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

October 21, 22, and 23, 2015

U.S. Access Board
1331 F Street N.W., Suite 800, Washington, DC 20004, 20850
Agenda http://csrc.nist.gov/groups/SMA/ispab/documents/agenda/2015_agenda-ispab-october-meeting.pdf
ISPAB homepage http://csrc.nist.gov/groups/SMA/ispab/index.html

Board Members	Board Secretariat and NIST staff
Dr. Peter Weinberger, Chair, ISPAB, Google Chris Boyer, AT&T John R. Centafont, NSA Dave Cullinane, TruSTAR Technologies (joined via phone) Dr. Kevin Fu, University of Michigan Greg Garcia, McBee Strategics Consulting Toby Levin Edward Roback, US Department of Treasury **Absent with Regrets:** Gale Stone, Social Security Administration J. Daniel Toler, US Department of Homeland Security	Matt Scholl, NIST Annie Sokol, DFO, NIST Robin Drake, Exeter Government Services, LLC Priscilla Harvey, Exeter Government Services, LLC Tatiana Laszczak, Exeter Government Services, LLC

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

Wednesday, October 21, 2015

Welcome and Remarks

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

The ISPAB Chair, Dr. Peter Weinberger called the meeting to order at 8:42 a.m. He noted that the Board did not have the required quorum of seven board members present. The Chair welcomed the board members and commented about the great agenda. Mr. Scholl introduced Jeff Greene, Esq. from Symantec who will be receiving the appointment letter signed by NIST Director any day. Also receiving appointment day and joining as a new member at next ISPAB meeting in March 2016 is Dr. Annie Antón from Georgia Institute of Technology.

NIST and National Security Agency (NSA) Future Plans for Quantum Resistant Cryptography

Vincent M. Boyle, NSA
Lily Chen, Ph.D., Acting Group Manager, Computer Security Division, ITL, NIST (PPT presentation provided[1])
Adrian Stanger, Ph.D., NSA (PPT Presentation provided[2])

The Chair welcomed presenters Vincent M. Boyle, NSA; Lily Chen, Ph.D., Acting Group Manager, Computer Security Division, ITL, NIST; and Adrian Stanger, Ph.D.,. He referenced the NSA[3] announcement in August 2015 on quantum computers, which sparked request from the board to hear from NSA and NIST on their plans for quantum resistant cryptography.

Dr. Stanger explained that the main incentive for the announcement was due to the threat of the cryptographically relevant quantum computer. The effect of developing the quantum computer is that it would attack all public key cryptography and will have a major impact on security on everything from military, government traffic, internet, and commerce. NSA is concerned about retaining data security as it impacts their partners right now, although the launch date of the quantum computer is unknown and possibly will never be developed. The announcement was also abruptly made owing to a mandate for NSA to transition to strictly elliptic curve protocols for public key cryptography in October 2015. NSA felt an obligation to make the announcement prior to the October deadline and because some of their partners would conscientiously move forward with the transition on their own.

One of NSA's goals for interoperability is to have one cryptographic suite, instead of separate suites for secret and top secret levels. In the future of public key cryptography, there will be some quantum resistant standards that everyone should follow. The NSA does not plan to put out its own algorithm but plans to work with academia and private sector vendors to develop the algorithm in a concerted effort with NIST.

NSA resisted on mandating people to switch to elliptic curve cryptography because the transition to quantum resistant cryptography was forthcoming. Therefore, they allowed people to continue on RSA and Diffie-Hellman, and increased the key size to maintain security for a longer period of time. Some exceptions will call for shared symmetric keys to be used due to an absence of recommended standards. NSA's main concern is that encrypted government data will be vulnerable if and when a quantum computer is launched.

Dr. Chen highlighted NIST's plan to publish a NIST Interagency Report (NISTIR) in FY 2016, which will provide information to government agencies and industry on the "upcoming" migration to quantum resistant cryptography. The NISTIR will summarize the major results and progress in the topic area and discuss challenges and potential issues in the migration. Its goal is to prepare the user community by constantly providing updates. The major challenge is that NSA does not know when Quantum (Q) Day will happen, which presents a challenge to the preparation for Q Day as people may lose the urgency to deploy stronger cryptography at this time.

[1] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-10/oct21_chen_nist%20cryptography.pdf
[2] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-10/oct21_stanger_final_approved_nsa.pdf
[3] https://www.nsa.gov/ia/programs/suiteb_cryptography/

NIST is working to analyze the existing Public Quantum Cryptography schemes through research funding, collaboration, workshops and by growing the NIST research team. NIST is collaborating with the research community on security analysis and performance data. NIST is also working with industry to determine the practical impact on each specific implementation and trying to understand government needs. With collaboration with standard bodies using "drop-in" case studies, e.g. hash-based signature for code signing in Trusted Computing (TCG), Transport Layer Security (TLS), and cipher-suite with post-quantum schemes in Internet Engineering Task Force (IETF), etc. NIST is further working with the international community for general acceptance of Product Quality Characteristic (PQC) standards.

Mr. Boyle indicated that authentication will require stronger algorithms for confidentiality. Certificate chains and the Internet of Things (IoT) will also need to be quantum resistant. The block chain effect on symmetric key and hashes will exist, but with a smaller impact. The Chair noted that the early uses of public key had many algorithms that were not truly secure and suggested there may be a need for several algorithms. Dr. Chen agreed and stated that improvements will be made over time and that a quantum resistant algorithm will expand over time. Mr. Boyle noted that multiple key algorithms and standards will possibly be adopted in 7-10 years.

Federal Government Cybersecurity: The 30-day Cybersecurity Sprint[4] and the Marathon to Come

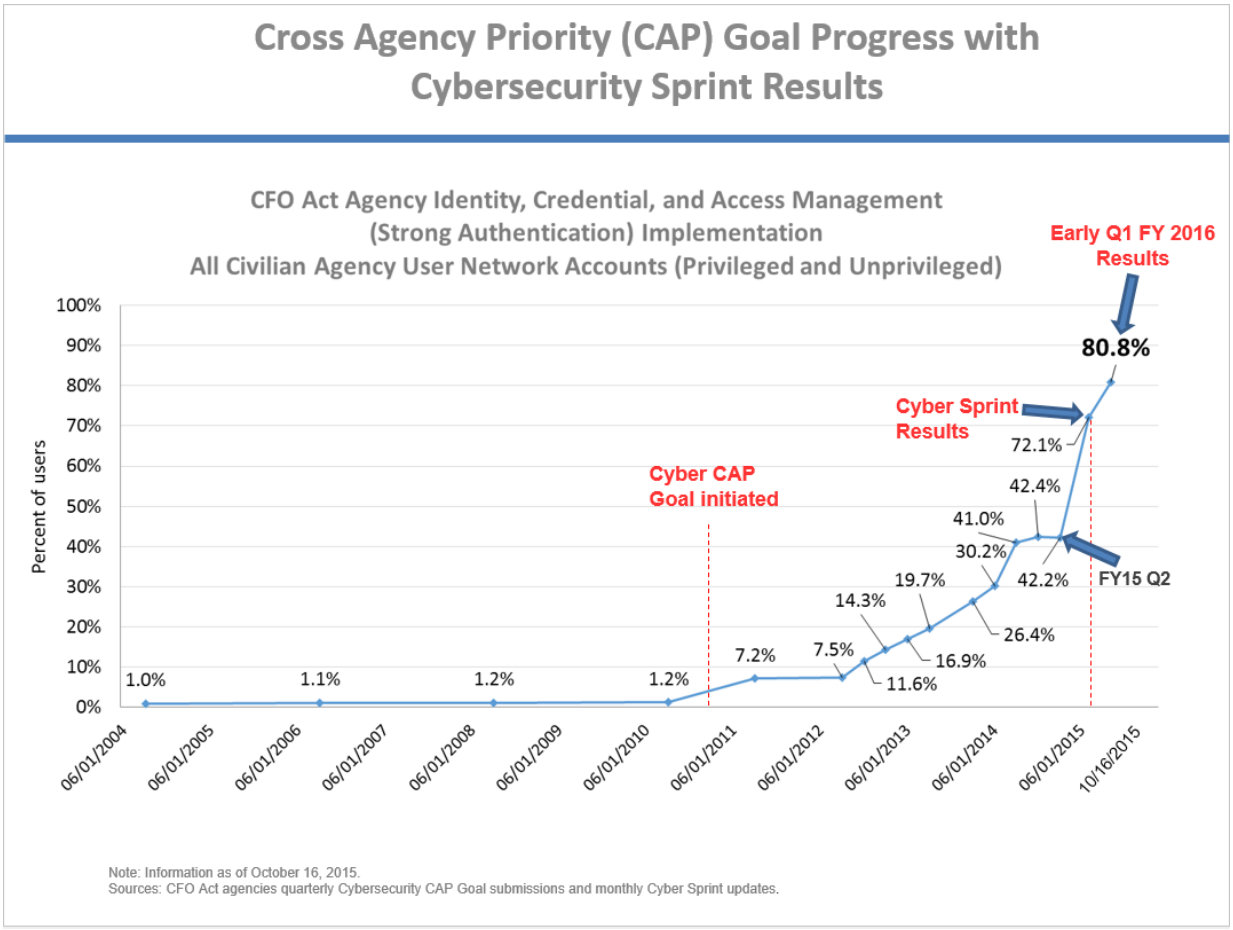
Chris DeRusha, Senior Analyst, Cyber and National Security Unit, Office of Management and Budget (OMB) (PPT Presentation provided)

The Chair welcomed presenter Mr. Chris DeRusha, OMB, to the meeting. Mr. DeRusha began by citing the OMB cybersecurity and national security unit was formally created in February 2015 due in large measure to an increased need for greater capacity to accommodate emerging cybersecurity challenges. He noted that Circular No. A-130 Revised [5] [6] [7] - Managing Information as a Strategic Resource was released on October 21, with a 30-day[8] public comment period, and it would be most appropriate for Carol Bales, the lead on the Circular A-130 effort, to speak to the Board at first meeting 2016. The Chair commented on the rationality of the OMB cybersecurity office's vision and mission.

Mr. DeRusha provided information on CyberStat Review Sessions (CyberStats),[9] a joint effort between OMB and DHS in which they work with agencies to review their cybersecurity posture in order to identify gaps and develop strategies to improve performance. They completed 14 CyberStats in FY2015,

[4] https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/enhancing-strengthening-federal-government-cybersecurity.pdf
[5] https://ombegov.github.io/a130/Proposed%20A-130%20for%20Public%20Comment.pdf
[6] https://a130.cio.gov/
[7] https://www.whitehouse.gov/omb/circulars_a130_a130trans4/
[8] The public feedback period has been extended by 15 days ending on December 15
[9] See M-16-03 Fiscal year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf ...CyberStats are evidence-based meetings led by OMB to ensure agencies are accountable for their cybersecurity posture, while at the same time assisting them in developing targeted, tactical actions to deliver desired results.

which was double the number completed in FY2014. The number of CyberStats completed in FY2016 may not double again, they will continue to be aggressive in their approach to assist as many agencies, departments and programs as possible. They have been able to baseline many of the agencies and are now developing new program models to target specific areas of focus.



