INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Modernization Act of 2014]

MEETING MINUTES

Nov 1 and Nov 2, 2018
4300 Nebraska Ave NW, Washington DC
Yuma Building, Room Y112

Board Members	**Board Secretariat and NIST Staff**
Chris Boyer, AT&T, Chair, ISPAB John Centafont, NSA Laura Delaney, DHS Greg Garcia, Health Care Coordinating Council Patricia Hatter, Quallis Marc Groman, Privacy Consulting Brett Baker, Nuclear Regulatory Commission, OIG Jeffrey Greene, Symantec (phone) Steven Lipner, **Absent with Regrets**	Jeff Brewer, NIST, DFO Robin Drake, Exeter Government Services, LLC Warren Salisbury, Exeter Government Services, LLC

Thursday, Nov 1, 2018

Welcome and Remarks

Chris Boyer, Chair, ISPAB, Assistant Vice President, Global Public Policy, AT&T

The Chair opened the meeting with a brief review of the agenda for the upcoming two days. Mr. Boyer noted there is much interest in supply chain and the National Risk Management Center (NMRC) from an AT&T perspective. AT&T is dealing a lot with 5G deployment issues, there are a lot of security concerns around 5G. It will be interesting to hear what the administration has to say about the National Cybersecurity Strategy.

There is one change to Friday's agenda. From 10:00 to 10:45 a.m., Dr. Jon Eisenberg from the National Academies of Sciences, Engineering and Medicine (National Academies) will be speaking. Following Dr. Eisenberg's presentation, at 10:45 Jason Kim from the new Department of Commerce Office of Space Commerce will provide a short introduction to that office and their activities. That discussion will lead into issues that are starting to gain attention related to space and cybersecurity for space operations, including satellites, remote sensing, launch, and ground base functions. Space activity is both commercial and

private. There are also GPS implications.

Members spoke about recent activities happening with their organizations and broader events with implications that may be of interest to the Board. Guidance and best practice documents from the Health Care Coordinating Council on medical devices will be coming out that will define relationships between vendors and the hospitals they serve. Cybersecurity guidance for hospitals on their devices will also be coming. It represents progress involving two important subsectors.

The UK National Cyber Security Centre recently produced a document on internet of things security. A European Union (EU) -wide cybersecurity certification scheme is being developed that will be of interest to the Board in the future. Japan other countries in the Asia-Pacific are looking at similar ideas. We need to make sure that the U.S. has some product that we can work with to manage that environment.

Brief on NIST Privacy Framework Program

Naomi Lefkovitz, NIST

The Chair welcomed Ms. Naomi Lefkovitz of NIST to the meeting to update the Board on the NIST Privacy Framework. The NIST Privacy Framework attempts to deal with the privacy challenges that come with technology and using technology, in the U.S. and internationally. There are multiple points of view about how to address these privacy challenges. It is something NIST is very interested in.

Understanding whether rule-based approaches are going to deliver any meaningful privacy benefit, or whether they will become compliance risks instead, has been part of the NIST Privacy Engineering Program. The Cybersecurity Framework is intended to protect critical infrastructure, but security doesn't solve all privacy concerns. Privacy also is concerned with implications arising from authorized information processing. Privacy implications and consequences arise from authorized and unauthorized handling of personal data. The Privacy Framework is a voluntary framework intended to be a guide for organizations to use to understand how to reduce privacy risk.

The Privacy Framework team hopes to replicate the process that created the Cybersecurity Framework. The Cybersecurity Framework provided a common language and systematic methodology. There is a greater need for a more common language and the ability for organizations to be able to talk about privacy risks and how to manage them.

A kick-off workshop was held October 16th 2018. The Privacy Framework (the Framework) is intended to be a living document and will be updated over time as technologies change or uses of technologies change that impact privacy risks. Some of the areas of concern and interest as the Framework development process continues, are the differences between where cybersecurity was five years ago and where privacy is today. There are a many common practices for cybersecurity.

When NIST developed the Framework and outcomes were defined, the ability existed to point to standards or other guidance that helped organizations get to those outcomes. It's not yet known if the same level of robustness in standards and guidance can achieved in

privacy to help organizations have better privacy outcomes.

What needs does the Privacy Framework hope to address? Organizational needs will dictate the structure of the final product and what it covers. The first workshop in October started with a working assumption to hold discussions to see if the initial material was the right direction to start with. NIST has been working in privacy engineering for some years. Organizations still seem to be challenged by bridging policies and principles in the privacy area. Getting that bridge implemented into effective privacy practices still seems to be a challenge. This Framework may help bridge that gap. There was a general agreement from the workshop this was a good starting place.

An ability to set benchmarks in a manner similar to the Cybersecurity Framework was thought to be helpful. It gives organizations the ability to profile and measure against outcomes. One observation was the near consensus that the group should not focus on the word "privacy", and not get tied up trying to define it. The goal is not to focus on the definition as much as the concepts involved. When it's looked at in terms of concepts, it becomes much more about adverse consequences from processing data.

What's important for the Board is making sure the Framework is able to distinguish between privacy and cybersecurity in this context. The Privacy Framework should complement the Cybersecurity Framework, because of the assumption that the data is already secure, and delves into possible purposes the data might be used for, and by whom. The list of data processing risks is an objective list. The judgement of how serious those risks are, or their magnitude is entirely subjective; but the list of risks itself is objective. Presenting the information in a framework will give people a means to look at their information processing and determine how that processing may impact individuals.

The use of the word “problem”, versus “issue”, versus “harm” should be considered when talking about security. There is unauthorized access and various harms including data breach. Finding the right word to describe consequences from privacy risk is challenging because the immediate thought is usually involves lawsuits. It causes a layer of tension and it may be a place where some private sector input would be helpful.

The threshold for taking legal recourse due to an adverse privacy outcome has been an issue. In the security world that point is a much more defined thing. There could be an adverse outcome that will not be satisfied legally. Organizations must consider what they do and how they process data. They should also consider whether potential actions might be embarrassing to others even if there’s no standing for a lawsuit.

The Framework is more about increasing trustworthiness in products and services. People lose trust when they’ve been embarrassed. It diminishes interest in using services or their speed in adopting services.

Another important attribute of the Cybersecurity Framework is that people who might not know anything about cybersecurity can use these guidelines. Can NIST find a way to make privacy practices more accessible to all levels of an organization? What should those practices cover? The profile could be done at the industry level or at the organizational level. The thinking was it was more appropriate for the privacy space where different types of processing might lead to very different types of risks and different solutions.

As NIST develops this Framework, it should be organized and then mapped. It could start with the fix because that's what some groups of people want to start with; it could start with outcomes, or it could start with consumer rights or company obligations. The discussion about privacy can start from many places. The framework that NIST produces has to offer all these paths and then cross-reference if it's going to be comprehensive and accessible. That is not a small task. The important point here is that risk can impact an organization in many ways. It can impact the country and society.

The hope is to complete the Framework in approximately a year. Privacy Framework development is being modeled after the Cybersecurity Framework development process. There will be sector specific conferences in the coming months.

There will be divergence between a U.S. policy framework and General Data Protection Regulation (GDPR) compliance in some areas. NIST is not producing a regulatory framework. It's producing a tool or guidance that can be used in benchmarking or privacy practices. The Framework doesn't predetermine any outcomes, and so just as risk is contextual, so are benefits. The same data collection activity in one context could prevent higher risks, but it may also prevent higher benefits. It means reviewing the entire context. The Framework should then allow organizations to make informed, intelligent decisions based on a full evaluation.

B-R-E-A-K

Brief on DHS Supply Chain Security Program

Emile Monette, Co-Chair, ICT Supply Chain Risk Management Task Force Program Manager, Cyber Supply Chain Risk Management National Risk Management Center, DHS National Protection and Programs Directorate

The Chair welcomed Mr. Emile Monette of the Department of Homeland Security to brief the Board on the DHS Supply Chain Security Program. Mr. Monette is the Government Co-Chair of the ICT Supply Chain Risk Management Taskforce, and the Program Manager for the Cyber Supply Chain Risk Management Program.

Mr. Monett noted a big problem exists with the technology everyone uses to run their lives because we rely on connected things for many activities. The problem with relying on so much technology is that it's not really known what's in it, and people tend to trust commercial and economic actors in the supply chain and the value chain, to make decisions that are in the best interest of the end user. The problem is that doesn't happen.

The world has moved toward purchasing a lot more things as services, particularly the federal government. A large part of contract spending for the federal government is on services as opposed to products. What has happened in the course of purchasing more services than products is the supply chain itself has become more opaque. End users and consumers have become further removed from those making decisions about the supply chain.

Outside of nation-state actors, criminals acting in their own interest are making decisions

that affect everyone. Consumers don't know those decisions are happening and have no control over them. The market has created incentives for all economic actors in the supply chain to externalize as much of the risk as possible. It means a lot of the risk ends up with the end user, without the end user having any control or knowledge of what that risk might really be. There are risks to governments and individuals from not understanding supply chain risk.

Most incidents happen through exploitation of a known vulnerability or weakness that existed at the time of purchase. How can those market conditions be addressed? It involves culture change. The behavior and culture of buyers blindly trusting actors in the supply chain must change. The behavior and culture of technology manufacturers must also change. Take the example of how people used to buy cars. A buyer selects a car, purchases it, and after they drove off a short time later a major repair happens. The dealers knew it was likely to happen and took advantage of buyers not having information about the car they bought.

Today, there's much more transparency in the car buying process. Everyone has access to services like CARFAX and TrueCar. There are multiple information sources for buyers to have more leverage in the purchase process. Buyers go into transactions much more informed and with much more leverage, and as a result can walk out of a dealership with a better deal. Dealers quickly recognized that everybody has access to CARFAX and to competitor's pricing for any car. It reduced nondisclosure of lemons and different problems in the auto industry. That level of culture change is what is needed for technology. The goal is better informed buyers, and sellers that demonstrate best practices. Best practice demonstration comes through providing objective evidence on the state of the article being purchased.

Change comes about through leadership. Senior leadership means dictating how things will be done going forward. It's starting to happen in the federal government. Leadership in the Department of Homeland Security has taken on this 30-year-old issue and decided to do something about it, despite knowing there might not necessarily be a solution.

Industry is now coming to the table interested in supply chain security. There is sustained interest in multiple committees of jurisdiction in Congress. Legislation has been passed, but hasn't gone to the president yet, but has passed the House and the Senate. The administration itself is putting forward legislative proposals on supply chain.

The Federal Acquisition Supply Chain Security Act of 2018 sets up the Federal Acquisition Security Council. The act creates a government-wide senior leadership body that is responsible for supply chain security. It creates a peer body to manage the supply chain for the public and requires some agencies to participate. It requires some information-sharing between agencies and provides the authority for agencies to exclude a supplier offer without disclosing why. The Department of Defense (DOD) has had this authority for several years but hasn't really used it. Anti-virus software is the prime example of how the department stepped out into prohibiting a vendor. It took a long time to build a case with disclosable information.

There's an appropriation bill with language for a certain set of agencies requiring them to

conduct supply chain risk assessments prior to making purchases. NASA, Commerce, and Justice have been required to conduct these supply chain risk assessments for certain types of IT purchases for some years.

The Supply Chain Risk Management Taskforce was announced by the Secretary at the end of July at the Cybersecurity Summit in New York. The charter was completed within the last week. The first task force meeting will be in the middle of November for the executive committee, followed by a full task force meeting. The executive committee will approve some proposed work streams put together by the co-chairs. All executive committee members have been identified and identifying the remainder of the full taskforce membership is ongoing.

