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

October 14 and 15, 2020

Virtual Meeting Platform: BlueJeans

Board Members	**Board Secretariat and NIST Staff**
Steve Lipner, SAFECode, Chair, ISPAB Douglas Maughan, NSF Brett Baker, NRC Akilesh Duvvur, IBM Brian Gattoni, DHS Marc Groman, Privacy Consulting Arabella Hallawell, NETSCOUT Systems Phil Venables, Goldman Sachs	Matthew Scholl, NIST Jeff Brewer, NIST Caron Carlson, Exeter Government Services LLC

Wednesday, October 14, 2020

Welcome and Opening Remarks

Steve Lipner, Chair, ISPAB; Executive Director, SAFECode

The Chair opened the meeting at 10:04 a.m. ET, welcoming everyone and providing a brief overview of the agenda and ground rules. On the agenda are bug bounties and vulnerability disclosure policies, updates from NIST on quantum computing and cryptography, and more. He noted that he is serving on the National Academies' Committee on the Future of Encryption. There are a lot of moving parts in that space, and he appreciates that it is on the meeting agenda.

The Chair said he received a positive response to the Board's recommendation on standards language. He re-emphasized the importance of Board members engaging with the speakers.

- Board member Arabella Hallawell noted companies are accelerating their digital transformation projects. She is interested in the impact, on both the federal and commercial sides, of the uptick in remote working. Has the pandemic accelerated this domain, and what does it mean for how we approach cybersecurity?
- Board member Doug Maughan said the National Science Foundation announced the first Phase Two Convergence Accelerator awards to nine research teams. They announced awardees for the 2020 cohort for research in quantum technology and artificial intelligence, and they issued a Request for Information on future topics for the Accelerator.
- Board member Marc Groman said he finds Ms. Hallawell's comment alarming. Speed and doubling down do not usually constitute the best approach to digital transformation. Also, he is focusing on disinformation and misinformation and is curious if NIST will be looking at this.

  The Chair noted that there will be a security and privacy update from NIST later in the meeting.

- Board member Brian Gattoni said he looks forward to the vulnerability disclosure conversations. CISA published an advisory on attacking the vulnerability chain. He reminded everyone that October is National Cybersecurity Awareness Month, so the time for amplifying that message is great. They continue to emphasize to network owners and operators that the basics matter when it comes to security.
- Board member Brett Baker said the IG community is paying attention to privacy, security, and the pandemic response environment and remote work. There are cloud aspects to it, and they're looking at it from a testing standpoint as well. There's a lot more work in blockchain.

ITL Welcome and Update

Dr. Charles H. Romine, Director, Information Technology Laboratory, NIST

The Chair welcomed Dr. Charles H. Romine, Director of the Information Technology Laboratory at NIST.

Dr. Romine thanked the Chair for his leadership and the Board members for their service. Mentioning that it was World Standards Day and the 50th anniversary of a date dedicated to recognizing the importance of standards, he said that nearly 100 people in ITL work on standards. He announced that NIST Cybersecurity Expert Donna Dodson received the 2020 Samuel J. Heyman Service to America Medal in the Safety, Security and International Affairs category. It is an incredibly prestigious award and well-deserved after Ms. Dodson's lifetime of dedication to service and making a difference. He then turned to an overview of ITL's current work:

- **Privacy Framework**
  - *Growing a Workforce for Managing Privacy Risk Workshop* was hosted by the International Association of Privacy Professionals September 22-24, 2020.
  - Microsoft published GDPR Crosswalk, by the Enterprivacy Consulting Group (ISO/IEC 27701).
- **Noteworthy Releases**
  - SP 800-53 Rev 5: Security and Privacy Controls for Information Systems and Organizations
  - Cybersecurity Telework Resource Page: It is important to acknowledge that the work environment and cybersecurity risk have changed.
  - NIST began validating cryptographic modules to FIPS 140-3, Security Requirements for Cryptographic Modules
  - Draft Workforce Framework for Cybersecurity (NICE Framework update)
  - SP 800-207 – Zero Trust Architecture
  - SP 800-211 – Cybersecurity Program Annual Report

  The Chair asked about telework resources and the current environment. It seems like we're getting a lot of forced experience trying secure approaches to telework. Are there experiences with things that have gone wrong or could go better? Is NIST working with DHS to look at lessons learned?

  Dr. Romine said yes. Some of the input is from the community at large. Early on with the use of teleconference software, there was a fairly regular occurrence of "Zoom bombing" – with any of the various teleconference platforms – all are vulnerable to bad actors. As a result, they are providing resources on secure teleconferencing. They have had conversations with DHS and other entities on best practices for remote work.
- **Responsible Use of Positioning, Navigation & Timing (PNT) Services**
  The Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services was issued in February 2020. It directs the Department of

Commerce and other agencies to work with the private sector to identify and promote responsible methods of using PNT services that appropriately manage risks.

Cybersecurity Profile for the Responsible Use of PNT: A draft annotated outline was issued August 31, 2020. A workshop was held September 15-16, 2020. A draft profile for public comment is expected in mid-October 2020.

- **Cybersecurity for the Internet of Things (IoT)**
  NIST worked on several documents, including:
  - NISTIR 8259 *Foundational Cybersecurity Activities for IoT Device Manufacturers* ensures that the devices that manufacturers sell have the capability to deal with cyber risks. NISTIR 8259A *IoT Device Cybersecurity Capability* is the core baseline.
  - The Federal Profile of NISTIR 8259A *Catalog of IoT Device Cybersecurity Capabilities* was published on GitHub.
  - A workshop on Cybersecurity Risks in Consumer Home IoT Products was held Oct. 22, 2020.
- **Industries of the Future**
  There are several areas where the administration, in concert with the private sector, has identified what are being called "the industries of the future," and ITL is involved in all of them. ITL partners with the Physical Measurement Laboratory on quantum information science, with the Communications Technology Laboratory on 5G and advanced communications, and with the Material Measurement Laboratory (MML) on the bioeconomy – or biotechnology – to improve the measurement science underpinning biotechnology. There is a vigorous program on artificial intelligence, particularly the promotion of trustworthy AI, and NIST has long been a key component in work on advanced manufacturing. There is a tremendous amount of activity cutting across all of these areas, using risk management associated with each one.
- **Encryption**
  - Post Quantum Cryptography: Round Three selections have been completed.
  - Lightweight Encryption: The Fourth Lightweight Cryptography Workshop was held virtually Oct. 19-21, 2020.
- **Trustworthy AI**
  NIST develops vocabulary and measurements needed for technical requirements of trustworthy AI.
  - A *Bias in AI* workshop was held August 18, 2020.
  - NISTIR 8312 *Four Principles of Explainable AI*, public comment period Aug. 17-Oct. 15, 2020.
  - Secure AI: NISTIR 8269 Terminology and Taxonomy; Final draft expected in the fall.
  - Dr. Romine participated in a trilateral call with the U.S., Japan, and the E.U., looking at AI and the background needed to establish an appropriate regulatory framework. NIST supports the measurements, standards, and vocabulary to support the policy makers who will establish AI regulations if warranted.
- **Novel Computational Paradigms for AI**
  - Establishing metrics and benchmarks for AI hardware
  - Foundational analysis of the computational capacity of a physical system
  - Analysis and development of algorithms for spike-based computation
- **Upcoming Symposium: U.S. Strategy for Resilient Manufacturing Ecosystems Through AI**
  Hosted by the National Science and Technology Council (NSTC) Subcommittee on Advanced Manufacturing and Subcommittee on Machine Learning and Artificial Intelligence: They are proposing three workshops, and there will be an opportunity to combine areas of expertise that haven't overlapped much in the past.

- **The Phish Scale**
  NIST developed a new method called the Phish Scale that could help organizations better train their employees to avoid phishing.

- **Biometrics**
  - NIST has undertaken the most comprehensive and accurate assessment of the accuracy of current facial recognition by assessing a database of millions of faces.
  - NISTIR 8311, Face recognition accuracy with face masks using pre-COVID-19 algorithms.
  - The next report will document accuracy values for more recent algorithms, some developed with capabilities for recognition of masked faces.

