intentional focus on bringing the best and brightest into government and retaining them. The CTO's office helped to institute the Presidential Innovation Fellows, 18F,[38] etc. Other offices such as

37 http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-06/ispab_june-12_cto-mission-priorities_amacgillivray.pdf

Office of Digital Strategy are increasing engagement between government and the public, OCIOs in government, and the US Digital Service (USDS). These groups are focused on delivering services and not products. Finally, David Recordon[39] was named Director of White House Information Technology in March 2015. He will be responsible for modernizing the White House's own technology.

The CTO is giving availability of large, publicly accessible digital data sets. Federal agencies have been working with the public and private sectors to make more data publicly available and easier to find and use. This raises an additional focus to add data scientists into government, and many government agencies are searching for data scientists.

There are many groups of people who have the potential to have an impact. Technology meetups are happening all over the US. Training and boot camps are going on all over, but not widely known to most people. Studies show men are much more heavily represented in certain areas. There are necessities to seek out varieties of opportunities to a broad range of people.

Additional areas of interest: Initiative to make broadband more available Includes connected initiatives; there are connectivity deserts in the US; increasing Science, Technology, Engineering, Mathematics (STEM) education; play space initiatives – a locality where multiple initiatives come together to solve problems. The challenge is to get more mileage out of budget while adding technical opportunities. CTO's Priorities arranged as 70% spent on core projects; 20% short sprints to change outside project course; 10% matchmaking, that is, putting people together that need each other to accomplish goals.

CTOs harvest valuable information about relationships. It is useful to know passion that drives Federal workers in various fields. Technology does not replace meeting people and building personal relationships.

On whether the FBI is reaching out to the CTO for advice on "Going Dark" problem, the response is that the President has been very specific problem. The President gave an interview on the going dark problem, a recommended read.[40] There is an ongoing process working on this problem.

The current administration has gone to great lengths to establish technology as central focus. Mr. McGillivray believed that results will demonstrate how this focus be institutionalized following the Obama administration. CTO will continue to communicate about what is being done, and to be able to point to those types of successes.

Updates on National Strategy for Trusted Identities in Cyberspace (NSTIC)

Michael Garcia, Ph.D., Acting Director, NSTIC [41] (PPT Presentation provided)

Mr. Garcia opened his presentation with an overview of NSTIC's primary goals: kill the password dead, address the "dog on the internet problem" and improve privacy. Identity and authentication are the roots to all existing cyber security problems. Identity or authentication (Exploitation of passwords) accounts for approximately 75% of breaches.

---

38 See ISPAB meeting agenda and minutes, February 2015 on the Overview of 18F https://18f.gsa.gov/ - http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-02/february-2015.html
39 https://www.whitehouse.gov/blog/2015/03/19/president-obama-names-david-recordon-director-white-house-information-technology
40 http://recode.net/2015/02/15/white-house-red-chair-obama-meets-swisher/
41 http://www.nist.gov/nstic/index.html

Mike Garcia presented these solutions:[42] Create an identity ecosystem: an online environment where individuals and others will be able to trust each other because they follow agreed upon standards and technical policy to obtain and authenticate their digital identities. Many other countries do this by using national ID cards. This will not happen in the US. Instead, develop a market place approach to underlying standards for guiding principles:[43] privacy-enhancing and voluntary, secure and resilient, cost-effective and easy to use. Create standards for inter-operability of credentials.

The identity ecosystem will allow bad technologies to disappear on their own when they get broken. Current system design does not allow broken technologies to disappear. Users should have a choice of how to authenticate themselves, and currently, there are not many options available to users. The idea that passwords technology is a failure has not been stressed.

There needs to be a market place of different types of solutions. People hate having their accounts hijacked and hate the account recovery process. People have a dislike for anything that blocks simple and convenient use of systems. People "trust" entities because they have to, not because they want to. The reality is that people do not trust each other on the internet. We deal with entities out of necessity. Trust on the internet is overused. Certificate authorities are intended to provide a basis for trust, but there is not a lot of trust. Trust has meaning in the context of a brand. A brand constitutes a promise. There must be some idea of trust because the average user won't have the knowledge to make a real determination. Where is trust derived? Trust could potentially be derived from a single federated credential. If there were better alternatives to passwords, passwords would not last long.

Connect.gov [44] is the government's answer to federated identity, a single service for establishing identity at public facing government applications. It is a double blind hub where a service provider can come in and be certified, and then integrate with the hub which will redirect to an agency that's authenticated. The agency has no idea what credential is being provided and the credential does not know the destination agency.