The committee anticipates working in three areas. One is related to a federal acquisition regulation rule proposing, providing a business case, or rationale for a FAR rule related to acquiring/purchasing by federal agencies certain types of IT. Certain IT or ICT need to be defined from original equipment manufacturers, original component manufacturers, or their authorized re-sellers. Industry has recommended this restriction for years. The counterfeit problem and the grey market economy problem for technology was discussed. DOD put the grey market technology problem into its own acquisition regulation supplement a couple of years ago.

The tricky part of the rule will be defining what products and services it applies to what the elements of the relationship between the original manufacturer and an authorized reseller need to be in order for buyers to have some confidence in that relationship. A lot of authorized relationships have stringent requirements for that authorized reseller to obtain the "authorized" title. Others are based on things like unit sales for the previous month that have nothing to with product or vendor trustworthiness.

There has been increased industry and government interest in participating in the taskforce. One of the challenges has been creating a structure that is representative of the entire industry. It’s a complex issue to arrive at a solution that is inclusive and transparent for all those impacted parties, and yet is not so large that it becomes unwieldy as a usable work product.

In the communications sector alone, there are many communications carriers and broadcasters and that's not close representing the entire IT sector and its supply chain. The taskforce will be doing some things that have been recommended for years but haven’t been done to date. It includes things such as requiring software to be made in a secure development offsite. It means requiring certain types of testing to be performed on the software before purchasing and actual installation.

The challenge and the complexity come in the opacity of the supply chain. After the first and second tier of suppliers, the primary contractor and the first-tier subcontractor, the number of entities involved increases dramatically. There isn't an ingredient list for IT bought off the shelf. Consumers wouldn’t necessarily know what to do with a software ingredient list if there was one, but this is where culture change on both sides of the equation needs to happen. Buyers need to be better informed and better educated about where the problems are, and sellers need to address those things.

The majority of supply chain incidents are not enabled by something that was put in place intentionally. It's enabled by things that existed from poor coding practices. The reason the economics are flipped is because those people deep in the supply chain are making decisions based on their own economic interest and they know that nobody's asking.

One of the things the supply chain taskforce can do is help companies identify how they're assessing risk with the best practices on how to assess the supply chain. One of the big challenges is understanding what all the subcomponents are that come out of a supply chain. It means if a consumer buys Product X, everything that goes into Product X is known, including the code. The taskforce might be able to lead development of some best practices on transparency and ways to assess and mitigate risk. The national sector is required to not only get the security assurances from first tier suppliers, but also security assurances from their suppliers' suppliers. It gets to be enormously complex and costly, and there are a lot of unknowns.

The obligation of the seller must be to understand their supply chain, and what third party software components are being used. Chips are easier to verify in most cases because they're physical. Chip suppliers check must more, because if it's shipped with a vulnerability, the seller has the responsibility to figure out whether it poses a risk to users. It's a shared responsibility.

Shared responsibility is what the supply chain taskforce is all about. Sophisticated commercial actors have been vetting suppliers and managing their suppliers well for a long time. Those same practices that manage the supply base for logistics and financial solvency are the same kinds of practices to use to get transparency and insight into the supply base for information assurance, software assurance, and hardware assurance.

Technology companies have been managing their supply bases and the cybersecurity of their supply base for some time. The goal is not to establish some new government regime that ignores good activities that have already been happening. The goal is to recognize good practices in a consistent way so that buyers can reward good practice with what they purchase.

Learning what companies are doing becomes a focus in learning how to improve processes. Information exchange is happening in both directions to build out a set of common approaches to the problem and documents would be helpful to everybody in the industry. There are other companies that are further along on this issue. The taskforce can help to get everybody to come together.

The real challenge with security is how to know that someone's actually doing what they're required to do. It's the harder part of the question. A second discussion may need to happen about whether there is value in security certifications and other ways to create more transparency about whether practices are actually being implemented. It would be helpful to companies to know when meeting a potential vendor that they fulfill certain criteria on security.

Making sure known vulnerabilities are addressed is a responsibility in reducing bad actions or the possibility of bad actions. When there is new technology, a vulnerability might exist that can be exploited. The way to find that vulnerability often comes from somebody who

wants to take advantage of that product suite rather than somebody who's buying that product suite. There's no incentive for a group of people who are trusting what they're buying to take something apart to see if there's something that exists that can be exploited.

A way to encourage manufacturers to possibly find and fix vulnerabilities before they can be exploited needs to be found. Contracts might have language to patch vulnerabilities within some time period. Patching vulnerabilities can be a differentiator for companies. It means there are processes in place and the value is that buyers know what they buy has at least some verified level of security.

How do we know there's a measure of security built in? In terms of best practices, there was an effort to establish standard practice for security controls and controls all along the supply chain. The ISO 20243 was a starting place, with the Open Trusted Technology Provider Standard.

It's cheap and easy to do bad things through technology. Let's make it more expensive and difficult by getting rid of known vulnerabilities. If there was more initial focus on vetting technology prior to putting it out for use then it would be possible to take some of that resource being used today to manage enterprise security and use it for something else. The total cost of ownership will be reduced.

The other important thing about the taskforce is that it's moving industry's focus beyond the transaction. The contract between entities is the transaction. Sophisticated commercial companies understand who their most important suppliers are. It might be that there's a vendor with whom a manufacturer might spend a small amount of money, but that one thing they purchase is critical to the mission.

This taskforce provides a platform for the government to have a strategic conversation with industry without some of the tension that's usually involved in a transactional conversation about contracts. The question becomes how to put some incentives in place to get better technology into the supply chain. It may be easier to proceed in smaller pieces with the understanding that the taskforce is going to probably need to be active in the longer term.

One action area is developing criteria and context for threat assessment. It's impossible to define the criteria for all products. It may be possible to establish some minimums. Picking out a particular type of product or use case for technology to set up an approved product list might be more useful. The goal is to pick out something that is manageable and achievable, but also meaningful. We don't want to spend time and energy putting effort into a project that is not impactful.

Brief on DHS National Risk Management Center

Mark Kneidinger Deputy Director, U.S. Department of Homeland Security | National Risk Management Center

The Chair welcomed Mark Kneidinger Deputy Director, U.S. Department of Homeland Security National Risk Management Center, to the meeting to update the Board on the National Risk Management Center (NMRC). The National Risk Management Center looks at

national critical functions as defined by the Patriot Act. The act pertains to those functions where a major intrusion may have a critical impact on the nation's safety and economy.

How a critical function is defined, and how it compares to current activities relating to risk assessment and sector activities needs to be understood. What's important is the interrelationships and dependencies a critical function may have. There are multiple cross-sector activities that occur and different technologies in use in those sectors. From a functional perspective, gaps exist in understanding the ripple effect across the private and public sectors.

The NRMC was created to look at cybersecurity and physical security together, because these areas have been evaluated independently in the past and an integrated view is needed now. Increased intrusion sophistication by nation states is happening. Industry needs to understand not only what it's doing as a sector, but also what the government is doing. The center will work with industry and government, examining the primary risks of each, where mitigation may be needed, or where policy needs to be developed, and where guidance might be needed. Then the ramifications can be understood on both sides.

Since its creation, the NRMC focus has been in a couple of major areas. First, it has focused on building an organization that has a heavy analytic background that can accept industry or agency partners. In building that organization, it started with the Office of Cyber and Infrastructure Analysis (OCIA) in DHS. OCIA staff make up the underlying foundation for the NRMC. In addition to setting up the lab structure, National Security Council (NSC) also detailed people from other parts of DHS with specific expertise in understanding more about cybersecurity. NRMC will be reaching out to additional state agencies, especially those that have primary sector and industry responsibilities. Additional expansion will happen once there is a better idea of where the focus needs to be.

The second focus has been sprints. There were several sprints identified as part of the cyber summit, including supply chains, setting up the charter, the task force, and setting the focus. Another sprint deals with looking at how to define national critical functions. The charter will include three primary sectors: mitigation, electric, and finance. The same process will happen with the remaining sectors. The intent is to include those sectors, which represent a large number of industries, and identify national critical functions through each sector.

The first stage looks at how to prioritize the most critical national functions, then to look further for related sector activities and dependencies. The first tri-sector meeting is being held today. The hope is to have industry and government working together to understand the consequences and ripple effects in those critical functions from an industry and government perspective.

The NRMC is not operational but strategic and looking to the future. A lot of effort has gone into meeting with all of the various sector coordinating councils, government coordinating councils, sector-specific agencies, industry partners, and others. Today, it's at the stage of being able to work with those sectors and start identifying the functions to be assessed.

The tri-sector is the initial focus. NRMC will be reaching out to the remaining sectors. There are metrics that were laid out which included the sprint activities. There's a Chamber of

Commerce meeting where we're going to be talking and reporting on all of the various sprints. There's also a measure regarding getting an operational body in place, and for setting up the capability to bring the private and public sectors in. The key metric will show what the impact has been. There will need to be an understanding of how the operational entity will work with the NRMC. It applies to sectors while the other element was to provide for the role between the two sectors.

L-U-N-C-H

Brief on Department of Commerce Botnet Roadmap actions from EO 13800

Chris Johnson, NIST; Megan Doscher, NTIA

The Chair welcomed Megan Doscher of NTIA, and Chris Johnson of NIST to update the Board on the Department of Commerce Botnet Roadmap Actions from Executive Order (EO) 13800. In the report it was agreed a roadmap would be developed to lay out the path forward and identify the players involved. The current draft is expected to be released later this month. The roadmap will not ever be final because organizations will want to be added, and details will change over time. Interest from stakeholders across various sectors is always welcome, and everyone is welcome to get involved.

The lines of effort covered in the roadmap are enterprise, infrastructure, technology transition, and the new one is education and awareness. Education and awareness elements were included throughout the other lines of effort. It was important that education and awareness became its own line of effort in order to talk about broad education and awareness issues. The previous version had 24 actions. Many individual task had multiple additional tasks. In this draft, they have been separated and there are now about 85 actions.

Each task has a description and contributors are identified. If anyone feels a contributor is missing, we will add the organization or entity as a contributor. The tasks should not be seen as assignments or as mandatory. The road map is supposed to remain flexible over time. The priorities can change in an administration, or something could happen in the news that changes priorities in both the government and private sector.

Stakeholder outreach will continue throughout the next year and beyond. After six months, some of the major stakeholders will share their progress in a workshop. Government will do the same. An update is due to the White House one year after the roadmap comes out. It will contain a review and a status report. Some of the board member organizations have joined partnerships that have volunteered to pursue some of the items in the Botnet Roadmap Report. NTIA has four working groups in session to present current progress. Special Publication 800-189 is in the development phase now. This publication talks about Secure Inter-Domain Traffic Exchange. It ties directly into some of the action items in the actual botnet report.

There is a series of competitions where teams of developers will come in and do time-box software development. Defect density and other attributes of the development process will be evaluated to try to identify tools or particularly effective approaches. We will look at the

data from this series of competitions to try and identify techniques that are particularly useful and helpful for moving the state of the art forward in software development.

The National Initiative for Cybersecurity Education (NICE) Framework serves as a reference tool for development of course materials within academia. There's a big focus on course materials on software development, determining best practices, and what sorts of educational pieces have to get into academia. What do we need to be saying to people that are learning software development and software engineering? Activities are moving forward and there's a long-term commitment to complete them.

One of the other work streams under the enterprise line of effort was in developing cybersecurity framework profiles for mitigation and protection. There is also work on advance enterprise network architectures, best practices for network management, mitigating the risk of automated restrictive threats, and some work related to IPv6 adoption. Zero trust networking also fell into the enterprise line of effort.