- **In 2022, NIST will celebrate 50 years of cybersecurity research.**

- **Q&A**
  - Mr. Groman said he was fascinated by the Phish Scale project and would love to hear more about it as data comes in, looking at lessons learned from other contexts. It might be novel in its simplicity – why haven't we taken this approach in such a methodical way before?

    Dr. Romine said he doesn't know of other research organizations that have sociologists, psychologists, and others from various fields working on cybersecurity. He is interested in how they shed light on practical implications in cybersecurity. His goal with the usability team at NIST is to take advantage of their deep understanding and scientific approach to quantitative and qualitative testing and use it to prioritize efforts in the cybersecurity arena. The popular concept years ago was to blame the user. They didn't really want to hear about the challenges. There's a lingering effect of the blame-the-user habit. The mantra ITL uses is: Try to make it easy for users to do the right thing, hard to do the wrong things, and easy to recover if the wrong thing happens. They would like to strengthen the ties between the usability team and the core cybersecurity team.

    Mr. Groman said there have been options to limit access or require longer passwords to improve security, but there was pushback from the higher-ups because the additional steps interfered and took another minute of time. He is wondering when we will get to the point that we may have to require someone to take one more minute to log in.

    Dr. Romine said it is important to understand the context, and he offered two illustrations. The usability team worked with the FBI's hostage rescue team, which goes into conflict theaters. Sometimes they must undertake a biometric scan of someone who is either uncooperative or dead. They wear a lot of gear and are potentially under fire. Authentication takes a long time because they have to take off their gloves, etc. In the second illustration, they heard about physicians who need to make a consult on an emergency basis, and they need to share data with a colleague. They take out their smart phone and snap a picture, violating every tenet of HIPAA in order to save someone's life. If done right, there can be both usability and security.

    The Chair said this is a rich area for improvement. The end result should be guidance that developers can consume without having to depend on resources they don't have.

  - The Chair asked if Dr. Romine would discuss the Board's letter regarding standards language.

    Dr. Romine said he was grateful to spotlight what NIST was already doing in this arena – searching for language that was inappropriate or loaded. NIST Director Copan received a letter from the Chair asking for an update and applauding the efforts NIST was taking, a comprehensive review of every document. They started by collecting examples of language they could search for and then identifying areas where language used was not carefully thought through. Processes are changing to avoid using language that is loaded. This undertaking is extensive – there are a lot of documents, and the effort is still in the preliminary stage. The amendments that are likely to come

out as a result of this analysis phase will come out over the course of time. They are very pleased about the input from the Board on this issue. One of the four core values at NIST is inclusivity, and it's important that they live up to it.

The Chair congratulated Mr. Venables for having raised the topic at the last meeting.

Mr. Venables said it was pleasing to see the progress being made.

The Chair announced a 10-minute break.

Bug Bounties and Vulnerability Disclosure in the USG

Alyssa Feola, Cybersecurity Advisor, Technology Portfolio, GSA

The Chair welcomed Alyssa Feola, Cybersecurity Advisor for the Technology Portfolio at GSA.

Ms. Feola introduced herself, offered an overview of her career, and described the bug bounty program underway at GSA.

The mission of Technology Transformation Services (TTS) at GSA is to improve the lives of the public and public servants by transforming how government uses technology. They help agencies make their services more accessible, efficient, and effective with modern applications, platforms, processes, personnel, and software solutions. They have multiple consulting arms, including the Presidential Innovation Fellows that started in 2012, other consultants, and the Centers of Excellence.

TTS's Vulnerability Disclosure Policy, available on the website, is used to manage the TTS Vulnerability Disclosure Program and Bug Bounty Program. They were early adopters of federal crowd sourced vulnerability disclosures.

- **Background on Bug Bounties**
  - The fundamental challenge of a security program is: How do we find security issues before an attacker finds them?
  - Bug bounties reward independent researchers who discover and responsibly report issues.
  - Bounties are a proven cybersecurity risk reduction tactic. In the private tech sector, most mature security programs include a bug bounty.
  - Operating a successful bug bounty is technically challenging and expensive. Platforms ease the difficulty and do so at a lower total cost.
  - In TTS and GSA in general, they have embraced the risk management framework.
  - They considered alternatives before jumping into software as a service solution. They considered developing their own platform or using a network of researchers from government or having people within their organization do some of the development. It didn't make sense to make their own platform when there was a commercial solution available that they couldn't replicate. In-house also wasn't feasible because they wouldn't get the breadth of skills.
- **Components of the Bug bounty Program:** Platform network access; Triage services; Bug bounty

  Some products within their product line do not end up generating vulnerabilities that have a bug bounty. There are others that are more experimental, delivering more features, that end up getting more bugs with related bounties.

  They elevated the ability within the platform for folks experienced in triaging bugs, so they can quickly identify if something is not applicable, informative, valid, or new.
- **Lessons Learned**
  - Staffing: At first, they had consultants do a rotation, and after a reorganization they went with a codified role and responsibility with dedicated workers. There were pros and cons with each

option. A fresh set of eyes in the rotation was good. On the other hand, dedicated staff could notice trends and establish communication with researchers and others.
- Directory: If external folks find a vulnerability in any .gov website and report it to TTS, if it's not in their scope, they can't triage it the same way. They are fortunate with the consultancy they have with other federal agencies.
- Level of effort and volume: You need dedication and prioritization.
- Better tracking: One of the biggest lessons is that it's best to start with a baseline – a manageable number of assets added into the bug bounty program. You can increase as you go and incorporate lessons learned. It's good to have a dashboard that keeps track of your reports.
- Scope: The clearer and more concise the better. They are working on getting the right verbiage for denial of service attacks. If the site is vulnerable to a DoS attack, they want to know. You need to take into consideration how to scope things for the private and public users. They have a lot of development and test environments on GitHub and have started incorporating lines and comments for the security researchers. The whole activity is something they are proud of. They have blog posts and have been featured in news articles. Having the chance to engage with the community of researchers and other federal agencies is what they feel is going right.

Challenges remain around governance. As a child organization within GSA, how do they work the mechanics for GSA overall to start this program? Also, there are so many other tasks to address, attention to the bug bounty program fluctuates.

- **Q&A**
  - The Chair said he has been peripherally involved with bug bounty programs. One of the things he's observed is that a bug bounty can be a way to pay people to find your mistakes and then you fix them one at a time. Alternatively, it can be a way to get amplification of the security capability of the people looking at the products and systems you're building and get feedback on the way you build them. He asked how TTS is conducting the feedback process and integrating the findings into development or operations.

    Ms. Feola said right now it is done as bugs occur on a per system basis. They might have one program that is good about sharing findings with other programs. Login might say, hey Cloud, we found this, and you should check for it too. But that's not an activity they are forcing each of their systems to do. They have a channel for sharing and dedicated biweekly meetings, but there is no set agenda topic. The programs are kind of siloed in how they do their own operations and security. They have different business objectives and priorities. If they have a contract turnover, for example, does the new cohort of developers potentially impact the number of bugs found in the wild?

  - The Chair asked if they are confident their developers are updating their tools, processes, and training to keep from making the same mistake over and over again.

    Ms. Feola said that she is positioned to notice if something keeps reoccurring. They're not seeing that too much. There are times when researchers find the same vulnerability at the same time.

  - The Chair asked about cross-site scripting and if they are seeing repeated incidences of similar kinds of errors or just one-offs.

    Ms. Feola said they take steps to keep from seeing repeated errors.

  - The Chair asked about whether a report goes into the testing process before a future deployment.

    Ms. Feola said they do remediation within a reasonable amount of time based on the criticality of a bug. There have been instances where they did a fix and it opened up a hole from before. It is not as if they are seeing an instance of cross-site scripting across the board.

- Mr. Gattoni pointed out a question in the chat: Many agencies don't yet have a VDP or a bug bounty. What proportion of reports aren't *for* TTS, and what do you do with those?

  Ms. Feola said they get at least two of those a month. They have been trying to submit them through the software as a service platform to help find the right points of contacts. Usually they use personal connections to find the appropriate points of contact.

The Chair announced a 1-hour lunch break.