There is a year-long pilot underway to build government credential. 18F's MyUSA [45] could be the government-wide brand for credential use. There is a trust issue toward adopting this type of credential. Trust in agencies has eroded due to breaches. Consent management will be the same. There are a lot of agencies that are willing to provide the credential service to the government. However, empowering an agency that has a known mission may confuse things.

Mike Garcia continued with an updates on pilots that have moved to the market place.

- Thirty million dollars have been awarded to 15 pilots over three years. Accomplishments include NSTIC aligned multi-factor authentication (MFA) solutions, some being used in Connect.gov. Government's role in developing the marketplace is to be a catalyst.
- 2.3 million NSTIC aligned credentials and nine new MFA solutions deployed.
- There has been a lot of impact of the pilots in those 125 organizations. This approach has been catching on. People are reluctant to try new ways because they are resistant to changes.

In March, NSTIC released a report, NIST IR 8054 NSTIC Pilots: Catalyzing the Identity Ecosystem,[46] on the pilots with summaries and overarching needs. [47]

---

42 NSTIC Focus Areas http://www.nist.gov/nstic/focus-areas.html
43 NSTIC Guiding Principles http://www.nist.gov/nstic/guiding-principles.html
44 http://www.connect.gov/
45 https://18f.gsa.gov/2015/05/18/myusa/
46 http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8054.pdf

Dr. Garcia provided an updates on the Identity Ecosystem Steering Group (IDESG). There are over 350 members from various organizations and academia with participants from twelve different countries. It is a global enterprise with some big players in the group. American commerce must have global solutions. NSTIC used grants to convene IDESG, which became a non-profit. Currently, the group is developing later versions of framework.

In closing, Dr. Garcia described next steps for NSTIC:

1. Increase focus on the science and technology. It is time to evolve. NSTIC is heading toward technology efforts in privacy as well as policy efforts in privacy.
2. Update Special Publication 800-63 [48] - They are working on comments as the comment period closed recently.
3. Continue the pilots program, but evolve toward a focus on specific use cases and gaps that emerge in the market.
4. Continue research on comparing methods of authentication to see which is best.
5. Focus on market research and analysis. Move to sharing costs with the government.
6. Continue to transition pilot program building and technical capacity to seed the marketplace with better solutions. Over time the pilot portion may shrink, to be replaced with other types of programs.

Public Participation – see Annex B for written statement
Ken Durbin, Unified Security Practice Manager, Symantec Public Sector

During yesterday's session on vulnerabilities, the scenario with struggle between CISPO and auditor. It is noted that advanced persistent threats are only successful when vulnerability is present. Once penetrated into any system, attacker(s) can begin to explore opportunities. We need to examine how vulnerabilities are categorized and how that impact risk assessment processes. Proposed future topic: Advanced Threat Protection (ATP) or insider threats, understanding vulnerabilities.

Many tools cannot specifically and thoroughly determine the environment. Can the antivirus be a means to attack a system? It is accepted that antivirus should be used, but there are quibbles about it (such as use of antivirus on Mac systems). In addition, programs with privileged access to systems can be vehicles for attacks.

Panel Discussion on "Open Source trustworthy software supply chain"
Dr. Kevin Fu, (Moderator), Associate Professor, University of Michigan
Mike Ahmadi, Global Director, Critical Systems Security, Codenomicon (PPT Presentation provided)
Brian Fitzgerald, Deputy Director, Deputy Director, Division of Electrical and Software Engineering, FDA CDRH OSEL
Billy Rios, Founder, Laconicly

The panel will be discussing proposals on transparency with respect to vulnerability in commercial products. Mr. Fitzgerald is an expert on medical devices and security. Mr. Rios has worked on security analysis of fusion pumps. Mr. Ahmadi opened discussion for the group with his presentation.

---

47 https://nstic.blogs.govdelivery.com/2015/04/13/a-retrospective-look-nstic-pilots-catalyzing-the-identity-ecosystem/
48 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

Mr. Ahmadi's company, Codenomicon, discovered the Heartbleed[49] vulnerability, and created the well-known logo and website. 2014 was an unusually busy year in the realm of cyber-attacks. 2015 is also busy as recent events have proved. Empirical data needed to prove what appeared to be a trend.

Medical software issues are widespread. Over 1600 vulnerabilities are known to exist in one commonly used monitoring system. Over three hundred of those vulnerabilities were in the Java run-time environment alone. All examples given here are connected systems.