One of the other lines of effort was the education piece. There was a big push towards educating the workforce, preparing programmers and engineers with the appropriate skill sets and knowledge. It also means educating consumers about making wise choices in the products they select and guidance about choices relative to the products that manufacturers put out. A portion of the education effort also looked at deceptive marketing practices where people are trying to hide aspects of deficiencies in products. The last line of effort is the development and transition. This gets into developing secure software; it's where the tool chain work comes in.

Guidance documents are coming out based on individual tasks within the road map. The road map itself will be a tool to keep tabs on what's happening within the federal government and industry. The botnet report is important because it is more of the tool. It is intended for stakeholders to be able to see where they are. The report will be posted sometime this month.

There is a prototype tool chain infrastructure to be used for running competitions. The prototype is in the approval process to validate it is production worthy and ready to support the loads expected during the competition. Work just started on the competition infrastructure to make sure it's solid. The competition is among people who are supposed to develop software using the framework or using the tool chain.

Teams of developers from industry or academia will be invited. They can bring tool sets of their choosing into the challenge environment. Then, they will do a time-box development effort. We'll provide them a specification that describes functional requirements and security requirements. They'll be asked to build a piece of software in a specified period of time. We will take whatever they built and provided to us at the end of the competition and run it through a scoring regimen.

The idea of being time-boxed recreates some of the time pressures that people feel in the real world when they develop software. The goal is to right-size the development effort to put a little pressure on the developers, but still make it something that's doable. The Board is interested in hearing more details after the road map comes out.

B-R-E-A-K

Update Brief on NIST Draft IR 8228 Considerations for Managing IOT Cybersecurity and Privacy Risks

Kat Megas, NIST

The Chair welcomed Kat Megas of NIST to the meeting to brief the Board on NIST Draft IR 8228, Considerations for Managing IOT Cybersecurity and Privacy Risks. It was about a year ago that Ms. Megas briefed the Board on the IoT (Internet of Things) Cybersecurity Program at NIST. The mission remains about development and application of standards, guidelines, and related tools to improve cybersecurity impacted devices and their environments.

There have been some changes since the IoT project was last presented. Some projects have been added, such as examining low power WANs (wide area network), and consumer related projects. There are also projects at the NCCoE (National Cybersecurity Center of Excellence), including consumer-related security. This project utilizes results of other NIST internal projects such as the botnet project to inform any publications or work that we do on IoT cybersecurity.

The IoT project held workshops, a colloquium, and a number of roundtables. The feedback from these gatherings was anything NIST does on IoT cybersecurity should be risk-based, outcome-based, and recognize no one size fits all. There was strong encouragement initially to look beyond the device. A big takeaway was a need for a common language to discuss IoT. It started with a major discussion around whether a definition of IoT is needed. The direction was another definition was not needed. However, a common language to talk about IoT is very much needed. When IoT cybersecurity initially became a topic of discussion, everybody talked about the device, and how there needed to be better security on the device.

An understanding of how IoT is used was really needed before being able to determine how to secure it. Some wanted NIST to publish specific guidance on IoT, but guidance already exists. Many good cybersecurity practices exist. It may become a matter of understanding how to apply them in the context of IoT. NIST IR 8228 is not an attempt to define everything relating to IoT and managing security risks. The goal is to discuss the parts of IoT that fall outside of normal cybersecurity practice.

Privacy was included in NIST IR 8228. Stakeholders felt that it would be not a good idea to address IoT cybersecurity without having a discussion of privacy at the same time. The Privacy Engineering program and the Cybersecurity for IoT program worked closely on this deliverable.

NIST IR 8228 is not a requirement for federal agencies. It was felt that IoT was so broad at this point, and a flexible approach seemed more important. The IR is meant to be an introductory document, and it's anticipated there will be future versions. There's potentially a desire for more guidance or more publications from NIST.

Efforts started to try to develop a common language to be able to speak about IoT. The

intent was to identify the capabilities that are most important to understand about a device in order to understand the risks the device might present. The group developed and identified four capabilities. They were introduced prior to putting out the draft. There was a lot of positive feedback. Industry liked that NIST didn't try to impose a definition, but gave them the beginnings of a common taxonomy to talk about IoT. The taxonomy was included in this version of IR 8228. The hope is that federal agencies and other organizations that read 8228 will use this as a tool for analysis to look at devices, walk through the capabilities, and ultimately understand what the device is doing.

Viewed from a privacy perspective, it was felt the IR was broken down well. It forces people to think through all of the elements involved in privacy and how to protect the device, versus the data, versus privacy.

The topic of trustworthiness is something that comes up quite a bit in IoT. It doesn't mean the same thing to everybody. Internationally, there is a lot of work, and people are trying to define what it means for an IoT device to be trustworthy. It's not just about security and privacy for an organization. People want to know a device is reliable. They want to understand the performance and d the resiliency. Governments want to understand the device is safe. Our efforts are focused just on security and privacy.

There has been some mixed feedback. Some wanted to add safety and not just look at cybersecurity and privacy, but also figure out where safety overlaps those areas. When cybersecurity has issues, it may affect safety, and how those cybersecurity risks are addressed may affect the safety of the device or people using it. NIST did hold a workshop on IoT trustworthiness in areas where personal safety can be impacted by IoT devices. It was an opening conversation to understand how it might work. Privacy is not a new concept for NIST. Privacy goes beyond just protection of data and the unauthorized use of the data. Privacy includes the impacts associated with authorized use of the data as well.

The purpose of this document should be one where once people read the document, it should help them understand the risks that are perhaps uniquely associated with IoT, and some of the characteristics and features of IoT that may affect how to manage IoT risks.

There are three high-level risk considerations. The first is thinking about how the device interacts with the physical world; the ubiquity of IoT sensors; and understanding how they interact with the physical world. The second one is about device access management and monitoring features. Many of these devices are black boxes. There are not a lot of existing management tools to use for a lot of these devices. Third, the cybersecurity and privacy capabilities in these devices aren't sophisticated and not very capable. Users may have to figure out different ways of achieving goals if the device is not capable of providing needed security.

Protecting device security, protecting data security, and protecting individual privacy are major areas. The reason device security and data security were broken out came from discussions about protecting devices. A lot depends on the interest, how the device is used, and what it is, that would determine what areas might be relevant in the IR and others not.

The last item was dividing the world into pre-market and post-market. It was important for organizations that are going to be procuring devices to understand all the capabilities for

security that could be on the device. Fourteen capabilities were identified.

Manufacturing guidance is part two of the IR. It was included in the appendix because it was the only part that wasn't about individual risk management. It is focused on the pre-market. NIST will continue to work with industry and start building the appendix out into something that could be more focused for industry. The IR is really oriented to enterprises. These are the organizations that plan to use, or already use, the Cybersecurity Framework. The Framework is for understanding what subcategories are affected by IoT, and where IoT may present challenges to achieving those cybersecurity outcomes.

The federal profile may end up looking different than an infrastructure profile, which itself may end up looking different than a consumer. Starting with a common base that can be tailored, everyone can speak the same language. The work included in the appendix was really meant to be a tool for organizations procuring IoT.

If we hear feedback to have a workshop before we put out a draft, we can do that. The U.S. delegation proposed to ISO IAC JTC1 SD27 to start work on a baseline for IoT documents a couple of weeks ago in Norway. The proposal was accepted.

Brief on National Cybersecurity Strategy

Michael Halas, National Security Council, Executive Office of the President

The Chair welcomed Michael Halas, National Security Council, to brief the Board on the National Cybersecurity Strategy. Mr. Halas is the Director for Government Cybersecurity with the National Security Council. His role covers mostly defensive activities related to federal, state, and local governments, including the National Cybersecurity Strategy which the administration released last month.

Last year, the President issued Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. The Executive Order required a set of reports from agencies government-wide. The following reports help provide context for the cybersecurity strategy:

- Federal IT Modernization Report (moving to shared infrastructure and cloud services among agencies)
- Federal Risk Determination Report (requires agencies to evaluate their cybersecurity risk posture and identify how to address risks)
- Report to Strengthen Cybersecurity of Federal Networks and Critical Infrastructure (how to better support federal networks and critical infrastructure against increasing risks)
- Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats (defending against automated threats, and ways to incentivize device manufacturers to increase security)
- Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future (discusses immediate solutions to increase the size of the workforce in cybersecurity to meeting demands that currently outpace the supply of workers both in government and the private sector)

These reports enabled the administration to develop a comprehensive national cyber strategy.

During the first year and a half of the administration prior to the report, the government sanctioned malignant cyber actors, indicted those that committed cyber-crimes, publicly attributed malicious cyber activity, and released information publicly to help network defenders protect against that malicious activity. Departments and agencies have been required to remove certain software from their networks that presented risks to federal information systems.

The strategy recognizes many have struggled to secure their systems while adversaries have increased their ability and frequency to launch malicious cyber activity at the nation's infrastructure and government systems. The report is a comprehensive national cyber strategy intended for government to lead the effort in securing cyber space within the U.S. It is a call to action to both the private sector and the government on how to do that.

The cybersecurity strategy mirrors the four pillars of the National Security Strategy:

- Protect the American people, the homeland, and the American way of life;
- Promote American prosperity;
- Preserve peace through strength; and,
- Advance American influence.

It's intended to emphasize and further the notion that cybersecurity is one element of national power and needs to be part of a comprehensive solution.

The first pillar promotes protecting the American people, the homeland, and the American way of life. The objective is to manage cybersecurity risks, and to increase the security and resilience of the nation's information systems. Within the plan, the pillar is broken down into three sections with a number of priority actions. The first section is securing federal networks, the second section is securing critical infrastructure, and the third is combating cyber-crime and improving incident reporting.

The first priority is further centralization and visibility into the federal information infrastructure. It includes improved DHS visibility as agencies move into cloud and shared services. EINSTEIN has a lot of visibility across the federal infrastructure and network traffic. It's important to keep security in mind and ensure that the correct government-wide visibility continues as infrastructure changes occur. It's consistent with the OMB Federal Cloud Strategy, which is the Cloud Smart Initiative and the Federal IT Modernization Report. It outlines some of the details about how the government transitions more into cloud and how it can do so securely.

There's a section on federal contractor security. It acknowledges there's been a history of contractors not properly securing their systems, even systems that the government is contracting for, and not allowing the proper visibility into those systems. It stemmed from not having the right contract clauses, allowing the government to do assessments it often is required to do by law on those systems. The strategy includes an effort to develop contract clauses to ensure that visibility exists in the government's own contractor systems to make sure those systems are secure.

Formal clauses are being developed to implement a rule on classified information. There is content on federal supply chain risk management. It doesn't make sense to have a whole number of agencies separately evaluating products for supply chain risks. A lot of that activity can move more effectively into one or more shared services with experts in evaluating supply chain risk, who can then share supply chain recommendations and assessments within the government.

An administrative legislative proposal exists along these lines that would reduce the inherent redundancies. The administration has been working with Congress to get the authority enacted. The Senate Homeland Security and Government Affairs Committee (HSGAC) recently pushed a bill through the committee that will go to the Senate that is very similar to the administrative legislative proposal. If the legislative proposal becomes enacted into law, there are roles for a number of agencies, including DHS and NIST.

Secure critical infrastructure is the secondary focus area in pillar one. Working with the private sector is key when talking about critical infrastructure because most of it is operated by the private sector. The strategy calls for developing a more comprehensive understanding of national risk by identifying national critical functions. It includes sharing information with communication technology providers to enable them to respond and remediate known malicious cyber activity at the network level. There certainly has been some talk that ICT providers and Internet backing providers may be in a better position than anyone else to present certain types of cybersecurity threats. It's important to make sure they have the information to do that when it's appropriate.

There's content on defending election infrastructure. While state and local governments operate almost all the election infrastructure, we are making sure that we're providing them technical assistance when they need it, including providing support and training, doing exercises, and sharing cyber threats that the federal government has access to that the state and locals don't.