DHS Binding Operational Directive 20-01 Develop and Publish a Vulnerability Disclosure Policy

Mike Duffy, Deputy Associate Director, Cybersecurity Division, Cybersecurity and Infrastructure Security Agency (CISA), DHS; Cameron Dixon, CISA, DHS

The Chair welcomed Mike Duffy, Deputy Associate Director of the Cybersecurity Division at the Cybersecurity and Infrastructure Security Agency.

- **BOD 20-01 Overview**
  - BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy (VDP)*, was issued September 2, 2020, by the CISA Director to all federal civilian agencies. It involved well over a year of planning, inter-agency discussions, public comment period, and industry engagement. They are at the starting line when it comes to a whole-of-government approach to this.
  - The directive aligns with OMB M-20-32 on coordinated vulnerability disclosure, and it supports the implementation of NIST standards: The directive was written specifically for how federal agencies can think through this policy and build it into their own processes. It is also written for the wider community. It was the culmination of a year of work with OMB, CISA, other agencies.
  - The directive helps standardize and establish a consistent approach across 101 different agencies and seeks to gain the benefit of all agencies working together for a "unity of protection."
  - Key Actions:
    - Set a security contact for each .gov domain within 30 business days of issuance. Due Oct. 2.
    - Publish a VDP and maintain handling procedures about how to incorporate it into an agency's process within 180 calendar days of issuance.
    - Expand VDP scope quarterly by 270 calendar days. Within 2 years, full scope.
    - Report metrics to CISA.

    Prior to 2020, they had one emergency directive, and in 2020 there were three. They are pleased with how the government as a whole was able to respond. One thing they need to look at is unsolicited reports that come from the wider community.

- **Why a Directive?**
  - "It shouldn't be hard to tell the government about a cyber issue." Collective cybersecurity is strongest when the public is part of the process and can contribute. CISA wants to make sure there is consistency in the way to apply the principles and lessons learned.
  - Benefits of Unifying and Standardizing Vulnerability Disclosure: It is helpful when they can set expectations and provide encouragement for some in government who weren't planning to follow certain steps. Few agencies had a VDP posted prior to FY2021.
  - Address the need and develop the roadmap ourselves (as a Federal Cyber Community): There are benefits to having the role of facilitator, identifying and sharing use cases from peer agencies, and establishing thought leaders across government.

Cameron Dixon added that many agencies do not have a VDP. Part of the BOD's strategy is to develop the organizational muscles for agencies to remediate on their own.

The Chair said in the old days the default place to report vulnerabilities was CERT/CC at Carnegie Mellon. The process added latency and probably reduced some of the pressure on the independent organizations to do the right thing. However, the central focus did provide a common collection point for lessons learned, trends, community-wide problems, and it encouraged vendors to be responsive. The agency vulnerability reporting strategy is the right one in terms of scale and timeliness, but are they getting the common picture of trends and lessons learned?

Mr. Dixon said that asking whether CISA is still in the loop is a fair point. They will try to collect information to allow agencies to aggregate some of the data, at least on their response abilities. There are some fundamental trade-offs here. Many agencies are not the first party providers of their infrastructures. Allowing agencies that are required to manage and maintain their systems to be in the driver seat and empowering them feels like the right call.

- **Public Draft and Engagement**
  - Summer 2019: Initial draft discussion with Federal CISO Council
  - Draft BOD 20-01 Public Comment Period
    - Posted November 27, 2019.
    - It was the first time CISA publicly issued a directive in draft.
    - They received 220 individual comments from 42 unique sources.
    - They had roundtable sessions with agencies and organizations. Many mentioned that their general counsel said they didn't think it wasn't time for a VDP, and others said their general counsel said it's a brilliant idea that should have been done years ago. Some said they didn't want people poking around their legacy systems. Some asked whether the VDP would just be inviting more vulnerabilities.
  - Coordination across interagency partners, including OMB, GSA, DOJ, DOC (NIST, NTIA), and the CISO Council. Mr. Dixon said that many agencies were concerned about the line between authorization and invitation. They included a lengthy FAQ to address the concerns upfront. Soliciting information from the public allowed them to expand the guidance.
  - Though the required actions and scope remained relatively the same, public comments significantly shaped the associated implementation guidance and CISA support approach.

- **CISA Support**
  - Templates and reference materials: Publicly posted implementation guidance, FAQs, and templates at https://cyber.dhs.gov.
  - Technical assistance and frequently updated information: Hosting interagency webinars and stakeholder roundtables with leading agencies and providing technical assistance when requested.
  - Central 'Vulnerability Disclosure Platform' Shared Service: They are planning to offer federal agencies a service via the CISA Quality Services Management Office (QSMO) to ease discoverability for researchers, reduce handling load for agencies, and automate metric collection.
- **Current Progress**
  - First Deadline: Set a security contact (10/2/20) – This is well over 90 percent complete across federal agencies – over 1,000 domains.
  - Next Milestone: Publish a VDP and handling procedures (3/1/21) – Many agencies are bringing in legal and policy departments. Many have started working groups and cross-functional teams.
  - Early Observations:
    - Many agencies are initiating VDP development.
    - Early adopters and leading agencies can offer insights to others.
    - Internal coordination and leadership involvement are key, and this takes time.
    - Incorporating unsolicited disclosures into vulnerability management programs can help agencies determine resource needs and readiness.

- **Vision for FY21 and Beyond**
  - Enhanced vulnerability management across government
  - Hardened, more secure online services and domains
  - CISA's ability to identify common challenges and persistent issues
  - Further collaboration with security researcher community and industry: See if agencies refine their vulnerability management processes and procedures; how agencies incentivize and drive the see something/say something behavior.
  - Start a positive trend across sectors (…*if the Feds can do it*…): BODs and emergency directives are written to be applied across any sector.

- **Q&A**
  The Chair thanked Mr. Duffy and Mr. Dixon for their presentation.

  Mr. Venables asked if there is any data about whether agency employees or just external people are reporting vulnerabilities.

  Mr. Duffy said there isn't a lot of data at this point.

The Chair said there is probably more to discuss on this topic and announced a break.

NIST Activity in 5G and Beyond Security

Jeff Cichonski, ITL, NIST; Nada Golmie, CTL, NIST

The Chair re-opened the meeting and welcomed Ms. Golmie and Mr. Cichonski.

Ms. Golmie started her presentation with an overview of 5G and its promise for improved communications capabilities, including improved connectivity, higher capacity, and autonomous communications (i.e., resiliency and low overhead).

- **What is 5G?**
  When they set out to develop 5G, there were basically three pillars for use cases:
  - Enhanced mobile broadband, which involves higher data rates (more volume and higher speed)
  - Massive IoT, connecting millions of devices
  - Low Latency/Ultra Reliable communications for things like self-driving cars, industrial automation, AR, and VR.

- **4G to 5G**
  One important thing to keep in mind is that 5G is driving the latency down, from tens of milliseconds to less than a millisecond. We are going from 1 Gb/s to over 20 Gb/s. The spectrum band for 5G is lower than the 3.5 GHz, and they will do a better job sharing it.

- **5G Standards**
  To make 5G happen, it takes a large ecosystem, including 3GPP, IEEE, IETF, and ETSI.

- **3GPP Perspective: 5G New Radio**
  Mr. Cichonski said that 3GPP wanted to have carriers deploy 5G in a realistic way, by adding onto existing networks rather than ripping and replacing. They designed it with a phased approach:
  - Phase 1 (3GPP Release 15) focused on the enhanced mobile broadband component. Carriers could take advantage of increased use of spectrum and increased speeds while recognizing that there were still a lot of technical details that needed to be worked out.
  - Phase 2 (3GPP Release 16) focuses on massive connectivity/ultra-high reliability, low latency, and the overarching package of all 5G capabilities. 5G phones on the market now are primarily using a Release 15, non-standalone version without the full slate of 5G capabilities.

  There are three overarching 3GPP working groups (WGs):

- Radio Access Network WGs focus on some of the hardcore radio layer aspects.
- Service & Systems Aspects WGs lay out requirements, design the architecture, describe and define the security architecture. This is where ITL participates.
- Core Network & Terminals WGs take all the other specs and write the bits and bytes that can be implemented by network vendors.