Entries in the NIST CVE database[50] have increased dramatically in the last three years. Heartbleed scored a five on the criticality scale for vulnerabilities. Codenomicon plotted Common Vulnerabilities and Exposures (CVE) stamped timeline, and noted that there was a thousand percent increase in 2013-2014. This demonstrates that the means to get into systems have increased.

Malware attacks on industrial control systems during 2012-2014 show an increase of 2866 percent. This is malware found on controlled systems (source Kapersky Labs). Several major incidents have occurred this spring on government systems (Army, OPM, IRS). This is dealing with malware found on systems. It is not known how many have been exploited. Verizon report states most attacks were 10 CVEs.

New devices are coming on the market. Risks in items such as smart TVs or IP phones are not known. Once in networks, malware can access the entire network as machine-to machine are trusted boundaries. A new version of the bill from the Chairman of the House Committee on Foreign Affairs, Rep Ed Royce, has just been released. Government agencies must include clauses requiring: Confidential buyer list or bill of materials to identify vulnerabilities, provide capability to patches and timely repairs. The Royce bill: Cyber Supply Chain Management and Transparency Act – Key Provisions brings transparency to software procurement, and it is currently working its way through Congress.

NSTIC is building a cybersecurity certification lab. It will be creating a third party certification that gives some level of confidence in the security of the products.

What fraction of products ship with vulnerabilities? About 27% of products across all verticals ship with vulnerabilities. In health systems and control systems, vulnerabilities are rampant.

The process of creating an Underwriters Laboratories (UL) certification is ongoing. GSA, DHS, NSA, DoD are supportive of this idea. Allow companies to make a risk base assessment of vulnerabilities. A UL certification will be available by end of the year.

The software industry has had no compelling reason to fix long standing vulnerabilities. Responsibility has to move down the supply chain. Vulnerabilities can be eliminated, but we need to do a better job of managing them. Software and systems have zero visibility.

Is software industry supportive of the Underwriters Laboratories concept? Software industry is only industry that absolves itself of liability with an End User License Agreement (EULA). EULAs are no longer sufficient and applicable for current use. Companies must assume some liability for security flaws in their software.

Laconicly conducts device research and discovers vulnerabilities that led to conducting variant analysis. There is disincentive for companies to do variant analysis, which is best done by a third party. But impact analysis remains the one challenge, and it should be done by a human being.

---

49 http://heartbleed.com/
50 https://nvd.nist.gov/ https://web.nvd.nist.gov/view/vuln/search

Laconicly is also looking at characterizing software. Antivirus allows exclusions for good software that cannot be distinguished from malware. Work is being done on identifying these types of software using information from manufacturers. It gives credibility to integrators and customers to know for certain that software came from manufacturers. There are three tiers of identification data: uploaded files (not trusted); data from installation; manufacturer data. The data provides an opportunity for the end user to verify directly without having to go to anyone else. A list of identified software is available free now.

Data from the manufacturer is the best source on what is safe code. The panel described a number of sources such as Whitescope is a free service that can identify sources for software in its database. Codenomicon has set up a database for bills of materials on BOMtotal.com that is free and open.

Previous premarket guidance[51] has been made public. They are working toward incentives and disincentives that will be codified eventually. Guidance from 2005 has been used to prevent a large of amount of post market mitigation of emerging threats. Constructed a new model predicated on a highly collaborative information sharing environment. However, there is a segment of people who have been advised that any admission of vulnerability is seriously detrimental to their interests, and they should resist making any admission of that type.

Corporate governance may play into this situation. There is a need to reexamine whether some aspects of medical devices can exist in the free market. It is necessary to find ways to incentivize manufacturers and corporations to not just hire smart people, and organizations with resources and capabilities to establish continuing relationships with manufacturers through to post market. This will help to deal with problems from pre-market stage. FDA's Premarket Notification 510 (k)[52] submission process may play a role. There may never be clean software in the pre-market because there is no way to predict vulnerabilities in the future.

There is a much longer lifespan for medical devices than most consumer devices. Vulnerabilities have not been detected with advance of installation. Lack of transparency impacts more than mainstream programs, it impacts safety. There must be a direct relationship between vulnerability, safety or effectiveness issue before oversight powers can be used. Inertia is a major deterrent to actions to rectify issues in this area.