In some cases, agencies send resources in instances where states and local governments may not be able to defend their networks. In criminal matters, the FBI provides certain types of assistance and investigates threats. DHS also does that upon request. The strategy recognizes that law enforcement plays a critical role in detecting, preventing, and disrupting most cyber activity. It's a little different than the type of role discussed in terms of traditional cybersecurity mission.

The election infrastructure section primarily calls for the Executive Branch to work with Congress to update electronic surveillance laws and computer crime statutes to enhance law enforcement's ability to prosecute cyber criminals, and to attribute the activity to individuals so that they can be prosecuted. There is a call to work with private industry to confront challenges presented by certain technological barriers in some cases, such as authorization and encryption technologies. It calls for working with industries to confront those challenges to enhance law enforcement's ability as appropriate.

The introduction to the strategy indicates the strategy is effective immediately and department agencies should be following its guidance and implementing their missions. It also calls for the National Security Council (NSC) staff to coordinate its implementation.

The NSC has a policy and planning role. NIST will continue with control in developing standards; DHS will continue with offering states assistance. These departments and agencies will be the ones doing the operational work called for in the strategy.

Pillar two promotes American prosperity. This pillar recognizes that economic security is tied to national security. The objective is to preserve U.S. influence and development of cyber space as an open engine for economic growth, efficiency and innovation. The first area calls for fostering a vibrant and resilient digital economy. It contains things like promoting best practices and developing strategies to overcome market barriers to adoption of secure technologies.

A lot of this content is informed by the EO 13800 report on workforce. It calls for us to invest and enhance programs that build a domestic talent pipeline from primary school through postsecondary education, in order to improve recruitment and retention of qualified cybersecurity professionals, and to promote and magnify excellence by highlighting cybersecurity educators and cybersecurity professionals.

Increasing the number of professionals is a challenging problem. The NICE Initiative and other existing initiatives are major parts of the strategy. The strategy calls for enhancing the workforce. The workforce report acknowledged that there is a gap between the existing supply of cybersecurity personnel and the number of jobs that need to be filled in the government and private sector.

Pillar three is, preserve peace through strength. The objective is to identify, counter, disrupt, degrade, and deter behavior in cyber space that is destabilizing and contrary to national interests. In short, this section promotes norms, improves attribution, and improves deterrence. It means enhancing cyber stability through norms of responsible behavior. The work is led by the State Department with a lot of interagency activity as well.

The strategy calls for working to ensure that there's consequences for irresponsible state behavior that harms the United States and its partners. All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States.

The goal is to launch an international cyber deterrence initiative, to build a coalition and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber activity. The strategy seeks to expose and counter the flood of online malignant influences, information campaigns, and non-state propaganda and disinformation.

Pillar four intends to advance American influence. The objective is to preserve the long-term openness, interoperability, security, and reliability of the internet. We want to encourage other nations to advance internet freedom, the online exercise of human rights and fundamental freedoms, such as the freedom of expression, association, peaceful assembly, religious belief, and privacy rights online.

It seeks to promote markets for American ingenuity overseas, including for emerging technologies that can lower security cost, and build international cyber capacity. It means working with allies and partners to optimize or combine skills, resources, capabilities, and

perspective against shared threats. The United States can be supported by its allies and partners in its cybersecurity mission.

The reports forced everyone to go through this exercise to get the government on the same page on what its strategic direction is. The move towards the cloud is new

The Section Nine Critical Infrastructure list shows more of a focus on assets. The move focuses on functions coming from the current administration. It's more of a focus on the entities or examples of infrastructure that are critical to the country.

Critical means any company that controls critical functions to the point that its failure could be a national failure. A company might be on the critical infrastructure list, but it doesn't acknowledge the critical supply chain behind the company are critical to providing that function. Those entities might not be on the list. A single point of failure within a small area could potentially have a massive impact that is owned and operated by one entity. The challenge is to start thinking about this in small steps versus taking on everything at once. At some point there will need to be discussion on services.

Review of Thursday Briefings

The Chair asked for feedback from the board or any new comments on the briefings.

Mr. Lipner suggested an additional briefing from Ms. Lefkowitz on the Privacy Framework, including more details for agencies. The Board should understand what the developments are.

The Board may want to consider weighing in with the concern there is a lot happening all at once in multiple areas. In order to make progress in these areas battles must be picked carefully and prioritize where attention gets focused.

DHS and Commerce, along with other agencies at large and the government as a whole needs to be thinking strategically what issues to focus on and then ask for engagement from NIST. It's an area of ongoing concern that there's limited bandwidth here. The projects the Board has discussed are all really important projects. There's an issue of sequencing and making sure work is done in an organized way so that resources are not overwhelmed.

The National Security Telecommunications and Advisory Committee (NSTAC) is putting out the Moonshot Report on November 15th. The Board may want to consider what the report entails. The report will be proposing a process that would be launched similar to the Space Commission that would effectively create a long term dedicated effort supported by multiple pillars which including a technology policy, and education to really create better security for the Internet. The concept is to create a safe-zone so that there's a more secure environment on the Internet for transactions that need to be performed.

The idea is how to create a secure environment for where secure transactions are necessary, while at the same time preserving things like privacy. People have come in and they say things like do away with anonymity, other things on the Internet, to create a more secure environment. How do we create a more secure environment where we can validate that individuals are who they say they are, and transactions are what they're supposed to be, but at the same time not undermining what the Internet is used for today in terms of

privacy?

The goal is to create some process because the solution is unknown. It's an attempt to say what might be achieved in the next ten-year period to create a process to support this type of internet security.

The end state is to try to get to, and participate in, the process to get there without saying, "here's how". The next NSTAC meeting is November 14th. The report is posted publicly on November 1st.

The Board would like to invite the authors of the moonshot report to come and talk. The authors were Sean Morgan from Palo Alto, and Unisys was the other primary contributor.

Public Comments

There were no requests for public comment.

Meeting Recessed

The meeting adjourned at 3:30 p.m., Eastern Time.

Friday, Nov 2, 2018

The Chair opened the meeting at 9:02 a.m., Eastern Time.

Welcome and ITL Update

James St. Pierre, Deputy Director Information Technology Lab, NIST

The Chair welcomed Mr. James St. Pierre of NIST to the meeting to update the Board on NIST Information Technology Lab (ITL) activities. NIST and ITL have continued to focus on its original purpose of cultivating trust. It has helped to examine all NIST's work in IT and metrology. Key areas of focus include artificial intelligence (AI) and IoT.

The Board is aware NIST has a number of mandates put forth by Congress and also aware that the administration recognizes the value and importance of the NIST mission and its ability to help. It has been challenging at times working to address those mandates. There are a couple of updates. The Cybersecurity Framework released a draft of Revision 2.0 in December last year.

The NIST Cybersecurity Risk Management Conference will be held in Baltimore November 7-9, 2018. The conference covers not just the Cybersecurity Framework and NIST's broader suite of standards and guidelines related to cybersecurity, but also privacy, supply chain dimensions and practices, standards, and activities from other communities.

Cultivating trust in artificial intelligence (AI) continues to be consistent with the Information Technology Lab's (ITL) purpose. Mr. St. Pierre noted Dr. Chuck Romine is now the co-chair of the NIST Financial Science and Technology Council's Machine Learning and AI subcommittee. ITL will be working with the Department of Labor, as well as another subcommittee of the National Science and Technology Council (NSTC) Joint Workshop on machine learning looking at cybersecurity and AI. Planning is in process and ITL is represented on the planning committee.

Thought areas for the workshop include using AI to improve cybersecurity including improved detection, increasing system resiliency against future attacks, developing defensive methods, and improving security of AI. There needs to be thought on how to protect these systems. If the intent is to heavily use and rely on AI, it's important to define and understand AI vulnerabilities and then improve resiliency of AI methods and algorithms against different forms of attacks No date has been set but early in 2019 is the expected timeframe. The goal is to work on AI improved security and improving AI itself.

Quantum transition continues on program-level standards and guidance. Post-quantum cryptography is moving along well. Sixty-nine submissions were submitted in round one of NIST's search for algorithms. In April this year, NIST had the first Post Quantum Cryptography (PQC) Standardization Conference. Round two will start in the second quarter of 2019. We'll continue to look at quantum cryptography performance.

For IoT, the objective is to share and amplify awareness of NIST's approach and the approaches others are taking. There are international-only panels with representation from Switzerland, the U.K., Bermuda, Israel, and Germany.

With the most recent update to early version quantum standards about six months ago, we're focusing on increasing use and adoption of the Framework. There is focus on the standards and guidance side of cybersecurity, with increased work on supply chain in privacy. It is one of the privacy framework activities underway now.

Cybersecurity is a part of enterprise risk management as agencies view security in the context of their missions related to Executive Order 13800. From a NIST perspective there is a broader enterprise risk management function. Cybersecurity is a piece of that discussion alongside physical security. Risk management isn't limited to cybersecurity and privacy, but must also include financial, the customer, and business. It has to include these other risk areas that are critical to business or mission. Cybersecurity should be included in that same level of consideration.

At NIST there is an enterprise risk management process, a risk management officer, and a subcommittee that tracks the audits of different areas of cybersecurity, financial, facilities, and current events. It looks at all risks and elevates the most immediate risks to the highest levels at NIST to be evaluated and prioritized.

Elevating risk and making the implications clear to senior management is an issue for companies in general. A lot of companies view risk as potential brand damage, reputational damage, or customer harm. It's seen as a business impact, so people make decisions based upon those factors. This has been an issue in the industry for years on how to translate damages from cyberattacks into dollar amounts. There are some companies that model cybersecurity risk in more detail, in order to get as much of a quantitative view as possible. People used to talk about trying to calculate annualized loss expectancy. The hope is that people at least track the movement in risks and as more things move toward that top line of what what's acceptable, those things receive attention. The Chief Risk Officer must do the translation and make sure the explanation is understandable.

OMB Cyber Office Update, FISMA Out brief

Derek Larson, OMB Office of the Federal CIO

The Chair welcomed Derek Larson of OMB to the meeting to update the Board on Cyber Office activities and FISMA. Mr. Larson is with the OMB Office of the Federal CIO. Mr. Larson will be discussing FISMA activities in 2018. There were two major FISMA metrics updates in 2018. Early in 2018 a number of new standards were added to existing standards as part of the administration's move to adopt a new aggressive stance with priority goals in the President's Management Agenda. The new metrics were added, and they looked at the outputs from the President's report on IT Modernization and the Risk Management report.

The IT Modernization Report tasked OMB to ascertain the FISMA metrics were in line with the President's agenda and make sure things move forward. There was an interim round of reporting on FISMA metrics to give agencies the opportunity to report using the new requirements. During that update, there was a much greater focus on high value assets. A number of metrics questions were moved from FISMA CIO metrics to FISMA IG metrics. There have been a number of questions on reports and tests, but most importantly, the

concern was centered on the soundness of the plans and tests that were being done. The IG seemed a better place to assess the information collected by OMB.

There is a much greater emphasis on enterprise visibility. A big problem has been that large agencies have fractured networks. OMB wants to move agencies toward having an enterprise view so they can understand everything that's happening on their networks. The Financial Information Security and Management Act (FISMA) also sought to streamline reporting measures by centralizing how agencies make their reports, so that agencies were not being asked to report the same information multiple times. FISMA uses Cyberscope to collect information from the agencies.

The fourth quarter reporting deadline just passed and the data is being reviewed. The Chief Financial Officers Act of 1990 (CFO Act) agencies just reported on their FISMA metrics for the third quarter of FY18. As with new reporting methods, some areas did drop, but a number of others agencies demonstrated a high level of network maturity in their network security. In the area of exfiltration and defense, all twenty-three CFO agencies hit the set target level.