Federal Information Security Modernization Act of 2014 (FISMA)[10] prompted a number of new requirements for the OMB Cybersecurity Office. Their office will be releasing some updated guidance soon, concurrently with an update on the Cybersecurity Communication Plan and Strategy. He also mentioned the DHS Binding Operational Directive [*A Binding Operational Directive is a direction to agencies to mitigate a risk to their information systems*] on Critical Vulnerabilities, a new tool issued by Secretary of Homeland Security Jeh Charles Johnson[11] in May 2015 as a result of FISMA. The directive is binding and a statute that focuses on level 10 vulnerabilities as provided by the Common Vulnerability Scoring System (CVSS). The CVSS provides an open framework for communicating characteristics and impacts of IT vulnerabilities and helps organizations prioritize and organize their response to vulnerabilities. The work has received major attention at the senior level at several agencies and Secretary Johnson has been conducting a high level of engagement on the initiative.

[10] https://www.congress.gov/113/bills/s2521/BILLS-113s2521enr.pdf
[11] http://www.dhs.gov/news/2015/07/08/remarks-secretary-homeland-security-jeh-charles-johnson-securing-gov

United States Chief Information Officer (CIO) Tony Scott recently launched a 30-day Cybersecurity Sprint[12] in order to fast track a series of high priority cybersecurity areas. The effort consisted of convening a large working group and sub-working groups to determine what gaps needed to be addressed. It focused on implementing five high priority actions including immediately deploying Indicators of Compromise (IOCs), tightening policies and practices for privileged users, implementing Personal Identity Verification (PIV) cards for network access especially for privileged users, and identifying high value assets and reviewing corresponding security protections. It also focused on targeted indicators that were apart of recent security breaches.

Another high priority area for them is implementing strong authentication processes for all civilian agency user network accounts and referenced a table that highlighted results of the sprint in this area. He noted their next step is to release the Cybersecurity Strategy and Implementation Plan[13] (CSIP), which is an action plan that highlights the tasks that can be implemented immediately and within the next 6-12 months to close policy and capability gaps identified during the sprint.

The CSIP is organized around five areas and is based on the NIST Framework for Improving Critical Infrastructure Cybersecurity.[14] The five areas include: prioritizing identification and protection of high-value information, timely detection and rapid response to cyber threats, rapid recovery from incidents when they occur and accelerated adoption of lessons learned from these events, recruitment and retention of the most highly-qualified cybersecurity workforce talent the Federal government can bring to bear, and efficient and effective acquisition and deployment of existing and emerging technology.

CSIP is focused on the Federal Civilian Government, that is, the"<dot>gov", and not "<dot>mil" domain. Mr. Garcia indicated there is a lack of security uniformity as it applies to supply chain management across the government and suggested that their last goal statement should state efficient, effective and accurate acquisition. Mr. DeRusha reiterated that the CSIP will focus on tasks that they can do now to connect resources and to make issues clearer to agencies in order to pave the way for new initiatives. Personnel at the secretary- level will provide quarterly updates and they will conduct agency specific outreach and engage with CIOs and CISOs to implement the plan.

In response to the Chair's question on determining which tasks cannot be completed due to budget constraints, Mr. DeRusha indicated that he is not privy to budget details; however, because everyone is aware of the sense of urgency of the high priority tasks, they are committed to accomplishing all of the goals. Mr. DeRusha closed by noting the upcoming policies including the CSIP, FY 2016 FISMA Guidance, Improving Cybersecurity Protections in Federal Acquisitions and Circular No. A-130 Revised. He encouraged the board to review the documents, provide input and participate in events as they unfold. Mr. DeRusha offered to provide further updates upon request.

[12] https://www.whitehouse.gov/blog/2015/06/17/fact-sheet-enhancing-and-strengthening-federal-government-s-cybersecurity
[13] See M-16-04 Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf
[14] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, http://www.nist.gov/cyberframework/

U.S. Department of Homeland Security-National Protection and Programs Directorate

Phyllis Schneck, Ph.D., Deputy Under Secretary, Cybersecurity and Communications, National Protection & Programs Directorate, US Department of Homeland Security

The Chair welcomed presenter Dr. Phyllis Schneck, to the board. Dr. Schneck thanked the board for inviting her to provide insight into DHS and that cybersecurity spans the whole department from the secret service and Federal Emergency Management Agency (FEMA) to homeland security investigations, with connections to many agencies and facilities. They do not consider cybersecurity as simply blocking attacks and sharing information. The National Protection and Programs Directorate (NPPD) within the infrastructure protection, works with FEMA and works with National Network of Fusion Centers,[15] which coordinates regional cybersecurity.

NPPD has policy, law enforcement and response components and is to realign resources to re-infuse the infrastructure protection effort with the cyber energy resources available. Within the NPPD is the Federal Protective Service (FPS), which guards all Federal buildings and monitors Federal HVAC[16] systems against potential infiltration and hacking into IT through the HVAC system.

The Chair commented that the Federal government seems to be spending more on physical security as compared to the private sector. Dr. Schneck responded that she does not know the amounts of money spent; however, she mentioned there are a lot of behind the scenes logistics involved in order to protect privacy and civil liberties. One of DHS's top priorities is to build trust with its Federal partners and with the private sector. The agency wants to foster relationships so that partners are comfortable with sharing information and with seeking assistance from DHS. The motto, "see something, say something" is applicable for people and for machines. The agency participates in numerous events and responds to requests for help which are carefully documented.

She provided an overview of DHS Einstein system,[17] an intrusion detection system (IDS) for monitoring and analyzing Internet traffic as it moves in and out of United States federal government networks. The system collects netflow data, detects attacks and blocks insurgents by recognizing activity based on things they have seen before. Einstein also provides situational awareness of the kinds of traffic that are trying to attack the Federal government, and the outbound connections agencies are tracking which potentially pose a threat. They are building their technology to be more biologically focused and leverage data collection of cyber threat indicators to get beyond signature technology.

Dr. Schneck mentioned the Continuous Diagnostics and Mitigation (CDM),[18] which examines how to protect the inside of the network and provides the best tools available in the private sector to Federal civilian agencies. The Chair inquired about whether the agencies are capable of putting these CDM tools into effect and using them effectively. Dr. Schneck believed that the agencies are capable, but assistance is provided as agencies may be under-resourced; however, they are unable to mandate that the agencies to use the tools. The Chair commented that dealing with the intrusion in malware requires ongoing attention and flexibility and is not clear how acquiring product is sufficient. While the presenter

[15] http://www.dhs.gov/national-network-fusion-centers-fact-sheet
[16] Heating, ventilation, and air conditioning
[17] http://www.dhs.gov/einstein
[18] http://www.dhs.gov/cdm

agreed, it is unrealistic to set a bar that could over-tax the agencies. The intent is to provide a resource to the agencies so that they can spend their time focused on their jobs and not finding solutions.

Dr. Schneck stated DHS desires to be open, and to welcome information about solutions available from the private sector. They are opening a Silicon Valley office to be more accessible, but their priorities are to push out as many capabilities as they can, to hire and place their people on site quickly, to work with interagency partners, and to support resiliency of the private sector. Acquisition has continued to be a challenge; however, they are pushing to achieve these goals.

Presentation from National Highway Traffic Safety Administration (NHSTA) (PPT Presentation provided)[19]

Cem Hatipoglu, Ph.D., Division Chief, Electronic Systems Research (NVS-3333), NHSTA
Nathaniel Beuse, Associate Administrator, Vehicle Safety Research, NHSTA

The Chair welcomed presenters Nathaniel Beuse and Cem Hatipoglu from NHSTA. In opening, Mr. Hattipoglu raised the fact that there are still many fatalities on the road today. Technology has helped immensely but many cyber physical challenges remain. New safety features and customer convenience features have introduced new challenges and vulnerabilities. While no real world incidents have occurred to critical safety systems, NHSTA has developed a research approach to help improve the safety posture of future vehicles. Technologies have prevented real world incidents but NHTSA is trying to balance technology with safety.

In January 2016, NHSTA will host a cyber roundtable with industry and government to develop best practices, and hopefully by June 2016, the industry to develop a draft outline of best practices. Ms. Levin suggested that the NHSTA's goal should not be looked at as finding a balanced approach but more of trying to provide safety while providing information security.

The auto industry has adopted a denial factor that safety risks exist. Past studies have affirmed and results from future studies will help to persuade the industry. The large industries are accustomed to regulation, the Chair offered, and without appropriate regulation they tend to become disorganized.

NHSTA's top priority is safety. Its mission is to reduce fatalities, injuries and economic losses resulting from motor vehicle crashes. Motor vehicles are defined as the equipment side of anything that can be used as a vehicle or plugged into the vehicle. Every automobile has a different architectural structure, and there is continuing work to understand those complexities. NHSTA is focused on new vehicles and is not authorized to regulate what private citizens do with their vehicles. The US Environmental Protection Agency (EPA) has authority to cite private citizens for emissions-related issues.

Federal Motor Vehicle Safety Standards (FMVSSs) stipulate mandatory requirements, and the Motor Vehicle Safety Act gives the NHTSA the authority to issue vehicle safety standards and to require manufacturers to recall vehicles that safety-related defects or do not meet Federal safety standards. FMVSSs are performance-based and appropriate for each applicable vehicle type. NHSTA enforces the FMVSSs by investigating possible safety defects, ensuring that products meet established safety

[19] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-10/oct21_hatipoglu_cyber%20nhtsa.pdf

standards, are not defective, and monitor the manufacturer's corrective action to ensure successful completion of recalls. The agency also enforces regulations on fuel economy, odometer fraud, and vehicle theft.

In addition to regulation, the NHSTA also provides consumer information and creates incentives for manufacturers to provide information on new safety technologies. They rate the performance of vehicles on different aspects of safety and conduct most of the testing which follows an objective/performance based style of an FMVSS.

NHTSA also studies behaviors and attitudes in highway safety, focusing on drivers, passengers, pedestrians, bicyclists and motorcyclists. In collaboration with state programs and other partners, the NTHSA identifies and evaluates behaviors of those involved in crashes or associated with injuries, develops and refines countermeasures to deter unsafe behaviors, and to promote safe alternatives in collaboration with state programs and other partners.

NHTSA is developing standards for Selective Ride Control (SRC) and vehicle communication. They investigated the demonstration of two hackers to develop a tool that can hijack vehicles. Over-the-air updates do not have best practice standards, which are being developed. Companies are required to comply with information requests made by the agency. Research is ongoing in various areas and NHTSA is working with DHS, NIST, FAA and other partners to research and evaluate design processes and standards, investigate protective/preventive solutions, research intrusion detection solutions, assess treatment solutions and conduct crosscutting research on vulnerability testing, software, including over-the-air updates, and evaluating heavy vehicle cybersecurity.

Discussion on Due Diligence on Cybersecurity, Standards and Compliance

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

The Chair welcomed presenter, Karen Jagielski, Federal Trade Commission (FTC). Ms. Jagielski summarized FTC jurisdiction and it operates within that jurisdiction. FTC enforces the FTC Act,[20] which prohibits unfair practices of competition, and unfair or deceptive acts or practices in, or affecting commerce. An unfair or deceptive act causes or is likely to cause substantial consumer injury not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or competition.

The agency focuses on commercial practices. Regarding cybersecurity, the FTC enforces the FTC Act; the Children's Online Protection Act (COPA) which governs how websites collect, use or share information about children under the age of 13; and the Gramm-Leach-Bliley Act, which requires financial institutions to explain their information sharing practices to their customers and to safeguard sensitive data. On several occasions the commission has gone to Congress to pass legislation giving the agency more authority to set data security standards. The FTC also provides consumer education by providing information to businesses and consumers on data security.

[20] https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act

The FTC developed a brochure, "*Start with Security: A Guide for Business*",[21] which provides guidance to companies on how to achieve reasonable security measures. In addition, they are working to oppose a bill calling for the privacy rule for any personal information collected by automobile dealers. The bill also mandates that privacy breaches constitute a criminal offense and calls for the enactment of an advisory security board opposed by the FTC.