- **The Basics of a Mobile Network**
  Devices connect to a radio access network (RAN) of base stations, which allow communications to move from base station to base station. Behind that is a core network or packet core, which handles signaling and connectivity, ultimately providing a connection to an IP network or telephony service.

- **Mobile Network Security**
  Security on a mobile network today is hop-by-hop, with different types of security provided at each hop. In the RAN, there is also access stratum security or "air interface security," which is the security from the device to the base station. This handles encryption and integrity protection of the signaling traffic and encryption of the user plane traffic. With 5G, for the first time, there is integrity protection on the link for user plane traffic.

  Another layer of security is used to secure the interface from the base station to the edge of the core network, using network domain security (NDS/IP). NDS/IP is about using IP Sec tunnels between the base stations and the security gateway that sits in front of the packet core. The packet core is a kind of data center operated by the network operator or carrier, and there is security within it.

  When using applications on devices, like iMessage, Facebook, or a banking app, there is the additional application layer security, which is end-to-end.

- **Known Security Issues with LTE**

  - Subscriber Tracking: The permanent identifier in LTE is tied to the user's account subscription and is sent over the air in clear text, making it easy for a rogue actor operating a rogue base station to capture and use it potentially for subscriber tracking.
  - No User Plane Integrity Protection: In LTE, there was no cryptographic key in the key hierarchy to enable integrity protection on the user plane.
  - SS7 Threats: Roaming attacks could be carried out on the SS7 network by rogue carriers presenting false roaming statements to legitimate carriers. Message interception is also possible.
  - False Base Stations: It is possible to set up an RF broadcast to look like a legitimate cell tower or base station and trick someone into connecting to it.

- **5G Security Enhancements**
  The goal with 5G was to improve the security posture of LTE. From a security perspective, 5G is an evolution of LTE, which itself was much more secure than previous generations of mobile networks.

  - Radio Network Security: They added user plane integrity protection, splitting out the radio node into centralized and distributed units, where the centralized unit can terminate security if you locate it to a more trusted environment.
  - Increased Visibility: You can envision an application querying an API on the network and making a decision about the security posture. If it determines that encryption is not turned on, for example, the app might force a VPN or force additional security.
  - Subscriber Privacy: The subscriber permanent identifier can be concealed and encrypted.
  - Roaming Security: Standardized application security at the roaming interface is added to protect against SS7-related threats. There is a new network function called Security Edge Protection Proxy or the SEPP, which implements application layer security for all of the services.

- Network Slicing: You can use the functional capabilities of a network, depending on what the device is trying to do, and route them to a different slice of the network, whether it's a low-latency application or a high-security application, for example.
- Authentication Enhancements: You can picture an IoT device that might not necessarily have a SIM card or an embedded SIM being able to authenticate to the network using EAP-TLS.

- **5G Cybersecurity at the National Cybersecurity Center of Excellence (NCCoE)**
  In October 2019, the NCCoE hosted an industry day and invited mobile network vendors. Nokia, Ericsson, Cisco, AT&T, T-Mobile, Sprint, IT vendors, and others presented their thoughts. They heard two main themes. First, 5G has a lot of new security features and capabilities based on the standards, fixing a lot of LTE issues. Second, 5G is going to take advantage of cloud technologies. They designed a project description focused on these two core tenets and decided to take a practical approach to make sure they are in alignment with industry.

- **Focused Security Capabilities:** Trusted Hardware; Isolation and Policy Enforcement; 3GPP Security Feature Enablement; False Base Station Protections

  They had a kick-off meeting September 23, 2020, and have a pretty impressive list of collaborators, including operators, network vendors, equipment vendors, IT vendors, and consortiums.

Ms. Golmie provided a review of NIST's efforts related to 5G:

- **Advances in Communications Metrology**
  - Public Safety Communications Research: NIST is heavily invested in public safety and making sure that communications in 5G work well for that sector.
  - Channel propagation measurement/modeling, and standards development/Antenna Measurement Facility
  - Security of advanced communications technologies and applications
  - Trusted Spectrum Testing/Spectrum Sharing Measurement
  - They operate the National Advanced Spectrum and Communications program, which is hosted by NIST but includes multiple organizations, including NSF, NASA, NTIA, and DoD. They facilitate access to facilities for testing and evaluation of very important and controversial types of scenarios with multiple applications and multiple devices sharing the space.

- **Chanel Sounders for 83.5, 28, and 60 GHz**
  About 10 years ago, NIST invested in the development of channel sounding capabilities to better understand wireless propagation in the higher frequencies. They developed the instrument, measurement data, and models that are abstracted from the measurement. NIST is interested in pushing the state of the art in the test meteorology and testing the science and developing new tools.

- **5G for Public Safety Communications**
  NIST has a fairly large program on public safety communications that started by looking at what 4G and LTE could do in the public safety arena.

- **5G Smart Manufacturing**
  This is a challenging environment from a wireless propagation point of view because there is a lot of metal in factories. For collaborative machines to work together, they need very low latency and extremely high data rates. Also, you want to be able to do precision manufacturing and correct design or other manufacturing errors on the fly. One reason people said they need wireless in this environment is that rodents eat wires. Also, wires are cumbersome and clutter everything.

- **5G mmWave channel model alliance**
  NIST started an alliance to make measurement data available to others. They host a repository of measurement data and models. They have sponsored workshops and face-to-face meetings co-located with major conferences and events, including IEEE, ICC, VTC, Globecom, NSF mmWave Research Coordination Network, and others.

- **Q&A**
  - Ms. Hallawell asked about private 5G networks and how NIST is thinking about those applications and use cases. What are the implications for control plane for 5G, and how would you deploy that on a more tactical basis?

    Mr. Cichonski said they are laying out a large catalog of security capabilities that might be available with 5G. They are probably never going to have a commercial network that allows EAP TLS authentication. Nokia is one of the collaborators interested in nonpublic networks from an industrial perspective. At the NCCoE, they are trying to build the Christmas tree before putting the ornaments on it. Some of the use cases of IoT and self-driving cars and edge computing require the Christmas tree and all the capabilities to be there first. Non-public networks are down the road, but on the radar.

  - The Chair said that security standards work has focused more on hop-by-hop systems. Now there is a focus on the importance of end-to-end security, and there are still things where hop-by-hop is important, such as paying for service and paying for bandwidth. Managing the combination of hop-by-hop and end-to-end simultaneously could be a nightmare for an administrator or security officer. Is there anything being done to make that better?

    Mr. Cichonski said the NCCoE hopes to help by educating people about what they're getting from their carrier. They want to inform organizations about the risks they need to be aware of when they're using certain applications. They want to explain how the cell networks are designed so people have an understanding of where they need to make informed decisions.

    The Chair said that, in other words, it's about users not assuming they have more security than they have so they can complement it as needed, even if it imposes costs.

The Chair asked for additional questions or comments and, hearing none, announced a 10-minute break.

NIST Cybersecurity and Privacy Update

Matthew Scholl, ITL, NIST; Kevin Stine, ITL, NIST

Mr. Stine said his presentation would focus on four themes:

- **Risk Management**
  In ITL, they want to help organizations manage risks in the context of their enterprise risk management (ERM) efforts.
  - Integrating Cybersecurity and ERM Guide (NIST IR 8286): They received a lot of feedback from diverse communities, inside and outside the federal government. The purpose of the guide was to demystify the intersection and bridge the gap between the two disciplines. They wanted to leverage familiar language and constructs, like the risk register.
  - Online training course for NIST risk management framework: This provides a video-based training on the application of SP 800-37.
  - Expect to see much greater and more meaningful integration of various risk management resources to produce a more coordinated and cohesive portfolio of tools.

- **Cybersecurity Measurement**
  - Recently they launched a focused effort on cybersecurity measurement. The objective was to develop guidelines to improve the quality and utility of information to support technical and higher-level decision-making. There are still gaps in nomenclature and taxonomy.
  - They issued a pre-draft call for comments on update on 800-55 (*Performance Measurement for Information Security*). Comments are due November 19, 2020.