The Office of Management and Budget (OMB) has worked very closely with the Inspectors General (IG) community to make sure they are working according to the same methods and standards. Previously, IG and IT metrics were done separately, and the data needed to be organized after it was collected. A lot of effort has been put into making sure things are in alignment and there is no duplication between the two sets of metrics. FISMA is collecting quantitative data; whereas, the IG collects qualitative assessment data. Last year was the first year for data collected following agencies moving to a maturity model.

This year everyone is more familiar with the model and the data should be interesting to evaluate. FY19 looks to be more consistent as there is now a greater understanding of what is required. There may be some changes but not at the previous scale. The next set of data should begin to reveal trends on agency progress.

A couple of years ago, The FISMA IG metrics switched from a yes/no response to questions, to a ranged response on agency maturity levels. Agencies are asked to evaluate where on the spectrum their level is. FISMA IG metrics are based on inspector general audits. FISMA chief Information Officer (CIO) metrics are self-reported; the annual assessment is done by the IG or an outside independent assessor.

The Board has noted in the past that there is some inconsistency in the cybersecurity experience level of IG offices to assess agency security levels. It has the potential to affect the accuracy of the assessments they make. Mr. Larson noted the IG community is independent of OMB, but they do work as partners. The Council for Inspectors General on Integrity and Efficiency oversees the IG work. There have been workshops for assessors and Chief Information Security Officer (CISO) offices to provide opportunities to ask questions on potential scenarios that may come up while making assessments. Mr. Larsen's office has tried to provide as much information as possible, but they do not try to help the assessors interpret answers they receive.

Review of National Academies Report, Decrypting the Encryption Debate, A Framework for Decision Makers

Dr. Jon Eisenberg, Study Director and Senior Director, Computer Science and Telecommunications Board

The Chair welcomed Dr. Jon Eisenberg, Computer Science and Telecommunications Board, National Academies of Sciences, Engineering, and Medicine to the meeting to update the Board on the study: *Decrypting the Encryption Debate: A Framework for Decision Makers*. The National Academy is a non-profit, chartered to advise the federal government and the nation. It has been advising in matters relating to science and technology since the 1860s.

Dr. Eisenberg was the study director for this project. His office has looked at data science education for undergraduates and the impact of information technology on the workforce. Encryption has become available by default on hundreds of millions of devices and hundreds of millions of users of messaging applications. Encryption is an important tool for protecting data systems. Individuals, organizations, and governments rely on encryption to counter an array of threats. Criminals and others use encryption to avoid investigation and prosecution. Encryption complicates law enforcement and intelligence investigations. Intercepted messages can't be understood when they are encrypted, and the contents of a smart phone can't be read when it's locked and encrypted.

The Academy was asked to look at the legal and technical options available to government to access plain text communications and stored data, to look at trade-offs associated with those options, and to provide a framework. It took the shape of a set of questions that one would ask about any path forward. No recommendations were made. It is based on an assessment that there's some pretty serious concerns. Value systems come with these questions. Stakeholders were involved with the effort along with technical experts. It seemed that group would not reach consensus on a set of policy recommendations. It was hoped that having a diverse group would help shed light on the question and how one might best approach it.

The study was mainly sponsored privately by the Hewlett Foundation, the MacArthur Foundation, and the National Science Foundation. Dr. Eisenberg presented a high-level view of the report from the study. He noted the detailed discussions in the report are worth reading as well.

The study committee included current and previous members of the ISPAB board representing a diverse group coming at this problem from different perspectives. There were people with strong civil liberties and privacy views, people with law enforcement perspectives, as well as people with experience in the intelligence community.

The expressed views of intelligence officials in the U.S. have been somewhat more nuanced than in some other countries. Law enforcement and some intelligence officials call for a reliable, sufficiently rapid, and scalable way to access plain text to fulfill their missions. They'll cite the increasing use of encryption by default for national security threats. Digital evidence is increasing in importance as human activity and crime have become increasingly digital. The effectiveness of alternative sources of digital evidence is limited. One of the things that became clear is that spelling out "reliable, sufficiently rapid, and scalable" becomes important to the law enforcement community. It's not just some way to access plain text, but something that achieves those criteria.

Some of the concerns raised include the issue of just how effective would an exceptional access scheme be in light of ways it might be bypassed. Other concerns include cybersecurity risks, risks to privacy and civil liberties, the impact that it might have on U.S. providers of products and services in a global market, and the potential to hamper innovation in encryption technologies are among the concerns. It may be less necessary than is stated given the wider availability of data, especially metadata and alternative means currently available to obtain access to encrypted data. There are a number of computer scientists who have reacted with concern to renew the proposals to regulate the use of encryption, citing security risks. At the same time, there are people in the technical community who are looking at technical mechanisms that would minimize these risks. The report walks through a number of options for providing access to plain text.

Keeping the status quo is one of the options and the pros and cons of the status quo should be evaluated explicitly. Another option is, don't regulate encryption but provide law enforcement with more resources, specifically other ways of accessing plain text; and more generally augment their capabilities to pursue digital investigations. The legislation could be enacted that requires device vendors or service providers to provide access, but not specify the technical means of doing so. There also could be legislation or regulation that mandates a particular technical approach or a suite of technical approaches.

This report is aimed at helping to think through the list of legislative options and how to choose among them. There are legal tools that are available today that don't necessarily require new laws. There's compelled disclosure of a biometric identifier: a face, a fingerprint. There's the possibility of requiring passcode disclosure. The legal status of those options is very much in flux and the subject of ongoing litigation; as is defining exactly where the limits are of compelled systems under existing statute by third parties or government. This set of tools is available, but it is somewhat unclear to what extent these tools will be helpful and how far they can go.

In a general sense, there is a need for technical approaches one can simply require without mandating a particular mechanism, such as vendors having some capability to unlock a device when in receipt of a lawful request. It could be required that the keys needed to unlock, or decrypt be escrowed. There's a particular set of proposals around device level key escrow that requires physical access to the hardware. The committee agreed weakening encryption and reducing the strength of keys was not the best path. There's the notion of not imposing technical requirements but requiring case-by-case reasonable technical assistance from vendors and service providers.

The study took note of the various technical ways one might use to bypass an access mandate. If there's access mandated at the platform level that opens up innovation at the application level that may or may not be as readily regulated. One can simply install alternative operating system software on many devices. There are lots of old devices around and the use of legacy devices and software certainly would have a reasonably long lifetime. Steganography and other tools might side-step this method.

The report describes the various alternatives to exceptional access in some detail as a means of getting information that's needed for an investigation. It attempts to look at the pros and cons of each. In many cases the data on a phone will be available from backup in a

cloud service; through lawful hacking of various types or providing law enforcement with better tools for accessing and analyzing the data that's available that isn't necessarily encrypted can be alternatives to exceptional access.

Data used in the study was non-classified. Working with non-classified data allowed a wider set of people to participate in the activity. The study sponsors wouldn't have allowed classified data to be used because there is a national security sponsor for this activity.

There's incomplete data on the impact on law enforcement. There isn't data beyond some examples of the impact of encryption on investigations. There isn't much data on deliberate use of encryption by criminals. There are people in the law enforcement community who have mounted some efforts to try to collect information, particularly at the state and local level where a lot these cases are encountered. It's difficult at the same time to measure the additional security risks associated with an exceptional access mechanism because it's difficult to measure security risks in the security space.

It's a global market, and it's not known what the U.S. would do when interacting with the strategies and policies in other countries in the global marketplace. It was important to highlight the tradeoff between access and retaining privacy in the report because there are simplistic views about wanting access but also strong encryption. There is a fundamental trade-off between exceptional access to an encryption scheme and weakening security.

The absence of an exceptional access mechanism hampers government investigations in some degree because they will encounter encrypted data that they can't access. How much security is reduced with exceptional access and whether the resulting level of security is acceptable will depend on specific details. The impact on society will depend on the ultimate impact of investigations and the scope and scale of associated crimes.

There's a lot of bleed-over from commercial products and services to some mission-critical, or even national security critical applications. We Dr. Eisenberg's team constructed a framework to form the questions that we are suggesting when considering any path forward. The idea is to help policymakers determine whether a particular approach is desirable and balanced. It helps policymakers think about the implementation details, whether security is implemented in a way that maximizes effectiveness and minimizes harmful side effects.

It was clear that options to satisfy everyone were unlikely, and solutions will at best be only partially effective. The goal was to make sure decisions made are informed by thoughtful consideration of the trade-offs. The word "approach" is used throughout the framework. In this way, the framework might be applicable to regulatory requirements, policy choices, or a technology, a system modification that might be imposed by law, or that a vendor might implement in response to general regulation of access.

The first question in the framework concerns effectiveness and is it effective at the scale of timeliness and reliability? The second question was, to what extent the proposed approach would affect the security of the types of data, services, devices, that the requirement would be imposed on; as well as cybersecurity more broadly. Associated questions include: What is the potential scale of which the approach could be compromised and what effect would that have; How would one go about detecting compromise of that approach; and how

would one recover from it?

The third question looks at privacy, civil liberties, and human rights. It concerns both the targeted individuals in an investigation and others more broadly. How well does the approach ensure that government access is only permitted with appropriate authorization, and only applied to the content that was specifically authorized? How does the approach guard against unauthorized surveillance; and would the use of surveillance end up being used so wide that it would chill free expression and free association of other values?

The fourth question looks at commerce, economic competitiveness, innovation and the impact be on the competitiveness of U.S. vendors. Would it limit their ability to market products and services as secure as the market demands? Would the proposal in some ways restrain innovation?

The next question deals with whether the proposed approach is consistent with existing law and other government priorities such as broader constitutional objectives and freedom of expression and association. It's been an element of U.S. foreign policy to provide tools to support democracy and free expression overseas, and so there could be some conflict there.

What impact would international developments have on the effectiveness of the approach? Is it practical to enforce a requirement in the U.S. when nonconforming products and services are available globally? The whole study committee signed onto that set of questions as a reasonable framework for thinking through the problem. The intent here was that developing and debating answers to the questions would help someone trying to make a decision think through. The report also offers a helpful kind of common vocabulary descriptions of the problem in context.

Space Commerce

Jason Kim, Office of Space Commerce, U.S. Department of Commerce

The Chair welcomed Jason Kim from the Office of Space Commerce to the meeting to update the Board on space commerce activities. Mr. Kim noted space commerce is a major sector of the economy. About 75% of what is spent globally on space is for commercial activities, not activities by governments, from NASA, military spending.

Most of that spending is considered IT because it involves communications, or broadcasting, or data collection through remote sensing of satellite imagery, or navigation through GPS. It's taking the unique properties of space, and harnessing them to improve life on Earth. Space commerce has been around for a while, but recently there has been a resurgence of interest. The cost involved in space activity has decreased. Advancements in technology have miniaturized the size of satellites. They used to be extremely large, and now measure 10 cm2 and cost a lot less. Satellites can be 3D printed in some cases. High school and elementary school students are actually building and launching sets of satellites they printed themselves.

Satellites can be bundled into packages of dozens, or even hundreds, at one time into one rocket and piggybacked on another mission. The cost is split across multiple missions. The result is the price comes down a lot. It democratizes space for everyone, but also creates

issues that hadn't been considered before. An example is, the communications industry is interested in launching constellations of thousands of satellites each supporting 5G access worldwide.

Dozens of companies are trying to get venture capital for space commerce. SpaceX is using reusable launch vehicles. Reusing launch vehicles drives down the per-unit cost of launching vehicles. There is a new space race going on among billionaires to be the first to launch humans into space from U.S. soil on a commercial basis with paying customers.