To date, the FTC has issued over 50 data security cases. Wyndham Worldwide Hotels[22] was one of the first to be litigated on data security. Wyndham initially argued a defense that the FTC did not provide fair notice of oversight practices but their claim was denied. The FTC looks at what is reasonable and there is not a "one size fits all" data security model. They look at each specific company and consider the nature of the business, sensitivity of the data, amount of data being collected and readily available tools to make the information secure. The FTC looks at industry practices and follows the Gramm-Leach-Bliley Act, PCI, and other general principles, but needs to have flexibility in order adjust to market changes.

With regards to the Chair's question on FTC interactions with regulators for financial institutions, the FTC does not have jurisdiction over financial institutions including banks, insurance companies and common carriers such as cell phones. However, the law allows them to prosecute actions by those institutions originating from mobile apps.

The FTC has been asking Congress unsuccessfully to pass general privacy legislation, create uniform standards and make technology neutral since the 1990s. The FTC staff consists mainly of lawyers, and not scientists. They have added technology staff to look at security. However, they rely heavily on their sister agencies to set security standards.

Technology should be built with security in mind from the beginning. In order to promote this initiative, the FTC hosts a series of "Start with Security" events, with a goal to provide companies with practical tips and strategies for implementing effective data security. These events are aimed at start-ups and developers and to bring together experts to provide information on security by design, common security vulnerabilities, strategies for secure development, and vulnerability response. "Start with Security" is based on Fair Information Practices (FIPS). The next event is scheduled to be held on November 5, 2015 in Austin, TX. The FTC also has created a one-stop shop and publishes regular blog posts to provide information, resources and updates on their initiatives.

Presentation of reports from U.S. Government Accountability Office (GAO)

Alicia Puente Cackley, Director, Financial Markets and Community Investment, GAO
Kathleen King, Director, Health Care, GAO
Heather Krause, Acting Director, Strategic Issues, GAO
Alison Snyder, Senior Analyst, Physical Infrastructure, GAO (PPT Presentation provided)

The Chair welcomed the presenters from the U.S. Government Accountability Office (GAO). Ms. King began her presentation on GAO-15-319 Potential Uses of Electronically Readable Cards for Beneficiaries

[21] https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business
[22] https://iapp.org/news/a/is-your-business-ready-for-ftc-oversight-of-data-security/

and Providers[23] with a brief overview of Medicare that serves 54 million people and has expenditures in excess of 600 billion dollars. One of GAO's areas of focus is transitioning to electronic cards for Medicare. Currently, Medicare uses paper cards which include the social security numbers of beneficiaries. In the past, GAO has produced report to obtain authorization to remove social security numbers from cards. Congress recently mandated the effort, and provided funding to support the initiative. The effort will span several years and cost hundreds of millions of dollars because social security numbers are utilized throughout all systems as identifiers and will be challenging to change. GAO has begun the process of transitioning to electronic cards by evaluating four areas: functions and features, potential benefits and limitations, steps that Centers for Medicare and Medicaid Services (CMS) and medical providers would need to take to implement the cards, and lessons learned from other countries including France and Germany.

GAO also researched three different types of electronic cards including barcode, magnetic stripe, and smart cards. They evaluated each card type's ability to authenticate providers and beneficiaries at the point of care, electronically exchange medical information, and electronically convey identity and insurance information. GAO discovered the smart card can provide more rigorous authentication because it is difficult to counterfeit, and assures that information is not altered through its PKI encryption and decryption technology. Smart Cards also have more storage capacity for storing medical records. All three card types have authentication features such as PIN number or biometric capabilities and could be used to convey identity and insurance information. Use of electronic cards can reduce errors and improve medical recordkeeping. In a report completed by GAO, it is noted that they were unable to determine if the use of electronic cards to authenticate providers and beneficiaries will reduce fraud. It could introduce new types of fraud into the system if people hack into the system and introduce malicious software.

The report also identifies one major implementation challenge that CMS must update its antiquated and complex IT systems for electronic card authentication. The systems may not require updates to electronically exchange information and provide identity and insurance information. Providers would also incur costs and face additional challenges in updating their IT systems. The report provided an overview of the electronic card options but did not provide a recommendation.

Ms. King mentioned that France and Germany were chosen for the case study because of their population size and close proximity to each other. Both countries implemented the use of electronic cards for the cost savings benefit of transitioning from paper to electronic records. However, they are now slowly transitioning towards utilization of smart cards for medical records storage capabilities. Unlike the United States, France and Germany are not concerned with the fraudulent misuse of electronic cards. Ms. Levin inquired if GAO would consider issuing cards that do not contain social security numbers while awaiting the implementation of electronic cards. Ms. King stated that Congress has directed CMS to issue cards with unique identifiers not associated with social security numbers and provided 300 million dollars to complete the project within four years.

Ms. Puente Cackley presented on the report: GAO-15-621[24]: Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law – an overview of the use of facial recognition technology,

[23] http://www.gao.gov/products/GAO-15-319
[24] http://www.gao.gov/products/GAO-15-621

a biometric technology used to identify individuals when measuring and analyzing physiological and behavioral characteristics. The U.S. Senate requested two separate reports from GAO, one on the use of facial recognition technology in the commercial sector, and another to provide insight into the FBI's use of facial recognition technology. The latter report will be released in 2016. The commercial sector report was released in July 2015 and examined the following: 1) uses of facial recognition technology, (2) privacy issues that have been raised, (3) proposed best practices and industry privacy policies, and, (4) potentially applicable privacy protections under Federal law.

One major concern regarding facial recognition technology is that it gives businesses and individuals the ability to identify almost anyone in public without their knowledge or consent. In addition, it can track people's location and collect information that can be used, shared and sold in ways that consumers do not consent to or understand. Government, industry and privacy groups are in the process of developing best practices.

Companies were selected because they were among the largest in the industries identified as potential major users of the technology, and privacy groups were selected because they had written on this issue. Currently, there is no Federal privacy law which expressly regulates commercial uses of facial recognition technology, and laws currently in place do not fully address key privacy issues raised by stakeholders such as defining the circumstances where the technology may be used to identify individuals, and storing personal information.

The FTC can investigate companies that use the technology to obtain financial information for deceptive practices. A multi-stakeholder group met in July 2015 but some of the stakeholders pulled out because they didn't think that the process would result in a strong set of best practices. The group continues, despite being less robust than when first started. The report did not provide recommendations; however, the GAO suggested that Congress consider strengthening the consumer privacy framework to reflect changes in technology and in the marketplace.

Ms. Krause presented on the report: GAO-15-608[25] Next Generation Air Transportation System – Improved Risk Analysis Could Strengthen FAA's Global Interoperability Efforts - a complex, long-term initiative intended to modernize the U.S. air-traffic management (ATM) system in coordination with other countries' ATM modernization efforts. Commercial aviation is a global network and to function properly, aircraft and aviation information must seamlessly transition across national borders. In 2012, GAO conducted a study specifically focused on the global interoperability efforts of Europe and the U.S. Since NextGen and SESAR (the European equivalent to NextGen), are now transitioning from planning to implementation, GAO was asked to provide an update on the 2012 report to provide a sense of stakeholders' perspectives on factors that might affect global interoperability of NextGen.

They also looked at what the FAA is doing to coordinate and collaborate externally with other countries and what they are doing internally to help support global interoperability efforts. GAO interviewed 25 stakeholders including manufacturers, airlines and airline service providers. It discovered the following two factors that can affect global interoperability: 1) the ability of international stakeholders to reach agreement on what international modernization actually means, and, 2) the implementation timeline

[25] http://www.gao.gov/assets/680/671755.pdf

required for interoperability, which is affected by geographical locations, lack of resources and financial constraints of other countries, as well as commercial aviation providers.

The GAO presentation concluded with Ms. Snyder's report: GAO-15-370[26] Report: FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen (see presentation).[27] NextGen is estimated to be a 40 billion dollar initiative with 20 billion dollars coming from government and 20 billion dollars from industry. The target date was originally 2025, but currently there is not a definitive soft launch date. GAO identified three key risks and cybersecurity challenges with the NextGen transition which included protecting the interconnected air traffic control systems that will be used for NextGen, securing protocol flight control systems or other avionics on the aircraft, and shifting the organization and management within FAA so that it can be responsive to the needs of NextGen. The NextGen process is based on the NIST Cybersecurity Framework. NextGen will enhance interoperability and incorporate cybersecurity controls into its acquisition systems.

The Chair mentioned the FAA is cautious about swiftly making changes and was not as timely as it should have been on implementing controls. Ms. Snyder stated the report recommended that the FAA be more responsive with NextGen and to quickly implement upgrades and updates as the systems' needs grow and change. The lifecycle of NextGen is continuous and there is not an expected end date of the system. NextGen will reduce the amount of air traffic controllers; but they will still be needed as backup. The focus of the report was on NextGen cybersecurity issues and not manufacturing steps for security protocols. Industry groups understand NextGen is coming and will have to train for it. Feedback from stakeholders has been accepted and taken seriously.

The meeting recessed at 5:00 p.m., Wednesday, October 21, 2015.

[26] http://www.gao.gov/products/GAO-15-370
[27] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-10/oct21_snyder_gao-15-370.pdf

Thursday, October 22, 2015

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

NIST Updates--
NIST Computer Security Division
NIST Applied Cybersecurity Division
Donna Dodson, Chief Cybersecurity Advisor, Information Technology Laboratory (ITL), NIST, and Director, National Cybersecurity Center of Excellence (NCCoE)
Matt Scholl, Chief, Computer Security Division, ITL, NIST

The Chair welcomed presenters Donna Dodson, NIST, and Matt Scholl, NIST. Ms. Dodson expressed her excitement about the prospects for Fiscal Year (FY) 2016 and for organizational efforts to manage the growth experienced over the past five years. She announced that in October 2015, NIST established the Applied Cybersecurity Division, adding that efforts are underway to establish a permanent division chief.[28]

Within the NIST Cybersecurity program, the team has always enjoyed a strong spirit of cooperation between programs and projects. In the past year, research and development related to computer security has strengthened in applying cybersecurity standards in business operations. The constant need for timely information provides NIST with the opportunity to build on the synergy already created. Mr. Kevin Stine has received funding and staff to move forward with his initiative and is currently sharing the overall infrastructure. Operationally, a joint cybersecurity innovation conference with DHS, TSA, and NIST will focus on security automation and related issues.

Mr. Scholl presented some of the recent accomplishments of the Applied Cybersecurity Division (ACD). Dr. Chuck Romine, Director of NIST's Information Technology Laboratory (ITL), is currently acting Chief of ACD, and oversees a broad range of expanding activities. Once leadership roles in the Computer Security Division (CSD) are defined, the relationship among leaders will be clarified. The group is working to implement coordination between divisions.

Additional external work includes a health care records security conference, (the eighth annual HHS conference); and a series of cryptography workshops. Documents have been produced on email security, white listing, virtualization security, working jointly with the Department of Defense and other agencies on guidelines for using PIV cards for physical access control, developing technology indicators that indicate threats on networks, putting threat information into structured threat information exchange format and making it available.[29]

There is concern about future threats and how to be forward looking. There is focus on building things better from the beginning; and providing corrections for commonly seen coding errors (buffer overflows, etc.). It is one piece of a larger effort. The problem is the underlying machines are unsafe.