Security must be seen as essential part of the device question. Lack of security in medical devices cannot be caught in premarket stage unless there is collaboration with the majority of the industry. But not surprisingly, there is a resistance in corporate America. The threat model does not account for the fact that there are bad people out there infecting software. Active adversaries are not part of the model. Threats from cyber-attackers have not incorporated in risk management. Safety and effectiveness issues have not been expressed by users. Authorities can only act on threats to safety and effectiveness.

Businesses do not want to take responsibility for their supply chain due to costs. When the compelling reason to fix these issues is detected, the issues have become too large and expensive. Many small

---

51 See "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Guidance for Industry and Food and Drug Administration Staff," (October 2, 2014), available at http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf; http://www.alston.com/files/Publication/7cd95656-cb69-4ca3-a42b-bc9ccb55564c/Presentation/PublicationAttachment/62f18c0a-2c90-41bd-afb7-c5f63f22fa38/14-818-FDA-Cybersecurity.pdf

52 http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k/

problems have become large, hence inertia wins out. The FDA has tools that allow people to report bad devices or drugs. FDA will work with manufacturers to correct.

Securability in premarket design should be an embedded design for it could become a big problem later. Supply chain management is something that can be accomplished. The General Services Administration (GSA) and specifically the Federal Acquisition Regulations (FAR)[53] can be part of the solution in creating appropriate market pressure.

The Federal Trade Commission (FTC) has taken position that consumers have the right to expect security when privacy policy has stated as much. Can the Food and Drug Administration (FDA) be used as model? Who determines risk? If security flaws exist, the government agency should demonstrate the possibility of harm, whether or not actual harm occurs. Sub-security must be seen in the context of the device in question. It is reasonable to expect that the ecosystem to have an area of discretion to talk to manufacturers regarding cybersecurity. Reporting must occur and there must be an environment of safety for manufacturers to feel they can fix security flaws. FDA is able to do independent analysis and exercise its unilateral recall capability if necessary. Open source at least has information available on software sources.

Board Wrap-up Review and Discussion

The ISPAB is established by statue while other boards are established or utilized by agency/agencies, e.g. VCAT is established by NIST. The board encourages participation in discussions from members of industry. There is a need for transparency and balance, and for the board to constantly solicit the opinion of attendees, guest speakers, and others.

Annie Sokol, DFO, requested the Chair and board to review a change of meeting dates for March 2016. The board has previously approved the meeting dates for 2016 but the US Access Board conference room was unavailable for March 2-4, 2016, and suggested alternative weeks of March 21-25 or March 27-31. The Chair and board unanimously agreed to change the meeting in March 2016 to March 23-25. Ms. Sokol will reconfirm with the representative of US Access and report to the board. The dates for June and October 2016 remained unchanged.

Ms. Sokol will also proceed to begin extension process for Greg Garcia and Toby Levin, and nomination process for new member.

The Chair noted that the board had not been active in drafting recommendation letter(s). The last recommendation letter was submitted in November 2014. The ISPAB is required to renew its charter early next year. Furthermore, fiscal year report is due in September, and it is critical for ISPAB to demonstrate relevancy and progress.

Board's Review discussions/sessions on Wednesday, June 10, 2015:

1.1 Information Technology Lab (ITL) Realignment and Proposed Applied Cybersecurity Division

Heartily endorse the proposed realignment of ITL to add another division. CSD has been growing organically, including new funding for import work on cryptography. Several other computer projects have matured. Realignment gives old and new work nice support for continued success. All were in favor and the motion passed.

53 https://www.acquisition.gov/?q=browsefar

1.2 National Initiative for Cybersecurity Education (NICE) Updates

The initiative needs traction such as additional funding or new ideas, although NICE received funding this year for the first time from DHS.

It is noted that cybersecurity has to compete with other course requirements for college students. It should be integrated into computer science majors. NSF is working through scholarship program to encourage security curriculum through internships and public service by students. The Federal government can incentivize creation of cybersecurity curriculums in colleges and universities. On the consumer side, develop awareness programs. "Stop, Think, Connect"campaign is an example.

Action: No action recommended by the board.

1.3 Executive Order 13694 Block the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities

Action: No action recommended by the board.

1.4 IG Reporting on FISMA

Forward progress has been made, but it is not clear to the board that we are gaining on the threat. The board questioned as to how long it will take to examine all security areas. It seems that while one question was answered, but others are out there, and new ones are coming.

***Action**: The Board is to consider drafting a letter in October meeting for strengthening measurement and evaluation of cyber norms. Also, to express concern that while progress is being made, on its effectiveness*

1.5 Vehicle Infrastructure (auto manufacturer communication and usability): Discussion on Data Security and Privacy

The Board would like to include a future meeting with NHTSA and FHWA on automated vehicles.