There's potential for the first commercial flights to be next year. Hundreds of people have bought tickets and put down deposits on flights costing a quarter million dollars each. It has the potential to revolutionize travel for people on the ground. A space hotel is in the works funded by Robert Bigelow with Budget Hotels of America. The Secretary of Commerce, Mr. Wilbur Ross, has taken a personal interest in space commerce. The Office of Space Commerce is expanding and participating in various space councils. We're supporting American companies operating in space.

The Office of Space Commerce partners with NASA. NASA has moved from a purely government organization to outsourcing a lot of things to industry. The space shuttle was used for missions to the International Space Station (ISS) at a $4 billion annual cost. Now NASA entirely relies on commercial services to get cargo up to the ISS. Starting next year, NASA will begin flying crews to the space station using SpaceX and Boeing commercial craft as a paid service. The Office of Space Commerce is working with NASA on a strategy for commercializing the entire presence of humans in lower orbit because it will do the same thing the shuttle used to do with the space station.

The government discontinued funding for cargo flights to the space station in 2024. NASA wants to inspire a whole new generation on commercial human habitats in lower earth orbit. We're working with them on that challenge. It's not an easy problem, but we're trying to incentivize commercial industries to go in that direction.

There is a plan to put instruments on the moon for scientific measurements. A lot of commercial companies are already proposing to have land rovers on the moon for commercial purposes. NASA will put sensors on those commercial moon land rovers. It's a very different approach than what NASA has traditionally done. The National Oceanic and Atmospheric Administration (NOAA) also has commercial activities in space including gathering weather data from commercially operated satellites and combining that with their government inputs to see if more data will improve the weather forecast.

It's a pilot project that's going on currently. It took a huge cultural mindset change to convince the government to rely on a line of commercial capabilities. NIST is involved with standards that support the industry in measurement and calibration of satellite instruments.

The National Telecommunications and Information Administration (NTIA) is involved with spectrum policy. The Minority Business Development Agency in the Department of Commerce just issued a grant to the Space Foundation to promote small business and minority business involvement Mr. Kim's office is trying to expand the idea of the U.S. as the flight provider of choice for commercial companies that want to get into space.

The President signed a couple of space policy directives that direct Mr. Kim's office to engage in activities that will make the U.S. the flight of choice for space commerce. One of those areas is regulatory reform. He's cutting red tape and making sure that businesses aren't driven offshore by overregulation. There's a couple of areas that the Department of Commerce participates in. Commerce is actively pursuing regulatory reform. One area is remote sensing regulations. Commerce is trying to simplify that issue in the National Oceanic and Atmospheric Administration (NOAA) proposal that will be out any day. It will create categories, so everything isn't defined as spy telescopes. The International Traffic and Arms Regulations (ITAR) have been changed and the next steps are being taken to remove items from the ITAR list and move them over to commerce jurisdiction. We're also tasked by the President to lead on space traffic management. A new sensor network will be online next year that will see 100 times more objects in orbit around the earth.

The catalog of space objects in orbit is something that the Department of Defense (DoD) currently provides because they have a missile warning system able to see everything in space over earth. DoD is the only agency who can perform the space monitoring function. They provide customer service to industry and satellite operators and provide collision warnings when their satellite is about to hit a piece of debris or another satellite.

DoD doesn't tell them what to do, but only provides the warning to the satellite operator. The President has assigned the monitoring function to Commerce because the agency is more geared toward providing customer service to industry. DoD will continue to run those systems and provide missile warnings, but they will provide the data to Commerce, in a cleaned-up version that can be released to the public. That version will go out to the open architecture data repository that industry can come in and augment, supplement, add value to remix and resell to commercial operators as a service.

NOAA puts out warnings and forecasts for tornados and severe storms. It puts the data out there so that industry or academia use it or create services. That activity creates over a billion dollars of added activities related to commercial weather. That's the type of thing NOAA hopes to do with this area of space traffic management or Space Situation Awareness (SSA) data.

NTIS is involved with government procurements of cloud services. Space commerce has no future if we can't address managing space traffic and doing something to prevent further accidents and collisions in space. Cybersecurity will be important in protecting these activities. The goal is to create a one-stop shop for providing services to the space industry. We're doing the regulatory reform and the space traffic management work to create a base and a stable environment for companies to operate in and to keep them operating in the U.S.

One of the other functions that Mr. Kim's office has supported for about 20 years is the national management of Global Positioning System (GPS). GPS is an Air Force system, but when it comes to policy at the national level, the focus is making sure GPS is responsive to civilian and commercial needs. There is a national executive committee that's involved with GPS. There is recent concern about the cybersecurity of GPS receivers and the resilience of critical infrastructure that all commercial users use for GPS.

There's been a rising trend in different jamming, spoofing, and other kinds of disruptions to

GPS. The issue comes down to GPS receivers being based on designs from the '70s and '80s where they were just considered radio. There was no cybersecurity built into them. GPS receivers are computers, and they allow radio frequency input of data into systems.

Radio frequency is embedded into phones. It's not distinguishable from the rest of the electronics in a phone. It is important to secure the data input from GPS just as for Wi-Fi, Bluetooth, or LTE. GPS is based on a many clock times and provides a billionth of a second timing accuracy for synchronization and vast networks of communications and power grids. Multiple critical infrastructures use GPS because it's convenient and cheap, but it's not secured well.

DHS released a best practices document that's available on GPS.gov which is our national portal on GPS information. The Board would be interested in hearing more about the security issues relating to GPS.

B-R-E-A-K

Brief on the National Quantum Information Strategy

Dr. Carl Williams, NIST

The Chair welcomed Dr. Carl Williams of NIST to the meeting to brief the Board on the National Quantum Information Strategy.

Dr. Williams presented a high-level view of the National Quantum Information Strategy. Quantum is an area that's receiving a lot of attention at the moment. The strategy came out on September 23rd. It's consistent with the National Quantum Initiative (NQI). There was a summit the day after the strategy was announced with about 100 participants from academia, industry, and the U.S. government.

People may not be familiar with Quantum Information Science (QIS), but the market for hiring in QIS is becoming increasingly competitive. Post-docs with a degree will get $250,000 or $300,000 offers. The field is internationally competitive. There's also the problem of creating a workforce that can work on QIS. There are issues with maintaining national security while creating a situation for economic growth in this area.

Everything now is built on quantum mechanics: transistors and lasers don't exist without it. Einstein spent more than half of his career trying to prove quantum mechanics wrong, even though he was one of the fathers of the field, because he didn't like certain strange properties. Phenomenon that seemed random bothered Einstein. These are the things that are essential to quantum 2.0, what is now called coherent superposition entanglement.

Superposition is this possibility of a bit in an "on" state, like a classical binary zero or one, but both are simultaneously held. An entanglement describes how to create correlations that are beyond anything classical, that tie the fate of two quantum particles together. It is that ability and its impact on information processing that makes up the drive to quantum 2.0. It has implications for sensing metrology in being able to build censors that are beyond what was possible using quantum 1.0 technologies. They provide better sensing capabilities.

There are issues with securing communications, simulations, computing, and Shor's algorithm (which states given an integer N, the algorithm, will find its prime factors). It has to do with the ability to break codes. NIST has an active effort coming up with quantum-resistant cryptography. NIST has programs across all these areas.

The general-purpose quantum computer necessary to break codes or to do hard quantum chemistry problems is probably still twenty to twenty-five years away. Progress is being made and some of the risk is that there may be workarounds to breaking codes, even with using a less powerful computer that could put current capabilities at risk. It may not necessarily allow someone to run Shor's algorithm.

There's a lot of speculation about what kinds of things could be done on a machine less capable than a general-purpose processor. It could be something like quantum networks for relativistic geodesy. An example of relativistic geodesy means looking at the various modes of an object. The Earth actually has modes. It's only been in the last year that it's been possible to see some of the modes of the Earth, meaning it rises and falls like breathing. It may be possible to use sensor information from the Earth rising and falling to predict earthquake activity well in advance by measuring stress in the tectonic plates. These are the kinds of technologies that can come out of relativistic geodesy research. The issue is that this technology requires building out a whole new industrial base to support it though many of its applications will be for healthcare or other areas. Supporting quantum 2.0 technologies will be the key. The set of things that needs to happen is very large. It will take a lot of effort to achieve it. There was an article in *The Economist*, showing what different countries' investments are in research and development. There's a lot of investment worldwide and there is a lot of competition going on. The research effort is quite large.

China has the largest number of patents in quantum. There's a lot of effort going on worldwide in satellite Quantum Key Distribution (QKD), or base QKD from China. The U.S. has the capability of competing in this realm. The easy part of the problem is attacking the classical systems and endpoints. In order to protect against attacks, there must be authentication, but there is no quantum authentication method.

There's also a lot of activity around standards in this area. The Chinese, the South Koreans, and others, would like to have standards in place to prevent us from pushing quantum communications and other things that we may be deeply concerned about. It is an issue. They are spending a lot of moneyand are outspending the U.S. The U.S. may not need to spend at the level these other countries are spending, but it could spend smarter. The E.U. is also spending money on this.

In the U.S., large companies and others are investing. There are more than 20 venture capital companies investing in quantum alone. We've been out to industry. If industry hiring plans are not put in place soon, the pipeline will run dry and the same situation will exist in quantum information hiring that already exists in artificial intelligence. This is how quickly the companies are growing their programs and investing.

Why would a company investing in quantum if, as we believe, it's more than a decade before there is a viable return on their investment? It is unusual for a company to invest in something that is more than a decade away. Industry's view is everybody talks about

revolutionary technology. One or two revolutionary things occur in a century. This is one of those revolutionary technologies that will change how we do things. We need to be aboard the boat when that boat leaves port. In reality, the boat has already left. Yet, it's still a decade more before these companies will know how to make a profit and what to do.

There is a whole set of supporting industries who provide component technologies. The support function must start being built. It is something that we are focusing on because it's not about the end product. It is about the spin off early technologies that become components later. We need to begin building out that infrastructure.

National security, economic competitiveness, and the frontier of science depend on investing. There are a lot of reasons to begin building out the infrastructure to support developing the infrastructure. We need to understand what quantum might do to us. In some cases, it's understood fairly well what quantum will do to public key cartography. There is a bill before Congress that passed unanimously in the House. The bill basically addressed NIST, NSF, Department of Energy, and Open Supervised Device Protocol (OSDP).

Both committees in the Senate have versions of the bill and it may pass in a lame duck general session. One of the other things that NIST has done is work with industries in a consortium in this area. That consortium seeks to help us begin to understand where industry thinks its going. It relates to forecasting technology before it happens. It's being done in collaboration or in coordination with SRI International, which is a non-profit organization on the West Coast.

The consortium had its second meeting last week in Boulder, Colorado. A governing board was elected for the consortium. Thirty-four companies have signed letters of intent to join. It's anticipated another dozen or more will join. A couple of companies in the cryptometry realm have talked about joining as well.

Universities have known that they need to form broader coordination in order to get things out and those groups are forming. We will figure out how to interact with them. The consortium is in its very early stages. The issue is we know we need to engage with them because we know as we build the supporting infrastructure that some of the users will be the academics, the national labs, and others.

NIST is working directly with corporations. It's important to get their buy-in and then figure out how to engage with the other centers that are forming. The purpose of the consortium is to support enabling technology to let us move faster, do the R&D better, and whatever's needed to facilitate coordination and working with government. Industry's absolutely essential because they're the ones who will say where they think the first pay-offs are. Industry can tell us where the focus needs to be, whether it's on standards or other things. Industry will need to indicate the level of workforce required so the government can create a broad enough R&D pipeline to meet the future workforce demand, including people that are coming out with undergraduate degrees who understand this technology.