[28] Post meeting note: Kevin Stine was confirmed as the Division Chief of Applied Cybersecurity Division
[29] See CSD webpage on *Events* http://csrc.nist.gov/news_events/events.html; and *Publications* http://csrc.nist.gov/publications/

CSD has produced draft documents on email[30] and virtualization security,[31] and is working jointly with other agencies on guidelines for using PIV cards for physical access control. CSD is further developing technology indicators to indicate network threats, converting threat information into structured threat information exchange format. The division continues to address concerns about future threats. The strategy is to "build better from the beginning" and to provide solutions to commonly-encountered coding errors. This work represents one piece of a larger effort.

The group is working to evaluate tools to assess software qualities and to ascertain why vulnerabilities exist at all. One objective is to assist the community to prevent or address known vulnerabilities and to ensure that software code (such as open source or proprietary) is developed in a "mature" fashion. Currently, innovation does match efforts to formalize software into an engineering strategy. The potential need for improvement is great, with the government being the last bastion of waterfall software development. Dr. Fu suggested bringing more evidence-based methodologies to software development. Applying scientific methods such as making research reproducible would be an aid to the cybersecurity research community.

Coding by its nature can be difficult to reproduce. Medicine and other scientific research is reproducible. Coding "grew in a bad way". The government and others are late to the game in thinking about cyber security and how code has been developed up to this point. There has been little consideration of the long term life of any code.

The National Initiative for Cybersecurity Education (NICE) is now working to educate students on how to produce hack-proof code and is reviewing existing code libraries for vulnerabilities. NICE is also testing standards performance programs for personal identity verification (PIV) cards and other artifacts. While travel is integral to NIST activity, a Presidential order restricts travel at the Department of Commerce or agency level due to transgressions by other agencies. Nevertheless, NIST retains the right to prioritize travel. Standard engagements will continue.

Mr. Scholl expressed his desire to address the board in the near future and added that a Federal Register[32] notice that was released in August 2015 proposing potential use of International Standards Organization (ISO) standards for cryptographic algorithm and cryptographic module testing, conformance, and validation activities, currently specified by Federal Information Processing Standards (FIPS) 140-2, and requesting public comments as to positive and negative aspects to the change in evaluating the impact of official travel to the budget and return on investment.

Next year, post quantum cryptography will be a priority. NIST will be looking at a new elliptic curve,[33] prompting re-opening the Federal Information Processing Standards (FIPS) on elliptic curves. Collaboration on post quantum elliptic curves has been requested by representatives from Germany,

[30] DRAFT NIST SP 800-177 Trustworthy Email http://csrc.nist.gov/publications/drafts/800-177/sp800-177_draft.pdf
[31] DRAFT NIST SP 800-125B Secure Virtual Network Configuration for Virtual Machine (VM) Protection http://csrc.nist.gov/publications/drafts/800-125B/sp800_125b_draft.pdf
[32] Government Use of Standards for Security and Conformance Requirements for Cryptographic Algorithm and Cryptographic Module Testing and Validation Programs https://www.federalregister.gov/articles/2015/08/12/2015-19743/government-use-of-standards-for-security-and-conformance-requirements-for-cryptographic-algorithm
[33] Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard https://www.federalregister.gov/articles/2015/10/20/2015-26539/federal-information-processing-standard-fips-186-4-digital-signature-standard-request-for-comments

Canada, and nations in the Asia-Pacific region. There are two elliptic curve issues: an issue with the random bit generator; a different set generates asymmetric cryptography and some of those curves are good. Some curves possess the desirable quality of speed and resistance to attack but break in a post quantum environment. Providing sufficient guidance in applying light-weight cryptography remains the overriding challenge. Three priorities exist: Post quantum curves, Light-weight cryptography, and how to provide sufficient guidance for use of light weight cryptography. The strategy implemented in the first five years is almost complete, but much work remains, including production of a road map to lay out the next steps in identity management.

The Identity Ecosystem Steering Group (IDESG) has come out with a framework for identity management and is working to identify and define tools and capabilities. As detailed in NIST Special Publication (SP) 800-63-2, Electronic Authentication Guideline,[34] the IDESG is also looking at opportunities to develop an appropriate, but not burdensome, framework of trust. The challenge: to clarify understanding of "Virtual In-Person" proofing. A major challenge exists on the initiation side, how people prove they are who they say they are. The GAO presentation on issuing Medicare smart cards played heavily on the identity verification issue. Methods and mechanisms in use today can assist. Privacy questions arise naturally during the process of dealing with these issues. They are evaluating different technologies for different use cases. Challenges exist within the United States in remote areas. The second part of (National Strategy for Trusted Identities in Cyberspace)[35] NSTIC's work is getting parties to have confidence in the PIV credential. As with all strategies to enhance security, issues related to privacy must also be addressed. An effort is ongoing to evaluate different technologies in different use cases. A major NSTIC objective is to encourage confidence among all parties regarding the PIV credential.

A request for information (RFI) relating to the cybersecurity framework[36] will soon be released for public comments. NIST Internal Report (IR) 8062[37] DRAFT Privacy Risk Management for Federal Information Systems was released in May 2015. Comments received so far indicate that the privacy community is quite receptive.

National Cybersecurity Center of Excellence (NCCoE) releases a new 1800[38] series of practice guidelines. The first part contains information for senior management. The second part is oriented to CISOs and others with similar responsibilities. The "bits and bytes" level provides information on how to recreate what was done. To date, the 1800 series of publications has been well received.

NIST also releases a report[39] on standards development and coordination between government agencies and the private sector. Within the United States, the work on standards has been led by industry, and it

[34] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf
[35] NSTIC homepage http://www.nist.gov/nstic/; NSTIC, Pilot Projects http://www.nist.gov/nstic/pilot-projects.html
[36] NIST Cybersecurity Framework http://www.nist.gov/cyberframework/
[37] http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf, see announcement http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-8062
[38] NCCoE / Library https://nccoe.nist.gov/library
[39] NIST IR 8074 DRAFT Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (2 Volumes):
Volume 1: Report http://csrc.nist.gov/publications/drafts/nistir-8074/nistir_8074_vol1_draft_report.pdf
Volume 2: Supplemental Information for the Report http://csrc.nist.gov/publications/drafts/nistir-8074/nistir_8074_vol2_draft_supplemental-information.pdf

cybersecurity coordination is increasingly becoming a top priority within and across government agencies. These two draft volumes propose a method of coordination, possibly in the form of a public registry for cybersecurity standards. Site content is currently maintained by government agencies, but would be greatly enhanced by responses to an annual request for data. In the end, the registry is only as good as the amount and quality of information provided by each agency. A final version of the framework is planned for publication in November.

To address the difficulty in tracking standards within the U.S. government, an NCCoE Phase 2 facility will open in January 2016. The space has increased to support 23 laboratories. The invitation to the ribbon-cutting ceremony will be extended to the board.

Mr. Scholl concluded his presentation by announcing that Dr. Ron Ross, recipient of a Service to America medal, will be inducted into the Cybersecurity Hall of Fame. He also announced that Dr. Kevin Fu is retiring from the Board. Dr. Romine thanked him for his service and expertise, and awarded Dr. Fu a Certificate of Appreciation. In response, Dr. Fu thanked the board for their assistance thus far, during his tenure on the board.

Department of Justice (DOJ) & Federal Bureau of Investigation (FBI)--Information Collection Going Dark Initiative--Overview, Challenges and Gaps

James Baker, General Counsel, Federal Bureau of Investigation (FBI)
James Burrell, Operational Technology Division Deputy Assistant Director (DAD), FBI
Kiran Raj, Senior Counsel to the Deputy Attorney General, US Department of Justice (DOJ)

The Chair opened the session by inviting the board members to introduce themselves. He then expressed his hope for clarify the relationship between law enforcement and national security aspects of the Going Dark Initiative, stating that developers are, in general, not well-versed in the legal aspects of the discussion.

James Baker, General Counsel for the FBI, introduced himself; followed by James Burrell, Deputy Assistant Director of the FBI's Operational Technology Division; and Kiran Raj, Senior Counsel to the Deputy Attorney General, US Department of Justice. Mr. Baker thanked the board for its interest, noting that this issue is important to the FBI, to the intelligence community, to state and local law enforcement, and to the FBI's partners overseas. The FBI needs the expertise provided by individuals and organizations such as NIST and ISPAB, who share the fundamental values held by the intelligence and law enforcement community.

Mr. Baker said that he frequently addresses multiple forums, encouraging participants to think about "the world we are going to have, and not necessarily the world we want to have," adding that, if we do nothing, we will end up having the world as it is – whether we like it or not. There are four areas of concern: (1) science and technology, (2) the economy, (3) the rule of law, and (4) the nature of the threat. Regarding science and technology, the "encryption genie is out of the bottle" and is available to both the good and the bad. Considering that technology will never roll back, data and network cybersecurity is significantly threatened.

Acknowledging that U.S. companies operate in the global marketplace, Mr. Baker asked who would bear the costs for public cybersecurity, considering that responsibility for encryption costs are becoming externalized. Regarding the rule of law, Mr. Baker asked under what circumstances, would we as a country, think the government should have access to communications and communications-related data. In relatively clear-cut instances of a cybersecurity threat, law enforcement is equipped with tools to request data from private companies. However, after making a legitimate case of probable cause, private companies are sometimes unable or unwilling to provide it, citing privacy concerns. In those instances, the question should be: under what conditions should the government have the right to access that information.

On the law enforcement side, crimes such as pornography, gun smuggling, gang activity, kidnapping, sex trafficking, child predators, as well as threats by terrorists and cyber adversaries should be considered areas where access is needed. It also applies to individuals and entities, whether locally or abroad, with whom the United States is at war. The issues are less about tactics than about policy and law – about how much society wants to provide information to law enforcement.

Since 9-11, the public expects the FBI and related law enforcement agencies to maintain a "zero-failure rate." The goal within the FBI is to be as close to the zero-failure rate as possible, but to achieve it, the FBI must have timely access to critical information in order to avoid and/or detect the threat. Some areas of the threat horizon remain dark and it is those areas to which our adversaries are most attracted.

The FBI aims to serve the American people, and will do what the American people want it to do. But because electronic surveillance is not as effective as it used to be, a new solution is critical – which is why the FBI and other agencies are reaching out to NIST and others to help solve today's challenges related to intelligence-gathering.

In response to the Chair’s question as to why orders are served on companies and not on the suspects, the reason is because the companies have the needed data and the suspects do not. In addition, it is to prevent the suspects from knowing that they are under investigation. The data itself can be thought of in terms of the infrastructure on which the information is stored and real-time detection of the encrypted communication itself. Ms. Levin suggested that achieving a zero failure rate should not come at the expense of the America we recognize. Mr. Baker agreed, saying that the balance between the two is precisely the challenge faced by law enforcement today.

The Chair maintained that the public should be informed that expecting a "zero failure rate" is unrealistic. Mr. Baker responded that the FBI has tried that approach, but without success, and that tools already used by the FBI, such as wire-tap authority, are not as effective as they were in the past. A recent incident was cited in which individuals in the United States communicated via Twitter with ISIL operatives overseas and that, when ISIL received unencrypted communications, they purposely moved them to "dark" channels. Currently, solutions to the rapid expansion of encrypted data are hindered because U.S.-based companies are reluctant to act, though the attitude is more positive among foreign providers. In short, trust between the government and the private sector is critical to keep abreast of cybersecurity threats.

How does law enforcement get access in individual devices? It depends on the device level and many complexities exist. The device must be configured in a particular way. Consideration must be given to how information on the device is stored, the percentage of data stored in the cloud may be small, and what is useful may also be limited. Data must be timely and scalable. The FBI is looking for a consistent policy decision that covers all elements.