Board's Review discussions/sessions on Thursday, June 11, 2015:

2.1 NIST Crypto Standards and Adoptions
Quantum Cybersecurity

It is necessary to ensure US libraries are understood and accepted. The board discussed on involvement in international standards, and pros and cons for developing NIST standards in international arena. Standards are about national priorities, standards, trade etc. It is noted that work on quantum computers and cryptography are still in preliminary stage.

Action: No action recommended by the board.

2.2 Data Breach and Supply Chain Security

The board requested for a follow-up presentation with the US Department of Defense (DoD) to discuss its supply chain program on counterfeits.

2.3 Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, A Proposed Rule by the Industry and Security Bureau

The Federal Register notice is really "after the fact" announcement based on decision made previously. The language discussed in the presentation is already in effect and the agreement is pretty restrictive. Any company that monitors its networks would be concerned about the language. The board is concerned that when people evaluate performance, there will be differing interpretations. The intention is deemed as too restrictive for companies to defend themselves while operating internationally. The board discussed on possible fix such as recommending an exception. There is a need to seek a binding interpretation of the language now. The public comment period on the agreement closed on July 20.

- Topic for the group to consider now: Whose work would a letter possibly reinforce?
- Future Topic: discuss consequences
- Main question is to consider the extent that the government is capable of tracking progress and not keeping up with changing threats.
- Draft recommendation letter: BIS should have knowledge of security provided by the CISO. BIS should identify risks for IT people for sensitive information.

Actions: The board approved the motion to draft a recommendation letter to NIST Director

2.4 The Communications Security, Reliability, and Interoperability Council (CSRIC) Report on Cybersecurity Framework

The board had no comment or action for this presentation.

2.5 Updates on NTIA Cybersecurity Request for Comment (RFC) Stakeholder Engagement on Cybersecurity in the Digital Ecosystem

NTIA was reviewing the comments and was able to provide specifics at this point. The board will like to revisit this discussion at future meeting.

Action: See above.

2.6 Updates on OMB Circular No. A-130 Revised

Update on A-130 is Important work, but it is not finished.

Action: Invite Carole Bales back for discussion following completion of the circular (Spring 2016).

2.7 NIST Computer Security Division Updates

The board had no comment or action for this presentation.

Board's Review discussions/sessions on Friday, June 12, 2015:

3.1 NIST Strategic Directions and Plans

The board was appreciative of Dr. Cavanagh's good presentation on NIST.

3.2 CTO's Priorities

The board remarked that the presentation provided an optimistic view of their work.

3.3 Updates on National Strategy for Trusted Identities in Cyberspace (NSTIC)

The board had no comment or action for this presentation.

3.4 Public Participation Period

The board had no comment or action for this presentation.

3.5 Panel Discussion on "Open Source Trustworthy Software Supply Chain"

The board had no comment or action for this presentation.

Board discussion on future meeting topics:

- Phyllis Schneck, Deputy Under Secretary for Cybersecurity and Communications, US Department of Homeland Security, National Protection and Programs Directorate
- Reschedule the discussion from DOJ and FBI on information collection, Going Dark Initiative – Overview, Challenges and Gaps
- PCLOB/David Medine: updates on EO 12333 as continuation to the discussion on Section 702 from 2014
- Invite NHTSA and FHWA on automated vehicles
- Follow up on the latest breaches – Presenters: not determined
- Automated information sharing, ISAO and ISAC processes
- Open data initiative
- Commercial off-the-shelf (COTS) for classified use
- Identity management and knowledge based authentication
- Government adoption of internet of things
- Government use of tools to make code better (tech and tech transfer);
- Anti-counterfeit and clone efforts
- Advanced Threat Protection and insider threats
- Strengthening measurement and evaluation of cyber norms (US Department of State)
- Use of internet for 2020 census – test plan, privacy and security precautions (Census)
- GAO Report on smart cards (getting rid of SSN numbers currently in use) (GAO)
- Dr. Kevin Fu
- Identity Management (KBA)
- Work on CPS and use in government agencies (potential standards, etc.)
- Light weight cryptographic issues (medical, auto, security and privacy issues)
- US Department of Defense (DoD) to discuss its supply chain program on counterfeits

Action to be completed in October 2015:

Suggest consideration of letter on medical device security for the October meeting.

Propose discussion of sending letter commenting on guidance from FDA on premarket security at the October meeting.