We need to be working on the problem because we know it takes a long time to fix. There must be serious work to resolve it. There are aggressive efforts underway to put standards in place and to provide blocking technology. We have been monitoring and watching because some of the components needed for QKD single full-time sourcing actors and other

things are also needed to provide quantum communication and quantum networking. It's needed to validate and verify the present quantum state and therefore, we know we have a secure handshake at the opposite end. In a non-quantum state, there is no assurance of security.

When looking to incentivize the R&D in this space, is there an anticipation that Moore's Law (an observation that the number of transistors in a dense integrated circuit doubles about every two years), is going to apply, and is that part of the long-range plan? At the Qbit level, that scale will hold. However, the problem's a little more difficult than just the scale. There're a couple companies that have roughly 50 Qbits. Within the next couple of years, some will have several hundred. Fifty to several hundred Qbits will be needed to begin to understand what the roadblocks to progress will be. To truly understand the engineering roadblocks, we need to have a few hundred Qbits to start with. Controlling and manipulating a few hundred Qbits is state-of-the-art. That breakthrough has yet to happen. It would take those companies five to seven years to come up with the engineering models. As they learn new things, companies will become very circumspect about what they share. Once companies progress to a certain point , they begin to think that they can develop the engineering pathway.

A threat to the current key structure will happen somewhere between 100,000 and 10,000,000 Qbits. Because of the error correction scheme, it takes a fairly complicated code. There's no easy, quick answer to this. The number of logical Qbits needed is roughly something on the order of about three times a key link. The larger that code space, the longer it would take to effectively run Shor's algorithm because of the time spent doing error correction and protocol increases.

It is true that the only way you can correct quantum state is to learn nothing about the state that you're correcting. It means learning about the syndrome without learning about the state. If anything is learned about the state, it crashes the whole thing.

There are policy issues that are national and economic security issues. The U.S. ended up with the semiconductor industry in large part because it made the largest R&D expenditure in the world at the end of World War II. Today, if you take both government and industry R&D, the U.S is down to 21 percent and declining. Every year the U.S. become a smaller and smaller fraction of the global R&D enterprise.

There are no longer millions of chip manufacturers. There is a handful because it's too costly. There are only two large commercial aircraft companies. In a global market, export control can be used to sink our chances. The U.S needs to figure out how to play the game smarter and more effectively. The strategy is to figure out how to begin building out the infrastructure. Companies will locate close to whoever owns the infrastructure.

The consortium is already having conversations about working with international entities. The best cryptography tools in the world come out of Europe and Japan. The U.S. does not own that market anymore. We need to go back to our trusted parties internationally. We also need to be sure that we own and have developed enough of this to be a major player in the field. There are many complicated questions.

The infrastructure will be built out with the things that first create commercial revenue

because that revenue allows reinvestment and farther support. There are applications in some of the atomic and platonic areas where this technology will go. Some of the technologies require cryogenics, to get temperatures down to about 100 millikelvin.

Quantum continues to come up as a major underlying technology that will enable other things with security. Quantum, the 5G network bill, artificial intelligence, and a few other technologies are underpinning technologies to a lot of the important things the U.S. wants to do as a country. It's important to make sure they're all on the right trajectory.

L-U-N-C-H

Brief on NIST Cybersecurity Framework Updates

Matthew Barrett, NIST

The Chair welcomed Mr. Matt Barrett of NIST to the meeting to update the Board on the NIST Cybersecurity Framework. Mr. Barrett last updated the Board on the framework in March 2018. Since the last, NIST published the final of version 1.1 Cybersecurity Framework in April 2018. New material was added on supply chain and supply chain risk management. Topics like identity proofing and authentication, coordinated vulnerability disclosure, and self-assessing cybersecurity were items that were addressed in that update. The original 1.0 road map was updated with retitled and consolidated material, along with adding topics.

NIST has been hosting free webcasts on the Framework. It has been tremendously well received. Every new webcast has 1,000+ registrants, and several hundred participants. Webcasts accompanied the drafting process of version 1.1, along with an overview when 1.1 was released. Recently, the webcast series was renamed, "The Cybersecurity Webcast Framework: Next Up". The new series is about the parties who are using the Cybersecurity Framework. It's no longer NIST speaking and educating people on the Framework. It's people bringing their own experiences with the Cybersecurity Framework to the webcast.

A recent webcast was with the University of Kansas Medical Center back in July. It featured the medical center's use of the Cybersecurity Framework, along with the Baldridge Cybersecurity Excellence Builder. They use both work products. The story is interesting because it's not only about cybersecurity, but they have participation from their larger enterprise risk and emergency services team.

Recently, NIST did a panel-style webcast with the Financial Services Sector Coordinating Council, the University of Chicago Medical Center, and the Coalition on Cybersecurity Privacy, Policy and Law. That webcast had 1,400 registrants, and 700 online at its peak. The average attendance during the webcast was 400 participants. Those events are livestreamed and recorded. Playback numbers have increased over time.

A lot has been happening with the webpage. NIST launched online informative references as a pilot and we have a number of pilot participants who are working that online reference format parallel the format of the Cybersecurity Framework. Informative references are pilot participants like the Center for Internet Security (CIS), the Information Security Forum (ISF), and Pivotal Cloud Foundry (PCF). There are additional mappings related to SP 800-

171, and SP 800-53 revision 4 that will be included in the informative references. NIST going to be talking about the catalog at conferences coming up next week.

All pilot participants will be at the conferences talking about their experiences. There is a new page called *Perspectives*. The idea is to inform a party's decision to use the Cybersecurity Framework. It quotes from key parties, many of them extracted from request for information (RFI) and request for comment (RFC) responses from the past as well as survey data.

Online learning modules were launched last February. They are brief and arranged topically, with downloadable PowerPoints for each topic related to the Cybersecurity Framework. There are seven modules on the core, the five functions, implementation tiers, and others.

NIST has been following Framework success stories. Since last spring, we have added four success stories to the site. They include the University of Chicago Biological Sciences Division, Japan's Cross Sector Forum, the Information Systems Audit and Control Association (ISACA), and the University of Pittsburgh, effective this morning. These parties each contributed two pages of material describing their Cybersecurity Framework use, and the value it brings them. There are two more success stories pending. They could be available as soon as next week.

We hope to receive feedback on the Framework focus areas. The focus areas have been pretty static since fall 2014. At the same time, NIST continues its focus on small and medium business, helping them understand how they might use the Cybersecurity Framework.

NIST has been supportive of providing input on the International Organization for Standardization (ISO) and their publication of ISO TR 27103. This is published. It is a full replica of the Cybersecurity Framework core with the five functions. In this instance, it's really the core of version 1.0 with its five functions, 22 categories, and its 98 sub-categories. There is no reference in the technical report to the Framework for Improving Critical Infrastructure Cybersecurity.

The framework international strategy is a dual path strategy. One path is to engage in the standards of development organizations such as ISO and others. The other is a bilateral national dialog. NIST has been supportive of the ISO development of ISO Technical Report (TR) 27103. They're working on a technical specification about important properties for national cybersecurity frameworks. A national framework ought to consider the importance of a risk-based approach that accounts for organizational objectives, cybersecurity requirements, and threat and vulnerabilities associated with the technical environment. These properties are under consideration for what would likely be Technical Specification 27101.

ISO is going through an update of some of their publications. Technical Reports 27001 and 27002 are up for update. There's an ongoing dialog about the extent to which the Cybersecurity Framework will, or will not, be featured in those ISO publications.

The nation count for the framework is well above 30 currently, including participation in related work products. Others are not the result of our direct collaboration including the

following countries: Italy, Japan, Israel, Bermuda, United Kingdom, Ireland, Uruguay and others. Portugal does not have a work product yet, but they're big on their framework. Work products exist in the Philippines, Malaysia, and the Ukraine. Uruguay is on Version 4 of its work product.

Uruguay's is notable because it was a government-based work product only, but recently released it out to their healthcare sector. They retooled it in concert with industry and released that to their healthcare sector. A key author of that work product will be at the workshop next week.

NIST has been supportive of the Financial Services Sector Coordinating Council's cybersecurity profile, which was released in version 1.0 on October 25, 2018 in Washington, D.C. The event was attended by organizations such as: HSPC, Focal Financial, City Group, Synchrony, First United, and USAA. All spoke about their cybersecurity framework use, and all talked about the importance of that work product in regulatory harmonization, and regulatory efficiency.

Mr. Barrett sat on a panel with representatives of the Federal Reserve Board, Securities and Exchange Commission, Office of Control of Currency, and the Federal Deposit and Insurance Corporation where those regulators were affirming that this profile is a reasonable way for regulatory compliance to be expressed to them, and to their assessors. It was an important step forward, relative to regulatory harmonization of financial services sector, something NIST has supported.

Small business is a focus. NIST continues its collaboration with the DHS Voluntary Program, the Federal Trade Commission (FTC), and the Small Business Administration on developing and extending small business resources. One of the key work products with the DHS Voluntary Program is an extrapolation of the implementation tiers of the Cybersecurity Framework, with a little bit more explanation of what a progression would look like for small businesses. The implementation tiers are broken down into eight smaller steps. There are specific referrals to work products that will help with each step.

DHS collaborated on the small business work product. The FTC provided videos and written materials for small business. NIST has been active in participating in videos and written materials with the FTC. Some of them may become NIST work products.

Looking forward, the work becomes less from the NIST perspective, and more about users. Sharing success stories will continue. The informative reference series will also continue because it is about things that parallel with the Cybersecurity Framework. These things are often managed outside of NIST. The draft version 1.1 road map needs to be finalized. Feedback we've received so far indicates the road map items themselves won't be changing. NIST guidance will be finalized on federal implementation of the Cybersecurity Framework. That document is in draft. We're also going to resume working on profiles to help small businesses reduce the time to customize the Cybersecurity Framework.

Internationally, Arabic and Portuguese translations of the Framework are underway. NIST will be publishing an official Spanish language translation of the framework in the near future. More than 10 percent of businesses in the U.S. are run by Spanish-speaking parties. There are 4.2 million businesses owned by Spanish speaking individuals in the U.S.,

contributing $660 billion annually to the American economy. They are an important part of the U.S. economy.

NIST is continuing its work of measuring cybersecurity. The most likely path will be a request for information to explore other people's perspectives on measuring cybersecurity. An important step will be to subdivide the topic of measuring cybersecurity in a logical way.

Future work on roadmap items includes governance and enterprise risk management. Specifically, better explaining how cybersecurity factors into enterprise risk management, better distinguishing between types of governance such as how they differ, how they need to align, etc., achieving better engagement with the Cybersecurity Framework at the officer level, secretary level, and in the broader federal government.

NIST Update

Matthew Scholl, NIST Kevin Stine, NIST

The Chair welcomed Mr. Mathew Scholl and Mr. Kevin Stine of NIST to the meeting to update the Board on recent NIST activities. The Board heard about NIST's activities in the quantum realm. NIST continues to work on quantum-resistant cryptography. In early FY19, the initial down select of the first set of quantum resistant algorithms will be ready to evaluate. The evaluation will be on how resistant they are against cryptanalysis and what protocols they work best in, their efficiency, and how agile they are.

NIST will be starting discussions regarding finding places within infrastructure sectors where current implementations need to be replaced. Dr. Williams believes there is time to do this work. There's a lot of trepidation about what to believe in terms of timelines for negative quantum events occurring. NIST is currently on track for having a standardized set of rules on quantum cryptography sometime between 2022 and 2024, which it believes is the target timeframe.

There were 69 initial algorithm submissions from 6 continents, 16 countries, and 26 states for the opening round of the competition. The goal is to have a suite of tools, consisting of more than two, but less than ten. There will be some tools that will be appropriate in some places but not in others. There should be some redundancy because it's not known what quantum machines will be able to do. The final algorithm selection needs have some redundancy just in case something crops up that we don’t know about now.