- **Workforce Pipeline and Development**
  - They led a virtual workshop on growing a workforce for managing privacy risks, hosted by the IAPP. The Privacy Framework effort is meant to be complementary to their efforts under NICE. They intend to share an update on revisions to the NICE Framework on Oct. 27, 2020, when the annual NICE Conference (virtual) gets underway. The conference will take place over four half days: Oct. 27, Nov. 5, Nov. 9, and Nov. 16.
  - The annual NICE K12 Cybersecurity Education Conference (virtual) will take place Dec. 7 and 8, 2020.
  - They are also in the process of updating the NICE Strategic Plan, to be unveiled Oct. 27, 2020.

- **Transitioning to Practice**
  - There is an emphasis on helping organizations transition standards into practice. A response to a PNT executive order is included in this effort. They also updated and finalized the Cybersecurity Framework Manufacturing Profile to help manufacturing organizations improve their cybersecurity capabilities.
  - DoE announced a partnership with NIST to focus on providing practical guidance for organizations engaged in operational activities.
  - The NCCoE recently hosted three virtual workshops in the applied cryptography domain: TLS 1.3 implementation; Automating the Crypto Module Validation Program; and Helping Organizations Prepare for Post-Quantum Crypto (PQC) migration. For the PQC migrations workshop, there were well over 300 attendees.
  - In September, the NCCoE issued two final 1800 series resources: One was on mobile device security, both corporate and personally enabled. The other was a final publication on data integrity and recovering from ransomware and other destructive events.

- **Q&A**
  - Mr. Groman asked about the status of the privacy workforce initiative. The number of people attending the workshop shocked him. He was a speaker, and his LinkedIn account was flooded after the event. People wanted to know more. What were the takeaways and next steps?

    Mr. Stine said they have a good solid structure for a taxonomy that they are leveraging from the NICE Cybersecurity Workforce Framework. The NICE team and the privacy team have been working very closely together to make sure that the Cybersecurity Workforce Framework updates are also considering how privacy would be able to leverage the same schema. They are off to a great start, but there's no taxonomy yet. They were thrilled with the participation at the workshop. They are still fleshing out the immediate next steps and digesting information from the workshop.

    Mr. Groman said maybe they can talk about it more at the next meeting, and he asked about the size of the privacy team in ITL.

    Mr. Stine said the immediate privacy team includes about four to four and a half full-time equivalents. Privacy continues to be a strategic priority area and a growth area.

- **Cryptography and Encryption Activities**

Mr. Scholl said the upcoming workshop on lightweight encryption will look at use cases and applications for a lightweight cypher. At the same time, they are looking at how small they can get the Advanced Encryption Standard (AES). A report is coming out soon, looking at it from basic constructions, brittleness of modes to potential upgrades, and changes in the future.

First Post -Quantum Recommendation – SP on Stateful Hash-based Signatures: While conducting the post-quantum competition, they worked in parallel with the Internet Engineering Task Force and completed two RFCs on the use of stateful hash-based signatures.

- Testing Program
  They continue to update and refresh work on FIPS 140-3.
  - Soon they will start testing a new area dealing with entropy inputs. They developed tests that assess the randomness of initial inputs. It will go into effect next month.
  - They opened part of the crypto testing for organizations that wish to self-test rather than go to a third-party lab. Cisco was the first out of the gate.

SP 800-53 was published and is final. They took the baselines out of that document and put them in a separate document (800-53B) so SP 800-53 is a catalog now. SP 800-53B enumerates the low, moderate, and high suggested initial security baselines for systems. Comments are being adjudicated.

Mr. Groman asked why the change was made in taking the baselines out of the document.

Mr. Scholl said it would be simpler to make changes to the catalog going forward. If the baselines need to be changed, they can be changed without having to reopen the entire catalog. Baselines provide a starting package.

Mr. Groman said separating them out makes a whole lot of sense.

- **Schema for metadata for use within the National Vulnerability Database**
  Mr. Scholl said they published a schema for metadata for use within the National Vulnerability Database (NVD) for information that they would like to get with submitted CVEs. When a CVE naming authority (IT company, research organization, etc.) finds a vulnerability and makes it public, it is assigned a CVE number and put in the NVD. They want to set standards around the metadata that comes in with the CVEs. As inputs into the NVD grow almost exponentially, hiring individual analysts to keep up with it is not a path of the future, so they need more federated inputs from industry that can be trusted. There has to be a standardized set of inputs and then a method for NIST and industry to cross check. In the future, organizations will be allowed to input scores.

- **Blockchain technology**
  They continue to conduct research into blockchain technology and recently put out some documents around tokenization of blockchains and blockchain management.

- **Expanded issues of Telework**
  They put together a summary of current telework security guidance and continue work on mobility security, zero trust architecture environments, and platform interoperability.

- **Identity**
  An update to FIPS 201 is coming out soon. They are looking at the current token, PIV card, CAC card, and asking if it is the right form factor for the future. They are also interested in other types of identity – machine identity, process identity, virtual instance identities.

  Other areas they are looking at are threshold crypto, homomorphic encryption, and digital twinning.

- **Q&A**
  - Mr. Baker asked whether HHS and NSF are involved in blockchain pilots. OMB and MITRE have been working with use cases. Did they reach out to ITL?

    Mr. Scholl said they have not, to his recollection.

    Mr. Baker said that in the IG community they have been weighing in from a control standpoint. They are interested from the perspective of what you can use blockchain for with regard to oversight. If NIST wants to do something in that space, he could help tee up some contacts.

  - The Chair asked if anyone is worrying about post-quantum blockchains.

    Mr. Scholl said yes. In NIST's document about foundations of blockchains, there is a section on post-quantum and looking at signatures used in some of the blocks and whether or not they are quantum resistant. There are signatures across the board that have a potential future threat that may require re-signing.

  - The Chair said it is important that they focus on getting the relevant cybersecurity skills beyond the cybersecurity experts. It is a concern he's had with the NICE effort. They need to focus on the population that has to apply these technologies.

    Mr. Stine said he agrees. What we're really talking about is not just a cybersecurity workforce but a workforce skilled in cybersecurity. They are focusing on broadening the community quite a bit.

  - Mr. Scholl said someone had mentioned disinformation or misinformation. In his division, they are not doing a significant amount in identifying or labeling disinformation or misinformation. There is some work in information sourcing and tracking, however. The information access division has some research looking at information source and origin, especially when information has been modified or changed. But this does not necessarily go to the correctness of data.

    Mr. Groman said he is working on that subject in other government contexts. NIST's work on the Phish Scale project sparked some interest. NIST has other expertise that should be brought to bear in the area of dis/misinformation. The subject would benefit from cross-collaboration.

Public Comment

No public comments were received.

The Chair closed the comment period for Day 1.

Day's Review and Board Discussion

- Suggestions for letters and recommendations.
  - Mr. Groman said the timing is right for a short and sweet but strong letter of recommendation that the DoC, NIST, or relevant entity devote more resources to the privacy efforts. They are doing a tremendous amount of work with four people. But given the demand in this area, there is not going to be a single project that is not going to demand someone with a privacy background to weigh in. We are way behind the eight ball as it is. The letter can be as short as one paragraph and should indicate support for the work being done to date and recommend more resources be allocated.

    The Chair asked if there are guidelines about what they can say regarding resource allocation.

    Mr. Scholl said it is his understanding that this is within the scope of the charter.

    The Chair asked for feedback from other Board members.

Mr. Gattoni said he doesn't have any opposition to it, but he has seen folks coming into this subject from the legal area and Big O opinions. Down at the tactical level, when they are making adjudications in system design, data retention, etc., he doesn't know that a Big O policy approach to design decisions is the right mix.

Mr. Groman said that is exactly his point. The word "privacy" doesn't mean anything until you start looking at things like controls. There aren't enough people with the knowledge or skill set who can sit across from someone in engineering. In the absence of those experts, we are going to get people who shouldn't be doing the job – who just want to think deep thoughts and write haiku about privacy. That's exactly why he would like to increase the resources at NIST because NIST is trying to take privacy out of philosophical debates at a high level and integrate them where the work needs to be done. Privacy by design – he thinks NIST gets that more than most. He would echo Mr. Gattoni's point – the letter can point out the need for more resources in order to ensure that privacy is being addressed at the right stage by individuals who have the right expertise.