The meeting adjourned at 12:38 P.M., Friday, June 12, 2015.

ANNEX A

List of Participants

Last Name	First Name	Affiliation	Role
Ahmadi	Mike	Codenomicon	Presenter
Archer	Jerry	SallieMae	Presenter
Baker	Brett	National Science Foundation	Presenter
Bales	Carol	OMB	Presenter
Cavanagh	Richard	NIST	Presenter
Chen	Lily	CSD, ITL, NIST	Presenter
Chenok	Dan	IBM	Presenter
Dodson	Donna	NIST	Presenter
Echols	Michael	U.S. Department of Homeland Security (DHS)	Presenter
Fitzgerald	Brian	FDA CDRH OSHL	Presenter
Friedman	Allan	National Telecommunications and Information Administration	Presenter
Gacki	Andrea	U.S. Department of Treasury	Presenter
Garcia	Michael	NSTIC, NIST	Presenter
Kurtz	Paul	TruStar	Presenter
Lacher	Andrew	Mitre	Presenter
Lesser	Nathan	ITL, NIST	Presenter
Macgillivray	Alex	The White House	Presenter
Manson	Antione	DHS	Presenter
Mayer	Robert H.	USTelecom	Presenter
McBride	Tim	ITL, NIST	Presenter
Megas	Katerina	ITL, NIST	Presenter
O'Toole	Brian	U.S. Department of Treasury	Presenter
Petersen	Rodney	ITL, NIST	Presenter
Rarog	Bob	U.S. Department of Commerce	Presenter
Remaley	Evelyn	NTIA	Presenter
Rios	Brian	Laconicly	Presenter
Ross	Ron	CSD, ITL, NIST	Presenter
Sheridan	Peter J.	Federal Reserve Board	Presenter
Barrios	Brian	Mitre	Visitor
Brooks	Sean	NSTIC, NIST	Visitor
Brown	Evelyn	NIST	Visitor
Denaro	James	CipherLaw	Visitor
Durbin	Ken	Symantec	Visitor
Jacobucci	Erin	Strooch & Shrooch & Lavan LLP	Visitor
Kerban	Jason	US Department of State	Visitor

Last Name	First Name	Affiliation	Role
Magri	Josh	FSR / BITS	Visitor
Romine	Charles	NIST	Visitor
Schmidt	Amelia	Strooch & Shrooch & Lavan LLP	Visitor
Sedgewick	Adam	NIST	Visitor
Stine	Kevin	NIST	Visitor
Thomson	Jay	NCCoE	Visitor
White	Nathan	Access	Visitor
Curran	John	Telecom Reports	Visitor / Media
Higgin	Joshua	Inside Cybersecurity	Visitor / Media
Mitnick	Drew	Access	Visitor / Media
Otto	Greg	FedScoop	Visitor / Media
Pereira	David	Politico	Visitor / Media

ANNEX B

Public Participation Statement, Friday, June 12, 2015

As submitted by:
Ken Durbin
Unified Security Practice Manager
Public Sector, Symantec

First, I would like to compliment the Board on the quality of the briefings conducted over the last couple of days. I found them to be very relevant to my area of responsibility as an IT professional, but also as a private citizen. I particularly like how the Board doesn't hesitate to interrupt and ask the tough question of a presenter, no matter who they are, or represent, to keep the information relevant.

I would like to address a topic brought up in yesterday's session titled "Data Breach and Supply Chain Security." Before I do I want to say that I really enjoyed the topic, and the quality of the presenters.

One of the panelists talked about vulnerabilities, and the classic battle between the Auditors and the IT Department. IT ranks vulnerabilities so they can patch those deemed "critical" and not spend resources on the remaining "trivial" vulnerabilities. The Auditors, of course, only focus on the unpatched "trivial" vulnerabilities. It's the "trivial" vulnerability I would like to discuss.

In all fairness, I'm sure the presenter did not mean "trivial" in its lightest sense. I'm confident he meant that when ranking the vulnerabilities, a "risk based decision" was made to not spend the resources to patch them. That's a perfectly acceptable way to rank vulnerabilities.

However, the vast majority of successful attacks depend on the target having an asset that is miss-configured, or has an unpatched vulnerability they can exploit. Even with a Risk Based Decision approach, given the sophistication of today's advisory, is it still acceptable to decide to not patch a known vulnerability? I ask the question without having an answer of my own. I'd like to propose that the Board consider this question as a possible topic for its next meeting.

Thank you for your time and attention.