The other quantum cryptography issue that Dr. Williams highlighted was in the area of talent and people. NIST continues to build personnel strength in data science and bringing together people in interdisciplinary areas. There is a need for computer scientists, physicists, material scientists, and data scientists to form a research bench that’s going to be ready as this goes forward.

NIST has the ability to create an environment where people who do this type of research want to come to NIST because it's groundbreaking research. NIST has Nobel Laureates who have been working on this for a long time. There are over 700 associates, researchers, and staff within ITL.

There is a mathematics division within ITL that is now building up staff strength in

quantum mathematics. They're starting to put together classified quantum algorithms and are looking at them from a mathematical perspective to see how it affects cryptography as well as modeling capabilities. Mathematics is a gap area that needs to addressed now so that the research capabilities exist going forward, not just in physics but in IT. NIST is partnering with the University of Maryland on the Quantum Information Computer Science Institute (QuICS) to work on quantum information science.

The new cybersecurity national strategy put out by the White House contains a brief statement that says the U.S. government will identify, plan, and be ready for the post-quantum cryptographic transition. The transition will be the one place there may be a natural migration through product evolution, or a Y2K-type effort.

For the classified community, it's a much more difficult conundrum because of its immediate requirement for keeping information secret. For any classification requirement there's a store and wait effect, which makes their effective quantum day 20 years from now. NIST needs to have something ready well before that day comes. The current timeline is to be ready between 2020 and 2022. The first order will be to those national security systems that need that type of forward capability. Prioritization needs to be looked at generally, to determine what things need to be first and figure out how to roll it into the rest of the infrastructure.

Industry is incredibly eager to work with the algorithms being researched by NIST. They're eager to do it because there may be some misunderstanding as to what the actual threat timeframe is and wanting to be first to market with any quantum computing tools. NIST wants industry to wait because the tools are not final and the final list of five hasn't been decided on. Industry is looking forward to that time when they can start to work on the algorithms. NIST anticipates classic and quantum cryptography will need to exist at the same time. There must be backwards compatibility. The lab is currently updating some of its testing and conformance protocols, especially for cryptography.

Mr. Stine and Mr. Scholl have been working on updating some of NIST's identity management programs, including relooking at PIV card specifications. The updated process will be opened for new comment, followed by doing PIV cards in the next year or two. NIST also will be looking at evaluating other commercial identity mechanisms that can integrate that will be interoperable with NIST systems. It means if an applicant comes into the federal government where their information is in order, and there is an acceptable alternative form of identity proof; that alternative proof could also be used in a government product, service, or technology that may not be PIV-friendly. There are products in the government that are not PIV-friendly like phones, tablets and network appliances that may be more applicable to these other types of strong identity mechanisms that we ought to make use of.

NIST is continuing research in software security vulnerabilities. NIST would like to extend and expand the National Vulnerability Database to potentially tag software libraries to prevent reuse of bad code and relate that to exploits. There is potential for better metrics and to potentially flip how metrics and vulnerabilities are used, in order to make it more outcome-based rather than numeric. People should be applying context to vulnerabilities, rather than taking a NIST raw score. Work will continue on tools and capabilities to help

develop more meaningful vulnerability information in the future.

NIST brought in an IBM Watson instance, and built an AI model to train it to the vulnerability dataset. We're running vulnerability scoring generation through the Watson AI engine. The results are being analyzed in parallel with human output and comparing the results. It's been in process for a couple of months now. The current model looks like its tuned pretty well, so that if a vulnerability meets a certain set of recognizable criteria, the AI scores it. If the criteria aren't met, it kicks it to an analyst. The AI is working with things where the patterns and vulnerabilities are familiar. The machine and the analyst each score the vulnerability. We check the results. If it looks good, it's posted. We're starting to introduce more automation into the scoring system. As we do that and increase confidence, we need to externalize the process onto the vulnerability owners and have them start to generate scores themselves and be cross-checked by a consortium to keep it honest using these tools prior to open publication.

There is now a process where permission is given to organizations or even companies to declare their own CVEs and feed those into the system. The process is starting to federate out. Microsoft, Oracle, Cisco, and organizations that do vulnerability analysis first, now do it themselves. They can generate their own CVEs and populate the CVE database.

The thing we've been seeing recently, which I think has been alluded to, is the case where a single vulnerability may impact multiple vendors, where there were too many vendors in how you coordinate and so on. That's a hard problem.

Other updates include the 11th annual Safeguarding Health Information Conference with HHS, Office for Civil Rights, Building Assurance through HIPAA Security and Privacy Authority. The event seems to grow year after year in-person, and exponentially in webcast participation. Increasingly, the types of organizations participating, are the small provider practices. It speaks to the availability and accessibility of different types of resources; not just the publications, but the different types of events that are low cost or no cost or that can help improve the accessibility of these types of events and resources to the entire small business community. It was exciting to have that type of turnout online for that event and getting the feedback. It's been generally positive.

On November 6-7, 2018, in parallel with the Cybersecurity Risk Management Conference in Baltimore, is the annual NICE Conference in Miami. It is being hosted by Florida International University with their partner, New America, and working with Rodney Peterson and the NICE team. The title of this one is Innovations in Cybersecurity Education, Training, and Workforce Development.

November 13th and 14th will be the first workshop on smart grid cybersecurity, specifically focusing on cybersecurity for the smart grid. The purpose is to get stakeholder input to help shape our characterization of smart grid cybersecurity risk solutions and gaps. There will be discussion focusing on interoperability, risk profiles for smart grids, devices, services, and security and communications methodologies.

NIST participated in DC Cyber Week October 15-19th. It's an annual free event, open to anyone. Registration is requested for a better estimate of who might attend. There were probably 80 to 90 participants, a majority of those were students who came from colleges

in the Baltimore and DC areas, with other students as well. There was a lot of energy and excitement. Having that many students take the time to come to an event that was, in some cases, an hour or more away, to spend a few hours at the event was pretty exciting. NIST participated the last two years and if they do DC Cyber Week again, NIST will participate.

Ms. Lefkovitz provided an update on the Privacy Framework and Ms. Megas talked about NIST IR 8228. IT was one of those work products that was initiated out of an interagency group chaired by the National Science Center (NSC) a couple years ago to get a sense of the different standards and activities related to IoT cybersecurity. The IR should be out within the next few weeks in final form. We expect it to be updated periodically going forward.

A lot is happening in the context of the Cybersecurity Framework. Since the Board last met, the Small Business Cybersecurity Act was passed. NIST is looking at how to work with the broader community, partnering with other agencies, taking advantage of the industry efforts, and helping to raise awareness that these types of resources exist for small businesses.

NIST is working with DHS, and FTC is increasing its small business activities. We co-developed and co-branded one-pagers and other simple materials related to small business cybersecurity as well. We are working with other parts of NIST such as the Manufacturing Extension Partnership (MEP) program, which has a focus on small manufacturers, to help them improve their cybersecurity.

We are working with the Baldridge Performance Excellence Program. Increasingly, other technical laboratories and engineering laboratories are working with us specifically to develop control systems, tools or references for small businesses.

At the National Cybersecurity Center of Excellence (NCCoE), there are about 40 National Security Education Program (NSEP) partners. DigiCert recently joined. They are a digital certificate provider not just for people and organizations, but also connected devices. NIST is excited to have them as an NSEP partner at the center. The second new partner is Micro Focus, an HP Enterprise spinoff.

We've initiated a lot of new projects at the NCCoE. There's been more frequent releases of different types of publications. The practice guides have been released over the last several months. New projects have started including one in identity and access management for smart home devices.

There is broader ITL program participation on AI. There's a newer effort looking at some of the current innovative ways to secure AI architecture, valuing, developing an ontology or taxonomy for talking about AI, as well as security capabilities.

Data and confidentiality continues to be an area of interest. We have some numbers coming from our data integrity projects that examine different ransomware use cases. NIST also announced the technology partners and creative collaborators that will be working on the securing picture archive and communication systems.

Additional priority areas for this year include IoT relating to the infusion pump work. Some of the work related to current projects will continue to revolve around IoT mitigation strategies in DDoS. There are projects in federation with the Federal CIO Council, in the early stages looking at our advanced network technologies. The other networking piece

will be a zero-trust networking project. We are working with and through the CIO Council on that. There was an inner-agency workshop on zero-trust networks that helped to scope the project.

B-R-E-A-K

Board Review and Discussion

Chair and members of the ISPAB Board

The Board reviewed the previous two days of meetings. Mr. Boyer will be stepping down as Chair but will continue as a Board member. Mr. Lipner has offered to assume the role of Chair starting in March, 2019. He is looking forward to working with the members and returning to more active work with the board. It is an opportune time to do so.

Major takeaways from the previous two days include:

1. The national quantum strategy and the budget for quantum research.
2. The Moonshot Report was published this week. It talked about other technologies that underlie our ability to make leaps in security including quantum and augmented intelligence. That's the idea of artificial intelligence but a human being that's involved as well.
3. 5G network enhancements. Looking to enable a 10-year or forward-looking security project involving security and privacy particularly so that privacy concerns are considered as we try to solve this issue.
4. The Board wishes to hear more on the law enforcement exceptional access discussion. The Department of Justice has spoken to the Board in the past. The board is interested in ensuring we have DoJ come back and talk more about this area.
5. The Botnet Report from NTIA is coming out in draft. It will be released in the next couple weeks.
6. The Supply Chain Taskforce will kick off November 15th. The National Risk Management Center had its kick-off meeting November 1, 2018. There will be updates on where each these projects are in the next week.
7. An additional update on 5G and GPS security.
8. An IoT update and a Privacy Framework update.
9. The OMB Cloud Smart Initiative was mentioned may be a potential area to revisit.
10. An update on quantum work. Moonshot Security Engineering and the Risk Management (SERM) taskforce and NTIA response.

The Board's next meeting will be in March, 2019. A tentative request for March 21-22, 2019 will be sent to the Board, and a final determination will be made at a later time.

Meeting Recessed

The Board recessed at 3:32 p.m., Eastern Time.

List of Attendees

Last Name	First Name	Affiliation	Role
Scholl	Matt	NIST	Presenter
Brewer	Jeff	NIST	DFO
Barrett	Matthew	NIST	Presenter
Doscher	Megan	NTIA	Presenter
Monette	Emile	DHS NPPD	Presenter
Lefkowitz	Naomi	NIST	Presenter
Kneidinger	Mark	DHS	Presenter
Johnson	Chris	NIST	Presenter
Megas	Kat	NIST	Presenter
Halas	Michael	NSC EOP	Presenter
Stine	Kevin	NIST	Presenter
St. Pierre	James	NIST	Presenter
Eisenberg	Jon, Dr.	Computer Science and Telecommunications Board	Presenter
Williams	Carl, Dr.	NIST	Presenter
Barrett	Matt	NIST	Presenter
Drake	Robin	Exeter Government Services	Staff
Salisbury	Warren	Exeter Government Services	Staff
Heyman	Mat	Impresa Solutions	Visitor
Kerban	Jason	Department of State	Visitor
Coyle	Paul	Wiley Rein, LLP	Visitor
Menendez	Carmen	Self-Employed	Visitor
Mathis	Paul C.	Crowell &Moring, LLP	Visitor
Leonard	Matthew	GCN/FCW	Visitor/Media
Gruden	Michael	Crowell &Moring, LLP	Visitor
Marres	Joseph	Nextgov	Visitor/Media

Last Name	First Name	Affiliation	Role
Baker	Mariam	Inside Cyber	Visitor/Media