The Chair asked Mr. Groman to draft a letter overnight that they could look at the next day.

Mr. Groman said he would come up with something. The topic is misunderstood.

- The Chair said that he may propose that they weigh in on the matter of vulnerability reporting, bug bounties, and the use of vulnerability reports as a learning tool, which is something you can use for continual improvement.

  Mr. Gattoni said it was good to hear about operationalizing the data reporting mechanism.

The Chair recessed the meeting at 4:03 p.m. ET.

Thursday, October 15, 2020

The Chair opened Day 2 of the meeting at 10:06 a.m. ET.

Hardware Security Issues Overview

Dr. Mark Tehranipoor, Professor, Cybersecurity and Director, Florida Institute for Cybersecurity Research, University of Florida

Dr. Tehranipoor said he wears multiple hats at the University of Florida. He is an Intel-endowed professor of cybersecurity and also the director of five centers and institutes. His main focus is on establishing hardware root-of-trust. The idea that hardware could be as problematic as software has been neglected over the past two decades.

- **Hardware Attacks**
  - **Trojans and Untrusted Foundry**: Trojans in integrated circuits are a major concern. China is spending billions of dollars and hiring away talent from the U.S., Taiwan, and Korea. Well-paid jobs are created for Koreans to go to China to work in the semiconductor industry. There are even emails that say, "Hey, when you come, why don't you bring that IP with you too." Congress has been talking about bills, bringing the foundries back, but even if we bring the foundries back, the shortage of talent for secure semiconductors is mind-boggling. There's nobody working in this area and nobody teaching it in the academic environment.
  - **Counterfeit ICs**: The counterfeit issue has been around for two decades. There are many other countries doing counterfeiting and then bringing the chips and systems back into the market.
  - **Side-channel and Fault Injection Attacks**: The tools on AI machines have been generated to develop malware, and every 4 seconds on average we get a new model, which we use. You can actually buy a $200 exploit kit in the market and do a very sophisticated side channel attack.

- **Reverse Engineering:** When Iran captured a drone 6 or 7 years ago, they called and said they reverse engineered it, and the U.S. said, "You guys are bluffing." Then they put the entire document on the web. We need to protect IPs and systems that are being put on the battlefield.

  Bloomberg BusinessWeek published a story on Oct. 4, 2018: "The Big Hack: How China Used a Tiny chip to Infiltrate U.S. Companies." Supermicro, a Taiwanese company with headquarters in San Jose and Taiwan, sells motherboards to the intelligence community, Amazon, Apple, Facebook, Google, etc. The story basically claimed that China found a way to inject a very tiny chip inside this PCB, which was able to hijack the entire boot-up process, inject its own malware, and take over the motherboard. They said they had 17 sources. Amazon and Apple denied it. There was a follow-up story that added more details.

  Dr. Tehranipoor has his own start up and is developing many of the solutions. He was surprised at how many companies used Supermicro. It translated, he believes, into a $10-12 billion loss on that day. People ask him if the story is true, and he has no information to share. His answer is that the problem is real. These guys could do it. His students can do it. Anybody could do it.

- **SoC Security**
  In the past, if you opened an old mobile phone, you could see maybe a handful of chips. Today, you see only one chip with maybe 50 different IPs in one chip. Now the target -- attack point or attack surface -- has become one big chip.

- **Security along the SoC Design Lifecycle**
  They start with specification planning. They develop architectures and algorithms and then go into integration, where they try to transfer the information into what they call GDS2 – geometrical representation of a chip. Then it goes into a foundry to be fabricated, tested, validated, etc., and then to high volume production. From high volume production, it goes into the supply chain. There are security considerations in every step of the process.

  The problem is that it's ad hoc. From one company to another, there are different levels of understanding of the exact same problem. There are opportunities for NIST to help with either establishing a standard or bringing these companies together to share best practices. The biggest problem is the integration phase of the chip design process.

- **Understand Supply Chain Vulnerabilities**
  Dr. Tehranipoor biggest concern is the supply chain. The number of different entities that have to be involved in the design process is mind boggling. Cisco starts to build a chip and then they hand over a piece of the design or the entire design to a group in India. Then it goes to China and then to East Asia for fabrication. Then it goes to Indonesia for packaging and then somewhere else for testing. Throughout the system, it is subject to attacks. Eventually it gets to end of life, but unfortunately, electronic devices are recycled and come back into the supply chain.

- **Solutions with Lifecycle in Mind**
  The solution is divided into three major areas:
  - **Protect the IP**: If an adversary gets their hands on the IP and they do not know what the key is, the function is never going to be correct. This is easier said than done. Where is the key? Who is transferring the key? Where does the key sit? How secure is the storage? How is the key is handled and distributed? At the University of Florida, they have basically an optical photon emission capability. They can literally see everything. We need to establish independent security protection layers. The first thing is to protect against malicious change.

- **Protect the Assets**: If you look at your mobile devices – the biometrics, bank accounts, bank information, usernames, passwords – everything basically goes through them. They're all subject to attack. When it comes to side channel, they can be broken in a matter of minutes. Ninety nine percent of the time, it's an implementation problem.
- **Protect the Supply Chain:** They need to provide end-to-end solutions. They are trying to develop device to system solutions. At every step of the process, any of these entities can establish verification with respect to the systems they have in their hand, to ensure that the PCBs are fine.

  They need to develop standards. Logic locking, side-channel assessment, and backside protection. They can develop standards for provenance, traceability, etc. Automation is key. Complexity is the enemy of security.

- **Recommendations**
  - Designed-in-Security: Standards
  - Automation: Reduce complexity and cost
  - Design with life cycle in mind: device → systems; traceability and provenance
  - Powerful but low-cost inspection
  - Hardware upgrade → Zero day; Everybody says hardware cannot be fixed – you have to replace it. The direction they're going is to make hardware look like software
  - Smart devices → DT for secure semiconductors; collect data during their lifetime, especially security data

- **Q&A**
  Mr. Duvvur asked about best practices regarding the hardware upgrade process. Is there an approach, or has somebody gotten a best practice around it, especially if you have agile fleets that are deployed in a cloud or set of clouds with technology like dedicated HSMs, for example? Is there an approach to ensuring upgradability as it is so pivotal to the operating environment?

  Dr. Tehranipoor said it is done quite ad hoc. Intel, IBM, Qualcom, etc., all do it differently. On the positive side, at least they're talking. There is a best practice and sharing being done right now in the testing and reliability domain, and he has been asking for this to be done in the security domain. It's hard for Intel or Qualcomm or some other organization to say, "Hey guys, I'm just here to tell you that we have this bridge." It's hard. He gets it, but there has to be a way to share in a non-public setting, just within a consortium of companies.

The Chair thanked Dr. Tehranipoor for his presentation

Grand Challenges for Embedded Security Research in a Connected World - Computing Community Consortium (CCC) Visioning Workshop Report

Dr. Tomas Vagoun Cybersecurity and Privacy R&D Technical Coordinator (contractor) National Coordination Office for Networking and Information Technology R&D

Dr. Vagoun said the Computing Community Consortium (CCC) Visioning workshop was held with about 50 participants. The CCC's mission is to look at larger problems in computing and bring parties together to better understand key research issues and challenges. The workshop was held to consider the embedded security issues in a connected world and look at it from the perspective of five themes:

- Medical/wearable devices
- Autonomous systems (drones, vehicles, robots)
- Smart homes
- Industry and supply chain
- Critical infrastructure

The workshop report was released in May 2020. They had a briefing in the CISA interagency working group in August 2020.

- **Key Challenges and Recommendations**
  - **Medical Devices and Wearables:** Areas of security and privacy are not covered by FDA and not really regulated. A long legacy makes it challenging to change or update system interfaces. Regulation on software, such as cloud-based services that are part of medical delivery, is unclear. There are complexities with globalization and distribution away from countries of origin.

    Recommendations: Applying classic cryptography, security, and control theory to vulnerabilities and attack surfaces could yield novel solutions. Ongoing efforts need to continue to create appropriate fallback or safe modes so that those devices have a better measure of resilience when dealing with unexpected circumstances or attacks.