States and local law enforcement agencies do not have resources to get this type of information. The problem has multiple layers. Expansion of encryption has made the job of law enforcement harder. Is there a progress toward workable solutions being proposed? The problem can be solved technically, but U.S.-based businesses are reluctant to act. Foreign providers are a different case.

There seems to be a divergent number of issues involved. There is not a one-size-fits-all solution. Part of the problem is that U.S. adversaries today are communicating using U.S.-made devices over U.S. networks, thus increasing the responsibility for cybersecurity to the FBI and the U.S. government in general. The FBI has been trying to deal with other aspects of going dark besides encryption. Considering what a solution should look like will determine its guiding principles. Dr. Fu noted those in security and privacy have concerns about the capability being misused. The solution is not necessarily that the government be the keeper of the solution. There needs to be trust between government and the private sector.

In conclusion, the discussion considered a number of questions. What are plans for carrying this forward? Is there some process that it is hoped will produce solutions? The FBI is confronting the problem today. They will keep trying different solutions until something works. Policy-wise – Education, outreach, discussion so that the public will learn about this concept. Trust, as far as is possible, but also building confidence in government as public debate is the focus. There may not be a single solution while there are many options. The presenters would appreciate future feedback from ISPAB and to assists in setting standards. How can standards help? That will need to be determined.

Updates on Executive Order (EO) 13636 Cybersecurity Framework

Matthew Barrett, Program Manager, NIST Security Outreach and Integration Group, NIST

The Chair welcomed presenter, Matthew Barrett, NIST, who last spoke to the board in February 11, 2015. Mr Barrett would like to have the board's feedback to his summary of the group's current activities, and updates on its plans. As of his last update, the group was on the verge of significant improved website[40] enhancements to increase an understanding and awareness of the Cybersecurity Framework, including an expanded section of Frequently Asked Questions (FAQ)[41] which now addresses 47 questions and an increased number of links to Industry Resources,[42] all of which contributed to approximately 500,000 page views to the website.

The group continues to participate in robust outreach activities, working with non-CI (Critical Infrastructure) groups such as the National Restaurant Association (which expresses an interest in the CI

[40] http://www.nist.gov/cyberframework/
[41] http://www.nist.gov/cyberframework/cybersecurity-framework-faqs.cfm
[42] http://www.nist.gov/cyberframework/cybersecurity-framework-industry-resources.cfm

Framework), collaboration with over 24 foreign governments, including a Mexico-U.S.-Canada tri-lab, 11 European Union (EU) nations, four Middle Eastern and five Asian nations, all expressing varying levels of interest. Also, received interest from standards organizations including the British Standards Institute (BSI) as well as by support groups representing the audit, insurance, and legal communities. Interest was also expressed by government regulators such as the Communications Security Reliability and Interoperability Council (CSRIC) Working Group 4 and extensive interaction with the Securities and Exchange Commission (SEC), the Federal Deposit Insurance Corporation (FDIC), and others.

A presentation on future work including a draft RFI on whether the framework should be updated, a discussion on the long-term governance of the Cyber Security Framework, expansion of the role played by industry, and exploration of what government-industry relationship. Another effort in focusing on recognition programs related to cybersecurity and risk management with the intention of encouraging information sharing regarding best practices. An RFI workshop is being planned for spring 2016 as well as a discussion and subsequent publication (also slated for spring 2016), to clarify the relationship between cyber security and risk management frameworks.

In addition, the NCCoE is working in conjunction with the U.S. Coast Guard to develop a cybersecurity framework profile in the maritime environment, beginning with an examination of the cybersecurity aspects of moving crude oil from point A to point B. A publication, based on that interaction, is slated for mid-2016 publication.

Mr. Barrett invited input from the board regarding his presentation. Referring to the release of NIST publications related to the internet of things (IoT) and international strategy, Mr. Garcia asked how those efforts would coordinate with framework development. Much of the former work exists outside the scope of current framework efforts. But a harmonious relationship between the framework and efforts cited by the questioner are nevertheless important. As an example, he cited workshops between his group and individuals representing NICE to discuss issues related to the cybersecurity roadmap. He also indicated that the insurance industry has voluntarily asked related organizations if the cybersecurity framework can be used as criteria to determine rates of principal payments.

Industry should share the role of governing the Framework, adding that if government assumed a disproportionately large role, the final product might not be attained due to a lack of decision. Industry successfully manages many generally-accepted principles, such as those governing accounting, and encouraged NIST to seriously consider steps already adopted by industry.

A question was posted on the possible influence of the recognition program such as Malcolm Baldridge Award might serve as an example of encouraging innovative best practices. In the field of cyber security, recognizing the "best" best practices might not be productive. Recognition at that level might tend to dampen compliance by non-recognized organizations. A possible compromise might be recognizing the best by category, with an emphasis on framework alignment rather than being "the best" in the field. At the same time, this should not be mistaken as accepting mediocre practices. The framework is, after all, the product of canvassing the best practices. It was then suggested that recognition might take the form of a list of organizations aligned with the NIST Cybersecurity Framework, thus avoiding the stigma of choosing favorites. Mr. Barrett closed with an invitation to ISPAB for continued input and feedback.

Promoting Privacy, Transparency, and Accountability for Commercial Unmanned Aircraft Systems (UAS): NTIA's Multi-Stakeholder Process [43]

James Verdi, Director of Privacy Initiatives, National Telecommunications and Information Admin (NTIA), U.S. Dept. of Commerce

The Chair welcomed presenter, Mr. James Verdi, NTIA. Mr. Verdi began his presentation with NTIA's parameters, as set out by the President – to be a multi-stakeholder and agent regarding privacy, transparency, and accountability for commercial and private flight. The goal being to establish best practices to mitigate privacy concerns while promoting growth and innovation. NTIA's parameters do not include government operations, nor do they include private companies or contractors operating on behalf of the government. As examples of entities which will use UAS as part of doing business, Amazon (package deliveries), Google (internet service), aerial photographs (currently taken by satellites or manned aircraft), movie studios (who want to avoid risks associated with using manned helicopters), and hobbyists are prominent examples. The President views UAS as a technology poised to be a driver for economic growth and innovation in the United States, but which can only be implemented if the public believes technology would not be used to put millions of eyes in the sky to invade individual privacy.

The NTIA is not a regulatory agency, but works as a neutral broker with industry and civil society to craft common sense best practices. Some uses of UAS do not constitute privacy issues such as a UAS delivering pollutants into someone's pool. NTIA focuses on who operates the UAS and what practices are in place to ensure the devices don't create a nuisance or safety hazard when flying through populated areas, and that UAS don't stray into regulated areas like airports. One of the great advantages of working with the NTIA is there is no worry that discussions will result in regulations.

NTIA had its first meeting in the multi-stakeholder process during the first week in August, followed by meetings in September and October. Based on stakeholder input, the meetings produced two competing drafts. A meeting between the US Department of Transportation (DOT) and the Federal Aviation Agency (FAA) occurred on Monday, October 19 to address an increase in "close call" safety issues such as interfering with fire suppression efforts in the Western United States and injuries incurred when UAS flew into crowds at sporting events.

Because commercial operation is in its infancy, it is difficult to enumerate every scenario regarding the use of UAS. Commercial UAS have already been registered and recreational use of UAS will soon require registration. If money is involved in some form when using a UAS, it is considered a commercial transaction and therefore, subject to regulation. Examples given were wedding photography and deliveries for a fee. What is less clear, are instances in which hobbyists sell their product after the fact. Over time, arriving at best practices might best be served by encompassing a multitude of scenarios. Until recently, private use of UAS has mainly consisted of hobbyists using devices in limited

[43] https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua
http://www.ntia.doc.gov/blog/2015/improving-privacy-transparency-and-accountability-unmanned-aircraft-systems
http://www.ntia.doc.gov/federal-register-notice/2015/notice-best-practices-multistakeholder-process-re-uas
http://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-unmanned-aircraft-systems

circumstances like air shows and weekend meetings. But numbers of UAS are growing exponentially, and it is anticipated that they will be popular Christmas gifts.

Regarding public notification of an overflight, one of the draft documents states that, when reasonably practicable, commercial entities operating UAS should provide information about the location of the planned overflight and to notify individuals who are likely to be affected. Since the public is routinely notified when utility workers are expected to be in the vicinity, notification should be a reasonable expectation when commercial entities use UAS in the course of doing business.

In February, a Presidential memorandum outlined privacy, transparency, and accountability policy regarding UAS. Federal entities using UAS will be required to have a policy in place, and to report to the President on how they intend to use UAS and on ongoing efforts to promote privacy and accountability. Those same policies apply equally to state and local government entities. It also applies to any entity accepting Federal money to purchase UAS. Local entities that do not accept Federal funding are not accountable to abide by Federal policy. Currently, the NTIA is focusing on "small" UAS (lighter than 55 pounds) and on "micro" UAS (less than 4.4 pounds). NASA and the FAA already have a "see and avoid" standard, and are working to develop one addressing "detect and avoid." Attention is especially focused on the impact of UAS on air traffic control.

Prior to the next multistakeholder meeting scheduled for November 20,[44] the goal is to have one working draft instead of two. By December-January, stakeholders will be able to work in parallel and to incorporate feedback from outside the working group by the end of January. Based on feedback from meeting participants (who overwhelmingly disliked having to deal with government security) most meetings now occur in non-government spaces located in Washington, D.C. In general, these sessions have been well-received albeit some criticism. Criticism included wanting NTIA to take a more active role, and for not providing a technical level set regarding mobile technology. It was noted that achieving consensus does not always mean there is a positive decision. Sometimes there is no conclusion, but most decisions from past meetings were unanimous or overwhelmingly positive.

In order to improve understanding, NTIA has held, and is holding technical workshops to bring together a wide range of stakeholders, including industry, civil society, and academia. The group will craft best practices to help guide commercial and private UAS operators. The next meeting will focus on vulnerability disclosures. NTIA cybersecurity meetings are ongoing and Mr. Verdi hoped to introduce stakeholders at future meetings.

Cyber Norms

Chris Painter, Coordinator for Cyber Issues, Office of the Secretary, U.S. Department of State

The Chair welcomed the presenter, Mr. Painter, US Department of State. Mr. Painter informed ISPAB that the US Department of State recently proposed an international strategy to govern cyberspace. Its objective: to identify emergent and potential norms whose acceptance by the international community would address the growing number of threats to cyber security. The strategy would address issues such as the effect of cybersecurity on economic governance, on human rights, and on international stability.

[44] https://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-unmanned-aircraft-systems

Guidance, by like-minded countries possessed with the resources, would be provided regarding what countries can do to have institutions in place to address threats to cybersecurity, an example being the use of certifications and technical tools. On the nation-state level, the assumption is that no state has an incentive to lower cyber stability. The principles embodied in international law should also apply to cyber space. There is no need to create a new legal structure to deal with cybersecurity threats, referring to the UN Charter and to the Law of Armed Conflict as sufficient frameworks.

How these laws apply to cyberspace is still being defined, but concrete steps have already been taken. In 2013, an organization known as the UN's Group of Governmental Experts (GGE) met to discuss cybersecurity issues.[45] The GGE is represented by approximately 15 countries, including all members of the P5 (United Nations Security Council). In 2013, a conference on cybersecurity was held in London and attended by over 60 countries. Vice President Joseph Biden stood-in for US Secretary of State Clinton, and addressed the conference on the criticality of dealing with cybersecurity threats.