    Mr. Groman asked whether there is a discussion about data collection. What data is collected, what data is transmitted, where does it go, and how is it stored? Are there controls around that?

    Dr. Vagoun said that was noted as one of the major challenges. It figures into the view of research priorities. There are a lot of privacy issues with data, data collection, data ownership, etc.

  - **Drones and Transportation:** Traditional modes of transportation are increasingly computerized, connected, and vulnerable. At the same time, they are more autonomous. Safety is paramount.

    Recommendations: Develop a methodology and tools that incorporate security from the conception of the vehicle and enable reasoning. The methodology should also be able to leverage interactions among multiple layers or physical properties of existing systems.

  - **Smart Homes:** A lot of different systems are interoperating in the context of smart homes, in many ways not successfully. Integration issues arise. Different subsystems may have different security requirements. There's a need to emphasize standardization.

    Recommendations: There is a need for some kind of framework. Different subsystems and components can declare, share, and require security properties that they rely on, and negotiations or some kind of resolution take place through a framework.

  - **Industry and Supply Chain:** There are obvious issues about reliance on software and firmware. A lot of it is sourced from third parties. Due to the long lifetime of the hardware, new parts are nearly impossible to come by. Old systems and protocols are challenging to secure retroactively.

    Recommendations: Retaining the capability to manufacture new parts is a key solution to the threat of counterfeits. We need the ability to get to designs, the source of what those parts are, how they should be manufactured, and how they should be built. There was also discussion about some of the newer design techniques, the multichiplet approach, where designs can be separated into pieces so that there is a better control of the security properties and the resulting system, even if fabrication, for example, is taking place elsewhere.

  - **Smart Grid and Critical Infrastructure:** There is an opportunity to integrate traditional sources of electricity with some of the newer sources. New abilities can be used to take advantage of distributed power generation based on renewable resources.

    Recommendations: Educate power companies about the effects of their buying decisions. Retrofit smart grids or electrical delivery systems with more modern controls and security technologies.

- **Distinguishing Themes**
  - Ownership of systems and the overall economic situation drive a lot of the issues and opportunities around data, data collection, and data use.

- Regulations and incentives play a major role. How do you put together systems with different parts that may or may or may not have regulatory oversight?

- **International Perspectives Panel**
  The panel discussed how research and academic funding are evolving. Overseas, the opportunity to get funding and access resources is far greater than in the U.S. The U.S. may no longer have the global edge on embedded security research.

- **Recommendations**
  - The U.S. can gain economic strength by ensuring that highly competitive embedded security research is funded.
  - International collaboration should be encouraged, and there should be no discrimination. In the last few years, many prestigious faculty have moved from the U.S. to Europe, China, and Canada.

- **Dr. Vagoun's Takeaways**
  - When you look at the embedded systems, because of interaction with the physical world, there are many different systems that have different environments when it comes to safety, security, and privacy. We don't have a holistic approach or framework to integrate safety, security, and privacy requirements, and we need to develop one.
  - Research Priorities: Develop and leverage unique properties related to the physics and locality to improve security; develop solutions for safe-mode/fallback operations; advance methods to integrate security in real-time systems; advance split-ASIC and multichiplet design techniques
  - Research Funding: It seems that the U.S. is falling behind.

  All of this should be viewed as a strategic issue. The U.S. needs to invest in innovative secure design solutions. The secure design approach combines software and hardware assurance tools and verification capabilities to provide for trusted manufacturing outcomes.

- **Q&A**
  Mr. Venables asked if there was any sense that people are looking for 20% - 80% approaches.

  Dr. Vagoun said the report doesn't present that analysis.

  Ms. Hallowell mentioned the NIST Cybersecurity Framework and asked whether the workshop had any specifics around frameworks when it comes to hardware security.

  Dr. Vagoun said people at the workshop were familiar with the Cybersecurity Framework. The workshop didn't offer any path forward for a combined framework. That level of detail was not discussed, but it was clear that not having this was a major impediment.

  The Chair said when he thinks of a grand challenge, he thinks of single research problem. In this case, what struck him is that a lot of the issues in embedded systems are about the absence of implementation or engineering that we've known how to do in the cybersecurity space for decades. We aren't able to do them, or they just aren't done. There are also some specific things beyond that, including Split ASIC. Is anybody pursuing a program to follow up on this?

  Dr. Vagoun said that, as a community, they have stated that that the safety/security/privacy framework is a priority. But if anybody specifically is looking at this, he's not sure.

  Mr. Groman said that all of the recommendations and conclusions resonate with everyone on the Board. He thinks the problem is not that we need more research or conferences or another blue ribbon panel. He would call the problem a lack of will/interest. The fact is that the C Suite – which in government could be the secretary of an agency – has to make decisions about competing priorities. For whatever reasons, we have not made privacy and security a priority in this country. It has to be a leadership priority over other competing priorities, and resources must be invested.

The Chair said that he and Mr. Venables and Mr. Groman are all saying variations on the same thing.

Mr. Groman said that, as the purchaser, we can insist on a level of security, but we don't. As data becomes more central and more of a risk to the U.S., we have to ask hard questions earlier.

Dr. Vagoun added that security is 1/3 technical and 1/3 economics and 1/3 social/behavioral. We spend a lot of time on the technical and not as much on the economic incentives and disincentives and the social behavior. There's an attempt on DoD's part to have a regime in which if you do business with them you have to be at a certain level of security. He is seeing some changes. If it works out, there are higher requirements that will have to be met.

The Chair said he would like to continue the conversation in the afternoon and announced a 10-minute break.

Internet of Things Security and Baseline Capabilities

Katerina Megas, NIST; Michael Fagan, NIST

The Chair welcomed Katerina Megas and Michael Fagan of NIST to talk about IoT security baseline capabilities.

Ms. Megas provided an update on NIST's IoT-related activities:

- **Recent Program Activity**
  - Publications
    - NISTIR 8259: *Foundational Cybersecurity Activities for IoT Device Manufacturers* (May 2020)
    - NISTIR 8259A: *IoT Device Cybersecurity Capability Core Baseline* (May 2020)
    - Pages.NIST.gov: Draft catalog of IoT Device Cybersecurity Capabilities/ Supporting Non-technical Capabilities (June 2020)
  - Events
    - Webinar on Core IoT Cybersecurity Baseline (June 2020): Nearly 700 registrants and lots of questions around conformity, how to demonstrate conformity, how to adapt the baseline to need, and use cases.
    - Federal Profile Workshop (July 2020)
    - Consumer IoT Cybersecurity Workshop (October 2020)
- **NISTIR 8259 Series: Progress**
  - Draft: July 2019: *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers*
  - Draft: January 2020: *Recommendation s for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline*
  - Final: May 2020
- **Upcoming Program Activity**
  - Publications:
    - NISTIR 8322: *Workshop Summary Report for "Building the Federal Profile for IoT Device Cybersecurity" Virtual Workshop*
    - Draft NISTIR 8259B: *Profile of the IoT Core Baseline for the Federal Government*
    - Draft SP 800-213: *IOT Device Cybersecurity Guidance for the Federal Government: An Approach for Establishing IoT Device Cybersecurity Requirements*
  - Events:
    - Consumer IoT Cybersecurity Workshop (October 2020)

- **Essays to explore**
  - Creating a Profile for the IoT Core Baseline
  - Privacy considerations for implementing the IoT Core Baseline: They felt that the Privacy Framework should be in place before honing down to a specific use case like IoT; Privacy considerations are being raised in the context of how an organization implements the baseline.
  - IoT considerations for Confidence mechanisms

Ms. Megas turned the floor over to Mike Fagan.

Mr. Fagan provided an overview of their recent publications and work. Starting with NISTIR 8228, they established a scoping of the kind of IoT product that their work is trying to hone in on.