Returning to the applicability of international law, Mr. Painter said that the UN Human Rights Council is also cognizant of the applicability of cyber security in their domain. The U.S. is working very hard on this issue. It is important to keep in mind that actual incidents of cyber conflict are rare at best, but that we do see a lot of activity below that threshold. Peacetime norms could be created to apply over the long-term, apart from measures taken to address specific incidents.

There are four norms proposed by the U.S. (three of which have been supported for over 18 months):

1) A state should not conduct or support online activities which damage the infrastructure of another country offering services to the public.
2) A state should not interfere with c-cert responses to cyber incidents and that a state should use c-certs for good and not for evil.
3) A state should cooperate in a manner consistent with its domestic and international obligations with respect to other states investigating cybercrimes.
4) A state should not participate in the theft of intellectual property belonging to other countries.

Regarding the fourth norm, the President, sitting alongside Chinese President Xi Jinping in a Rose Garden press conference, was very clear about U.S. intentions and that "walking the walk" concerning agreements on the issue was critical.

Cyber norms per se are not guiding principles. They must first be universally acceptable. For example, it would not be universally acceptable for countries like Russia or China to propose norms prohibiting criticism of their form of government. A model for norm compliance might be compared to the Nuclear Non-Proliferation Treaty, in which signatories who break treaty obligations are sanctioned. The expectation is that countries recognize or will, in time, recognize that well-crafted norms are good for everyone.

[45] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security dd 24 June 2013 http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98

Government Adoption of Internet of Things (IoT) (PPT Presentation provided)[46] [47]
Chris Greer, Senior Executive for Cyber-Physical Systems (CPS), NIST
Martin Burns, Engineering Laboratory Office, NIST

The Chair welcomed Chris Greer, NIST, and Martin Burns, NIST. Mr. Greer defined the mission of the internet of things (IoT) as promoting the emergence of a secure, privacy enhancing, globally interoperable IoT in which U.S. companies are competitive. There are three characteristics of cyber-physical systems (CPS) in relation to the IoT. Firstly, it must be a network hybrid of information technology and interoperability of that technology. Second, it must be co-designed and co-engineered. Finally and most importantly, it should be adaptive and predictive in real-time-- the most challenging component, requiring fusion of cyber and physical. Mr. Greer cited two additional characteristics of the IoT. It is not focused on devices such as PCs and smart phones, but on devices not normally thought of as being connected to the internet such as toasters, refrigerators, and automobiles. It focuses on device –to- device interaction as opposed to person-to-person, or organization-to-organization interaction.

As defined, the IoT is a subset of the broader CPS landscape. Smart Grid, an application area of CPS, has some IoT components, but it has conventional, centrally controlled, enterprise IT elements to it as well. Although Smart Grid is a CPS, only a part of it is classified as IoT. This characterization also applies to intelligent transportation, advanced manufacturing among other areas.

There are a couple of important challenges in CPS. One is scalability. As an example, in the energy sector, a smart meter at the device level, is connected to a smart substation on the feeder line and then is connected to local, regional and continental scale grids. All of these are CPS in their own right, but as one moves up the scale, the complexity grows and the design for scalability becomes more challenging. This issue is not unique to the energy sector. It also applies to the communications and transportation sectors. However, the challenge remains that these systems are developed as verticals. The standards for interoperability are not the same for each sector. In other words, the real challenges are to achieve maximum capability and maximum economic benefit, because the goal is to not have a very large amount of internets of things.

One of the critical capabilities of CPS is compositionality. An integral part of the IoT is being able to use a device built for one purpose for other purposes, but it requires interoperability across domains. As an example, the City of Santa Clara worked with Silicon Valley Power to turn on the port on its smart meters enabling wireless access anywhere in the city.

One of NIST's goals is to promote forces for convergence. One of the major forces of convergence will occur through the Smart Cities initiative, which tends to consist of projects that gather together various infrastructures in a city around a common social goal. NIST has organized a program around three principles. First, CPS have a common intellectual foundation. Second, that it has a shared infrastructure that allows experiments across these domains. Finally, it has high value, at scale deployment that demonstrates the value of a compositional approach.
Mr. Greer introduced Mr. Martin Burns from the Engineering Laboratory Office who played an integral part in creating the framework of the NIST CPS Public Working Groups[48] with a goal to come up with

[46] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-10/oct22_cgreer_iot_overview.pdf
[47] NIST Cyber-Physical Systems http://www.cpspwg.org/

some basic definitions and analytical techniques that can be used to analyze, compare and describe CPS. The participants of these working groups are from government, academia and industry.

Less a year ago, the public working groups started a study focusing on reference architecture, use cases, security, timing and data interoperability. The completed initial work was pursued in parallel with key topic areas resulting in the release of the 0.8 version of the framework[49] in January 2015. The public review period closes November 2, 2015. Mr. Greer welcomed feedback on the study from the board.

Mr. Burns provided information on testbeds, the second level of scale. A testbed is being implemented on the NIST campus, and operates on the principle that experiments in CPS cannot be conducted in a single laboratory due to a possible lack of required resources or lack of knowledge of equipment. NIST is building in its own physical testbed, with the ability to federate using a high level architecture standard to enable experiments composed of hardware in the loop, desktop servers, clouds and collaborations with others. The architecture is based on work completed by Vanderbilt University. NIST views this as an exciting opportunity to build a community that can do complex experiments across domains in CPS.

Mr. Greer highlighted the third level of scale, the Smart Cities approach. There are good features of Smart Cities including being horizontal with the ability of crossing infrastructures and currently has vast economic activity. The problem is that there is a history of market failures of smart city projects for multiple reasons including custom integrations which do not allow new technologies to be introduced in the future; expense to maintain, thereby shutting out small businesses, and lead to vendor lock-in and other problems.

Because of this, NIST wanted to take on the idea of interoperable smart city solutions, deployments that are platform-based solutions that can be used in more than one city and for more than one purpose. To promote the emergence of this type of market, NIST started the Global City Teams Challenge, which promoted cities working together on shared deployments with multiple technologies in a platform structure. The 1st Global City Teams Challenge started in September/October 2014 and ended in June 2015. In June 2015, the Global City Teams Challenge Expo was held at the National Building Museum in Washington, D.C. and had 1500 attendees and 65 teams from four dozen cities from the U.S. and abroad with projects on everything from healthcare to smart grids.

On November 12, the 2nd Global City Teams Challenge[50] will launch, with a focus on quantifiable and measurable benefits to cities and communities that was not accomplished in the first phase. An important goal is to address smart cities market failures, demonstrate value of interoperable solutions, and to gather data on smart city architecture. NIST is convening a public working group in November 2015 to come up with a commonality of shared architectures and best practices. Dr. Fu mentioned the TerraSwarm project, a 30 million dollar research project at the University of California at Berkeley, in

[48] http://www.cpspwg.org/Working-Groups
[49] DRAFT Timing Framework for Cyber-Physical Systems, September 2015
http://www.cpspwg.org/Portals/3/docs/CPS%20PWG%20Timing%20Annex%20for%20Draft%20Framework%20for%20Cyber-Physical%20Systems%20Release%200.8%20September%202015.pdf
[50] http://www.nist.gov/public_affairs/releases/nist-global-city-teams-challenge-aims-to-create-smart-cities.cfm; http://www.nist.gov/cps/sagc.cfm

which NIST may find useful information regarding their Smart Cities projects. Mr. Greer mentioned that NIST may be interested in doing a Smart Cities hackathon as the platform grows.

Presentation from Dr. Kevin Fu: Analog Cybersecurity: Crying Wolf or Just Blowing Down an IoT House of Cards?

Dr. Kevin Fu, Member, ISPAB, and Associate Professor, EECS Department, The University of Michigan

The Chair welcomed Dr. Kevin Fu. Dr. Fu observed from reviewing ISPAB history over the last five years, NIST hosted eight panels on medical or health IT-related security and privacy issues. In one panel, Dr. Fu spoke on pacemaker security. In another, he sat on a panel addressing economic incentives to improve medical device security – which concluded with the finding there was none. In the last couple of years, however, some of the original attendees have "changed their tune" and have since taken active steps to mitigate the situation.

In May 2012,[51] Dr. Fu led a panel, **Highlights of New Federal Guide to Privacy and Security of Health Information,** which included people from NIST, the University of Pennsylvania, and others with backgrounds in health information technology. Mark Wolfson talked about the large number of computers running on Windows XP at Beth Israel Hospital. Dr. Fu said he would be interested to know how many XP devices still remain after three to four years.

Last June,[52] Dr. Fu hosted a panel on the software supply chain, **Emerging Guidance and Standards affecting Medical Device Security,** with the desire expressed that medical devices be shipped with information about internal software to better enable purchasers to evaluate risks. He also discovered a recent letter he wrote in 2012. After hearing several presentations from US Food and Drug Administration (FDA) and others, Dr. Fu noted a diffusion of government responsibility with no single agency responsible for cybersecurity policy. He noted at the time FDA's policy had a policy that likened to "let's just all get along", with a vague desire to share responsibility among agencies. To the purchaser experiencing a cybersecurity problem, the gist of their policy was "talk to your manufacturer," or, "install a firewall."

The good news is that in 2014, the FDA has issued an official guidance document, the first of two focusing on guidance[53] for the manufacturer regarding required steps prior to submitting devices for approval. Dr. Fu said this represents a huge step for the medical community. The document includes fundamental information like writing down risks to determine which to accept and which require mitigation. It also provides actions to detect and/or remove malware. The FDA is currently working on post-market guidance and grappling with methodology related to incident reporting and problems inherent in having a large number of stakeholders (hospitals, manufacturers, researchers, and others). It was noted patients are rarely involved in the dialogue regarding medical devices. As of today, many medical devices remain unsecured. Malware is disseminated and manufacturers become unwitting malware distributors.

[51] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2012-05/may-2012.html
[52] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2014-06/june-2014.html
[53] http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm418408.htm

On the positive side, a study was done to learn about the power consumption of a machine infected with malware. It has become easier to detect power consumption changes. Embedded systems have more limited states which can be enumerated and it is now possible to guess the state of a machine from examining its power consumption. But some intentional cyber threats remain elusive – a threat may trick parts of a computer to act as antennas for incoming information and light bulbs can become listening devices. It is also difficult to filter signals within range of the legitimate signal. Certain sounds can be sent to the gyroscopes in drones, causing drone systems to malfunction.
Clearly, as the degree of connectedness increases, threat vulnerability also increases.

Board proposes recommendation letter

This morning, Dr. Weinberger distributed a draft of a recommendation letter regarding quantum cryptography that was presented by Dr. Chen on October 21 to be reviewed by the board. The proposed text discusses that the solution is much harder than finding a cryptography algorithm. There will be many things that must be fixed in a coordinated fashion and agreement is necessary that all parts will work, and standards needed. The implementation will use commercial technology, requiring all participants to use the same technology. Since "old world" technology is not going away and must co-exist alongside the new technology, a plan should be crafted to implement the new standards and the proposed letter should urge a strategy for progressing to a plan to schedule meetings to implement the intellectual acceptance and adoption of the new standards. One challenge is articulating a strategy to measure progress. It is also possible that, in the end, there will be no drop-in replacements.

Dr. Weinberger proposed the motion that the board to draft the recommendation letter with the points summarized above. Mr. Garcia seconded the motion. All were in favor and the motion passed and was approved. A quorum was present for the board to vote.

The meeting recessed at 5:30 p.m. on Thursday, October 22, 2015.

Friday, October 23, 2015

The Chair opened the meeting at 8:30 a.m.

Password, Authentication and Metrology

Choong, Yee-Yin, Ph.D., Cognitive Scientist, Information Access Division, ITL, NIST (PPT Presentation provided)[54]
Kim Schaffer, DSc., IT Specialist, Computer Security Division, ITL, NIST (PPT Presentation provided)[55]

The Chair welcomed the presenters to the board. Dr. Choong began by reviewing on-going research conducted by the Information Access Division, NIST. At the outset, she stressed that the term "users" is multi-faceted. In addition to end-users, usability research impacts policy-makers, implementers, system analysts, and others. The presentation focused on end-users. There are three phases in the password management life cycle: generation, maintenance, and authentication.

Usability is not intended to be "touchy-feely" with the belief that no matter how great the system is, functionality is not there if the user cannot find the functionality. Password research studies cognitive processes and that the effort is not trivial. The first (generation) phase in the password management life cycle as required high-level cognitive activity, such as problem-solving, and this means the user must understand the requirements expected of them and often doing so in distracting external circumstances. Once the requirements are understood, the second (maintenance) phase in the life cycle begins. Generally, the maintenance phase is of short duration, focusing on the method (or methods) used to store the password.

The phase involving authentication is most often of longest duration and begins when the user is prompted to login (i.e., remembering the password among the several most of us are expected to use), requiring eye-hand motor coordination. If the user cannot remember the password, the user might have to retrieve the information by accessing other devices (laptops, iPads, etc.).

A recent study in password generation investigated user password generation space and the effects of rule presentation formatting. The study presented two sets of password rules: complex and simple in formatted and unformatted presentation styles. The 81 study participants, with an average age of 35 years, were evenly-divided between male and female. The task for each participant was to generate, within a specific amount of time, as many passwords as possible. Passwords based on a series or other clearly-identified pattern were allowed. Even though a pattern-based method of password-generation might simplify the task, it nevertheless revealed to researchers the method used by the subject to generate the passwords. Two timespans were noted: (1) from the beginning of the test to the first keystroke, to ascertain how well the test subject understood the requirements, and (2) the time required to complete the first password.

Dr. Choong proceeded to discuss complex and simple password rules. Complex rules require passwords to consist of one or more upper- and lower-case letters, one or more numbers, and one or more non-

[54] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-10/oct23_choong_password.pdf
[55] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-10/oct23_schaffer_describing-authentication.pdf

alphanumeric characters. Simple rules require no specific formatting. The test revealed that participants generated a total of 3,138 complex and 5,027 simple passwords, with an average of 100.8 passwords per participant. The average time taken to the first keystroke was 14.35 seconds for simple and 23.98 seconds for complex passwords, and the time taken to complete the first compliant password was 22.28 seconds for simple and 82.65 seconds for complex passwords. The test also revealed that formatted passwords resulted in better performance and that vowels comprised most of the ten most frequently-used letters, that most passwords began with an upper-case letter and that numbers and special characters predominated toward the end of the string.

Dr. Choong described an employee usability study, with participants chosen among Federal workers. The Employee Password Usability Survey, conducted in 2010-2011, was delivered online to 4,475 Department of Commerce (DoC) employees, capturing demographic information while ensuring participant anonymity. Each participant was asked how long it took to create a password. Considering that nine passwords per year were required, the data revealed that, on average, it took an individual 18.6 hours to create all of them. The explanation to so much time was consumed to create passwords reason was that system lockout resulting after too many successive password rejections often created delays while waiting for a system administrator to allow the user to reset the password. Time might also be spent asking colleagues for advice on creating a compliant password or for having to create a password which either had not previously been used or which differed sufficiently from a password which had been used. It might also be the case that the user forgot the password due to the length of time between logins.

Reaction to password policy was also measured. Most said policy required unduly long or complex passwords, or that password changes were required too often. Most felt that excessive security precautions frustrated efficient productivity. Another negative reaction was simply an expression of feeling overwhelmed. One of the solutions offered was the use of the single sign-on. Suggestions include change in employee attitudes would improve policy implementation, and the use of smart cards for identification/authentication. In general, most users favored usability over complex security. One of the fundamental objectives of such studies is to arrive at a workable combination of usability securely protected.

Public Participation – Chip Gibbons, Defending Dissent Foundation and Bill of Rights Defense Committee (see Annex B)

The Chair welcomed Mr. Gibbons to provide his public statement. Mr. Gibbons noted the importance of privacy rights and the right to dissent. He emphasized his presentation before ISPAB was not meant as an exhaustive discussion on the Going Dark Initiative, but simply to shed light on its impact on privacy rights and the right to dissent.

Dual concerns exist about technology: Technology in the hands of the people has been shown to have a democratizing effect. When technology is used by governments, the opposite effect occurs. The U.S. should not feel it is immune to these issues. Technology can have chilling effect on free speech. Email should promote a robust free press; but can be constraining in the context of government.

Mr. Gibbons reiterated the importance of privacy rights and the right to dissent in the context of the Going Dark initiative. While there are legitimate concerns about terrorism, there have been surveillance abuses. Many investigations of organizations begin as terrorism requests, even when there is no evidence to support the existence of a threat. The Supreme Court has recognized the right of citizens to protect themselves from government. The Bill of Rights and the fourth amendment is still the best guidance for government. Ms. Levin expressed appreciation to Mr. Gibbons and for his statement. Mr. Gibbons represents the groups that have worked to get legislation to prohibit law enforcement from surveilling on basis of first amendment activities.

2020 Census

Atri Kalluri, Chief, Decennial Information Technology Division, U.S. Census Bureau (PPT Presentation provided)[56]

The Chair welcomed Atri Kalluri, U.S. Census Bureau. Mr. Kalluri began by outlining the mandate of the Decennial Information Technology Division of the U.S. Census Bureau. The IT Division provisions systems to help implement the decennial census, to craft American community surveys, and to assist the geographic programs managed within the Census Bureau. He then introduced Kevin Martin, the Assistant Division Chief of Decennial Census Management Division.

At the outset of his presentation, Mr. Kalluri asked a basic question: "How would you measure America - its people, its races, and its economy?" The Decennial Census, mandated by the U.S. Constitution, measures the population and housing every ten years. Its findings define Congressional districts, thus informing the makeup of the U.S. Legislature. The key objectives of the census include counting everyone once, counting them in the right place, at the lowest cost per household, and ensuring that the quality of the census is maintained.

One challenge facing the implementation of the 2020 census is that it will occur in a rapidly changing environment. To minimize risk while maintaining quality, the census draws from multiple data sources. The state of the U.S. economy is a significant factor in determining the implementation method of the census. The Census Bureau plans to hire over 300,000 people to implement the survey. Details are available in the 2020 Census Operational Plan,[57] issued on October 6, 2015 and it is posted on the census website. It will be seen that technology is greatly assisting in cost savings.

Based on historical experience, the estimated cost to implement the 2020 census would total approximately 17.8 billion dollars. To date, incorporating advanced technology into the census process has reduced the projected cost for the 2020 census to 12.5 billion dollars – a savings of 5.2 billion dollars. The objective is to reduce the per-housing unit cost of taking the 2020 census to an average of $88.00, as compared to an average cost of $124.00 per housing unit in for the census in 2010. Mr. Kalluri pointed to four key innovation areas to explain the significant savings: (1) re-engineering the address canvassing process, (2) optimizing self-response, (3) using administrative records and third-party data, and, (4) re-engineering field operations.

[56] http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-10/oct23_kalluri_2020-census_nist_ispab.pdf
[57] https://www.census.gov/programs-surveys/decennial-census/2020-census/planning-management/operational-plan.html

In 2010, the Census Bureau hired over 140,000 canvassers who traveled (in aggregate) over 137,000,000 miles, covering almost every street in the United States – more miles than was covered by the United Parcel Service (UPS). To implement the new plan, the Bureau took into account day-to-day changes on the neighborhood level, including the pace and frequency of house construction and determining whether or not it is necessary to walk every street. To do this, 2010 data was factored-in and enhanced by adding measurements derived from sources such as overhead imagery. The Bureau recognized that authoritative address and other location information could only be identified at the local level. As a consequence, the Bureau entered into partnership with over 40,000 local governments. Several times per year, the Bureau factors-in and updates address information. "Mail-ability" and "locate-ability" are the key factors in this aspect of information-gathering to determine the location of a particular dwelling and is not about its inhabitants.

As to how the Bureau gathers data specific to new construction, Mr. Kalluri said the Bureau has two partnership programs to identify sources of new construction. If it is evident that the Bureau does not have the most up-do-date information, street canvassing is implemented. As to the consideration of using drones as a possible tool, Mr. Kalluri indicated the issue has been discussed and that logistics are possibly feasible, but that specifics have not yet been finalized. The use of drones is not included in the 2020 Census Operational Plan but might be considered in the future. In a majority of cases, canvassing is not needed, but that approximately 25 percent require it. The Bureau relies on USPS addresses and that physical addresses – not post box addresses – are used. Once finalized, the address list serves as the basis for the census. This new approach is projected to save over 900 million dollars. Another method of information-gathering is by self-response – the second key area of innovation. With the anticipation of high volume information derived from self-response, an online capability has been designed for the 2020 census.

To reduce the costs of using administrative records (the third key area), Mr. Kalluri discussed several objectives of the plan: improving the quality of the framework, increasing the effectiveness of advertising and other contact strategies, validating respondent submissions, and reducing the field workload related to follow-up activities. Commercial sources are used for information gathering, but Title 13 constraints are taken into consideration. The master address file is protected under congressional law, obligating the Census Bureau to protect the privacy of respondents. Data must not be identifiable to respondents and information provided by respondents is also protected. The information is used to tabulate data, but is not released for public consumption, nor is it released to other government agencies. Overall, this effort will save an additional 1.4 billion dollars.

As to whether social media will play a role, Twitter is under consideration to facilitate user response. The size limitation of tweets would prohibit direct responses, but it may be possible in the future to tweet links that could be used to respond.

In reengineering field operations, staff will be reduced by half – from 600,000 to 300,000. To comply with a Congressional request for specifics, a model is being used to verify the total. This effort itself will reduce overall costs by 2.5 billion dollars. The new technology will also reduce the time required to train staff. It is anticipated the 2020 census will have the largest self-response ever.

Does data exist to measure locations where self-reporting most often occurs? Data might be available from the 2010 Census and certain groups tend not to participate. The "digital divide" poses a challenge

to many who wish to participate in the effort, but the Census Bureau is working hard to ensure that respondent confidence remains high.

Board Review

During this meeting, the board had its annual group picture taken, which will be included in the 2015 NIST Annual Report. Ms. Annie Sokol, the Designated Federal Officer (DFO), had sent to every board member a package that includes newly prepared Handbook for ISPAB members, and ethics forms. Board members are required under FACA to submit their ethics forms annually. Ms. Sokol requested that members to return their signed forms to her as soon as possible.

DFO requested the board to discuss and approve work plan for the next fiscal year. The board provided the list to be uploaded on ISPAB homepage after the meeting:

- Quantum (physics, pre-shared keys, quantum key distribution, block chains)
- Cybersecurity
- Office of Management and Budget
    - OMB Circular A-130 Revised
    - Cyber-marathon
    - CyberStats
    - Measuring outcomes for cybersecurity
    - Cybersecurity protections in Federal acquisitions
- U.S. Department of Homeland Security
    - Fly-Away (Incident Response) Team
    - Einstein, Continuous Diagnostics and Mitigation (CDM) and measuring outcomes
- Networking and Information Technology Research and Development (NITRD) and Build-it-in initiative and NITRD – on how competent companies acquire IT
- National Highway Traffic Safety Administration (NHTSA) and automotive cybersecurity
- Federal Trade Commission (FTC) – security, protecting data
- Facial recognition, technologies, biometrics, and users
- Privacy technologies
- Privacy and Civil Liberties Oversight Board (PCLOB)
- Safe Harbor
- Acquisition

The board discussed a list of presentation topics for future meetings and possible recommendation letter(s). Presentation topics included various aspects of cryptology and cybersecurity at OMB. It was also suggested to invite a physicist to provide insight on the nature of Q (Quantum Day) and, if possible, to have presentations on DHS flyaway teams, future CIS guidance, quantum key distribution (QKD), block chain, and Circular A-130 following the comment period. Additionally, the members of the board suggested a follow up on the cyber marathon, cyber statistical reviews, Einstein and CDM. It is worthy to look into the "Build It In" initiative, and determine how competent companies acquire IT, receive an update from NHTSA after their January meeting and learn about harmonization strategies among agencies. Furthermore, an update from the US Department of State or other agency on the US response to Safe Harbor, a follow-up presentation from FTC, and GAO reporting on facial recognition technology from the FBI's perspective and from NIST on privacy engineering.

The board also considered writing a letter to OMB on efforts to harmonize regulations on acquisitions, as well as, a letter to NIST management thanking them for compiling a great agenda. It was suggested that the board remember to ask presenters how ISPAB could assist with their efforts.

Board's future meetings

The board reviewed the meeting dates set for 2016 as follows:

March 23, 24, and 25
June 15, 16 and 17
October 26, 27 and 28

The meeting adjourned at 11:15 a.m. on Friday, October 23, 2015.

ANNEX A

List of Participants

Last Name	First Name	Affiliation	Role
Baker	James	FBI	Presenter
Barrett	Matthew	NIST	Presenter
Beuse	Nathaniel	NHTSA	Presenter
Boyle	Vincent M	NSA	Presenter
Burns	Martin	NIST	Presenter
Burrell	James	FBI	Presenter
Cackley	Alicia Puente	GAO	Presenter
Chen	Lily	NIST	Presenter
Choong	Yee-Yin	NIST	Presenter
DeRusha	Chris	OMB	Presenter
Dodson	Donna	NIST	Presenter
Greer	Chris	NIST	Presenter
Griffor	Ed	NIST	Presenter
Hatipoglu	Cem	NHTSA	Presenter
Jagielski	Karen	FTC	Presenter
Kalluri	Atri	CENSUS	Presenter
King	Kathleen	GAO	Presenter
Krause	Heather	GAO	Presenter
Painter	Chris	DOS	Presenter
Raj	Kiran	FBI	Presenter
Romine	Charles	NIST	Presenter
Schaffer	Kim	NIST	Presenter
Schneck	Phyllis	DHS	Presenter
Snyder	Alison	GAO	Presenter
Stanger	Adrian	NSA	Presenter
Stine	Kevin	NIST	Presenter
Verdi	John	NTIA	Presenter
Eisenbers	Jon	NUS	Visitor
Garcia	Mike	NIST	Visitor
Greene	Jeff	Symantec	Visitor
Haag	Paul	FBI	Visitor
Kriz	Danielle		Visitor
Lesser	Nate	NIST	Visitor
Lifland	Tara	Adobe	Visitor
Lightman	Suzanne	NIST	Visitor

Last Name	First Name	Affiliation	Role
Mitnick	Drew	AccessNow	Visitor
O'Connell	Sasha	DOJ	Visitor
Schmidt	Amelia	Strooch & Shrooch & Lavan LLP	Visitor
Schroder	Matt	Adobe	Visitor
Smith	Matt	G2 Inc.	Visitor
Theofanos	Mary	NIST	Visitor
Wright	Helen	CRA	Visitor
Castelli	Christopher	Inside Cybersecurity	Visitor / Media
Curran	John	Telecom Reports	Visitor / Media
Lyngaas	Sean	FCW	Visitor / Media
Moore	Jack	GovExe	Visitor / Media
Noble	Zach	1105 Media	Visitor / Media
Otto	Greg	Fedscoop	Visitor / Media
Ravindranath	Mohana	GovExe / NextGov	Visitor / Media
Rockwell	Mark	FCW	Visitor / Media
Sobczak	Blake	eenews.net EnergyWire	Visitor / Media
Gibbons	Chip	Defending Dissent Foundation	Visitor / Public participant

ANNEX B

Statement of Public Participation

8 Bridge Street, Northampton, Massachusetts, 01060 ♦ 413.582.0110 ♦ www.bordc.org
♦ info@bordc.org

Testimony to the

Information, Security and Privacy Advisory Board

From the Defending Dissent Foundation

and

Bill of Rights Defense Committee

Presented by Chip Gibbons, Defending Dissent Legal Fellow

October 23, 2015

The Defending Dissent Foundation and Bill of Rights Defense Committee are national civil liberties organizations that work to realize the rights promised by the U.S. Constitution. The impact of technology on the liberties of all Americans is of great concern to us. Advances in technology have opened up great doors for people the world over.

Technology in the hands of the people has had a democratizing effect: people from all walks of life have access to unprecedented amounts of knowledge and are able to communicate across the globe with rapidity once unimaginable; the Internet has created a public forum for individuals to express their views, while its anonymity has allowed individuals afraid of retaliation for their speech to express potentially unpopular opinions; and the role of technology in organizing and facilitating new movements has been noted across the world—whether it is in the mass protests for democracy in Egypt and Tunisia or in being used to coordinate Occupy Wall Street and Black Lives Matter protests here at home.

But technology, when used by the government, presents serious challenges for civil liberties. First, as law enforcement and intelligence agencies gain new technologies, they often claim that existing legal frameworks do not apply to them. Both the Defending Dissent Foundation and Bill of Rights Defense Committee strongly assert the U.S. Constitution provides the framework for all government surveillance and that new technologies are not exempt from these protections. While the drafters of the Constitution could not have imagined smart phones, twitter, or emails when they wrote about the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" they nonetheless provided a clear framework for protecting personal communications from unwarranted government intrusion.

Second, as people have sought to use technology to facilitate democratic movements, governments the world over have sought to either restrict the use of technology, or turn technology into a repressive apparatus. The United States is not immune to this; this year marks the 40th Anniversary of the Church Committee, which demonstrated the very real legacy of government encroachment on democratic liberties in the United States. But such encroachments have continued: numerous Congressional reports, agency inspector general reports, and Freedom of Information Act (FOIA) Requests have repeatedly discovered the use of federal and local law enforcement to surveil, infiltrate, and collect information on First Amendment protected activities without any evidence of wrongdoing.

While this pattern of behavior is as old as J. Edgar Hoover, government use of technology has created a new chilling effect on speech. It has been reported that due to revelations concerning the U.S. government's surveillance of the Internet, journalists are now less likely to use e-mail to contact sources.[58] This is a great example of the democratizing power of the people's use of technology running up against the repressive potential of the government's use of technology. E-

[58] *See* ACLU & Human Rights Watch*, With Liberty to Monitor All: How Large Scale US Surveillance Is Harming Journalism, Law, and American Democracy* (2014) available at https://www.aclu.org/sites/default/files/assets/dem14withlibertytomonitorall07282014.pdf

mail should be enabling journalist to gather more information by being able to contact sources they may not be able to contact in person. Yet, technology here instead of being able to fulfill its role in promoting a robust free press is in fact creating new concerns for journalists and a chilling effect on speech.

Of particular concern to the Defending Dissent Foundation and Bill of Rights Defense Committee is the Federal Bureau of Investigation's (FBI) *Going Dark Initiative,* which this board heard about on Thursday. While both the Defending Dissent Foundation and the Bill of Rights Defense Committee inherently value privacy as a fundamental human right, our work highlights the importance of privacy to the right to dissent.

Due partially to consumer demands, private companies like Google and Apple are moving towards encrypting consumer data by default. This encryption protects important personal information, but also empowers people to speak freely and to organize for political change by safeguarding their personal privacy. In the past, the FBI has asked for built-in access to encrypted data saying current encryption policies hamper its ability to pursue terrorism investigations.

Some of the worst abuses of the First Amendment in the last thirty years, however, have been done under the guise of investigating terrorism. It was as part of a terrorism investigation the FBI spied on, infiltrated, and complied information on the Committee in Solidarity of with the People of El Salvador. A 1989 Senate Select Committee on Intelligence report found this investigation to be improper. Six FBI agents were disciplined as a result of the investigation.[59] A 2010 Department of Justice Office of the Inspector General report on FBI investigations of "domestic advocacy groups," such as the Catholic Worker Movement, Thomas Merton Center for Peace and Social Justice, Greenpeace, and People for the Ethical Treatment of Animals, showed that such investigations were often "terrorism investigations."[60] A 2012 FOIA request revealed that the FBI monitored the Occupy Wall Street movement as a possible terrorism threat—in spite of the fact that there was no evidence to support this.[61] It is also important to note that a more recent FOIA request has revealed similar improper monitoring of the Black Lives Matter Movement by the Department of Homeland Security.[62]

Even the federal government recognizes that its surveillance is not benign. Both the Supreme Court and the Federal Elections Commission have partially exempted the Socialist Workers Party (SWP) from campaign finance disclosures due to the "long history of threats, violence, and harassment against the SWP and its supporters by Federal and local law enforcement agencies and

[59] *See* Select Committee on Intelligence U.S. Sensate *The FBI and CISPES* (1989) available at http://www.intelligence.senate.gov/sites/default/files/publications/10146.pdf
[60] *See* U.S. Department of Justice Office of the Inspector General *A Review of the FBI's Investigations of Certain Domestic Advocacy Groups* (2010) available at https://oig.justice.gov/special/s1009r.pdf
[61] *See* Partnership for Civil Justice *FBI Documents Reveal Secret Nationwide Occupy Monitoring* (2012) available at http://www.justiceonline.org/fbi_files_ows
[62] *See* George Joseph, "Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson," THE INTERCEPT (July 24, 2015 2:50 PM) available at https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/

private parties."[63] While the FBI's counter intelligence actions against the SWP may seem like ancient history, the FEC renewed this exemption in 2013 citing a continuing threat against its members.[64]

When we have discussed encryption we have tackled it from two competing interests—that of individual consumers to secure important personal information from cyber criminals and the fear that bad actors may try to conceal their actions from the government. There is, however as the FEC exemption for the SWP shows, a third interest to take into consideration—individuals who want to protect their information from the government not due to their personal bad acts, but to shield themselves from the bad acts of the government.

The Supreme Court has long recognized that privacy is essential to dissent.[65] Knowing that the government may be monitoring their electronic communications activists, muckrakers, whistleblowers, journalists, and others essential to our democracy will think twice about what they type. This is why the Defending Dissent Foundation and Bill of Rights Defense Committee supports the right to encrypt information and strongly opposes any attempts by the government to erode encryption by including built-in access for the government. There is, in addition to this First Amendment concern, an inherent privacy right. On this note we recall the 1974 words of Senator Sam Ervin about the threat posed to our constitution by the government's "technical capacity to store and distribute information:**"**

> *Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom: the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.*

---

[63] *See Brown v. Socialist Workers '74 Campaign Committee,* 459 U.S. 87 (1982); Federal Election Committee Advisory Opinion 2012-38 – Socialist Workers Party available at http://www.fec.gov/pages/fecrecord/2013/june/ao2012-38.shtml

[64] *See* Federal Election Committee Advisory Opinion 2012-38 – Socialist Workers Party

[65] *See NAACP v. Alabama ex. Rel. Patterson*, 357 U.S. 449 (1958) ("*Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs"*)