- **What is an IoT device?**
  - Transducer capabilities interact with the physical world and are what make many IoT devices different from conventional computers.
  - Interface capabilities enable devices to interact with each other or for humans to directly interact with devices. Every IoT device has at least one network interface capability.
- **NISTIR 8259 and NISTIR 8259A**
  - They took a collaborative approach to developing the NISTIR 8259 Series. There were two public comment periods, two public workshops, multiple roundtables, webinars, and a federal profile workshop.
  - NISTIR 8259 *Foundational Cybersecurity Activities for IoT Device Manufacturers* provides specific recommended activities to help manufacturers address customer needs for IoT cybersecurity in their product development processes. It was divided into specific activities (8259) and device capabilities (8259A) for manufacturers.
  - Recognizing that IoT use cases span numerous industries and jurisdictions but that there are some common capabilities, 8259A provides a core baseline of IoT device cybersecurity capabilities for manufacturers.
- **Backdrop for Federal Profile of NISTIR 8259/A**
  - NIST has been working since January 2020 to create a full catalog of cybersecurity technical and non-technical capabilities that would be beneficial for a wide range of IoT devices. The capabilities in the catalog were created using 8259A and SP 800-53 capabilities. The capabilities catalog was published on the NIST GitHub to obtain feedback.
  - From the final initial IoT device cybersecurity capabilities catalog, NIST will determine the technical and non-technical capabilities (a subset of the full catalog) that will form the Federal Baseline. NIST anticipates other industries, associations, standards groups, and organizations will also use the IoT cybersecurity capabilities catalog.
- **NISTIR 8259B: *Profile of the IoT Core Baseline for the Federal Government***
  - They will be coming out with a draft of NISTIR 8259B, the profile of the IoT core baseline. To go with that, they will release a draft SP that will address what a federal agency needs to be considering as it procures or acquires IoT devices.
  - In addition to the formal publications, they are looking at some areas and maybe putting out an essay to use in conversations with stakeholders.
- **SP 800-213: *IOT Device Cybersecurity Guidance for the Federal Government: An Approach for Establishing IoT Device Cybersecurity Requirements***

They hope to get all these products out soon for public review to get that first set of comments and understand how they can make them even better. They are planning to release, hopefully, by the end of

the calendar year, the two documents that were just tested for public comments. Following the public comment period, they will hold a public workshop.

Ms. Megas said that one other thing to highlight is fragmentation, which has been a consistent message both from manufacturers and adopters, but mostly from manufacturers. If you're an IoT device manufacturer and your device is being sold to the transportation sector, the energy sector, or the federal government, how can we minimize the different flavors of devices that are going to have to be built? The U.S. delegation drove the proposal to the ISO/IEC Joint Technical Committee 1 and on this international standard towards a baseline. They are working on that concurrently so that they can avoid fragmentation.

- **Q&A**
  The Chair invited the Board to comment or ask questions.

  The Chair said one of the concerns he has is about the potential distance between the requirements and baseline programs and what developers or manufacturers actually deliver. He asked if they have done anything with the NCCoE to evaluate the things they're putting together and see how they match up to real implementation and deployment best practices.

  Ms. Megas said they have been talking to the project teams in the NCCoE and one of the things they're looking at doing is potentially start mapping to the Cybersecurity Framework to articulate how the IoT devices may be addressing or approaching different capabilities in the baseline.

  The Chair said it's important to be confident that what they're doing is going to affect.

  Ms. Hallawell asked about minimum security requirements for manufacturers of devices and whether they included anything prescriptive in the requirements.

  Mr. Fagan said the minimum wasn't so much minimum requirements as starting points for customers and for manufacturers to look toward and build toward. When it becomes a requirement, that is by a customer demand or when a manufacturer wants to treat it like a requirement.

  Jim St. Pierre said he thinks the question is about whether the baseline is prescriptive. It is outcome-based as opposed to prescriptive.

  The Chair announced a break for lunch.

Industry Bug Bounty Implementations Lessons

Katie Moussouris, CEO Luta Security

The Chair introduced Katie Moussouris, CEO of Luta Security.

Ms. Moussouris founded her company more than 4 ½ years ago. They do strategic consulting around a holistic approach. She is also the co-editor of the ISO standards that govern vulnerability disclosure and vulnerability handling processes.

At Luta, they don't support bug bounty Botox, which are done at the surface level and cosmetically engineered for maximum publicity but not a lot of actual security improvement. Unfortunately, dollars make headlines, and there has been an alarming uptick in bug bounty Botox over the last 4 ½ years.

- **Vulnerability Disclosure vs. Pen Test vs. Bug Bounty**
  Vulnerability disclosure is the process of receiving vulnerability reports from the outside, deciding what to do about them, and then releasing that information to affected parties. If the effected users are public, vulnerability disclosures are governed by two ISO standards: ISO 29147 and ISO 30111.

  Bug Bounty programs are a crowd-source hybrid with no special entry needed but the vulnerability finders get paid. Key differences between Penetration Testing and Bug Bounty programs have to do with managing risk.

They took a look at the Forbes Global 2000 back when she worked at HackerOne. Something like 94 percent of the companies had no way to report a vulnerability. That meant only 6 percent of the Forbes Global 2000 had an email address or a front door. Fast forward and it's not gotten much better.

- **ISO Standards 29147 and 30111**
  The Bug Bounty Platform coverage areas, when it comes to the ISO standards, can assist with despamming your inbox a little bit, acknowledging that the report was received, and a little bit of verification. This is not the vulnerability disclosure standard. This is the vulnerability handling processes standard. The process of weighing the relative importance of that particular vulnerability occurs internally. This is a contextual awareness of the vulnerability.

  A potential critical vulnerability is not necessarily going to manifest as critical impact in every organization. Third-party triage cannot help with that. If you have 200 critical vulnerabilities, for example, they cannot tell you which one of those to address first. You will know, based on your own product roadmap, other feature elements, and other mitigations you may be working on, etc. You will know, with a functional ISO 30111 process in place, how to relatively prioritize the outcomes.

- **How do we distinguish friend from foe?**
  Ordinarily, people are expecting if they put out friendly Vulnerability Disclosure Programs and a nice well-scoped policy that they'll get a bunch of friendly bugs. Ms. Moussouris started Microsoft's Bug Bounty Program 3 years before Google started its program. Google had a pretty well-developed and well-resourced ISO 29147/ISO 30111 compliant organization, and they had a good reputation with the security community. When Google started its Bug Bounty, they experienced a 10 times spike in submissions. And so, when preparing Microsoft for a 10 times spike in submissions, it was a big resource allocation question. Microsoft was already quite well-resourced with specialized roles across the organization in a well-oiled machine that had been operating with the biggest Vulnerability Disclosure Funnel in the world for many years. These programs can often induce a lot more traffic. It becomes difficult to distinguish friend from foe, which then impacts incident response resources. Endless skilled triage labor is what is required to perform this activity as advertised.

- **Cyber workforce shortage = Opportunity**
  There is a cyber workforce shortage, and Bug Bounty Programs have not addressed this problem. There is tension between the external reporter and the internal security team. Very skilled workers tend to use Bug Bounty programs as hobbies, whereas you have a mass of largely unskilled labor doing what Ms. Moussouris calls ‘spray and pray.’ Most of them generate noise. There are nine people who have made over a million dollars on the HackerOne platform. And the platform's been around allegedly since 2012. In the entire history of the HackerOne platform, with all 830,000-plus registered users, only 9,000 have ever been paid a Bug bounty.

  The most important thing to take from this is that we are not investing in the appropriate areas for sustainable long-term software security maturity. We are cranking out bug writers because we are not funding appropriate requirements, even in universities with computer science programs. None of the top 10 U.S. universities with computer science programs required security in order to graduate with a degree in computer science, and only seven of them had security as an elective.

- **Microsoft Mutiny on the Bounty**
  The number of vulnerability reports coming to Microsoft, pre bug bounty, was 150,000 to 200,000 non-spam email messages/year, which explains why they were hesitant to start paying hackers.

- **Hack the Pentagon – Hack the planet!:** 1,410 registered eligible participants; 1,189 total reports received; 138 total valid reports (horrendous signal to noise – almost every field in that target had a

flood of duplicate reports; never start a program at midnight if you don't want to receive a report shortly after midnight); 13 minutes – total time it took to receive first vulnerability report.

- **Hack the Army:** 371 registered eligible participants; 416 total reports received; 118 total valid reports; 5 minutes – total time it took to receive first vulnerability report.

- **Gaps in the BOD Guidance**
  The guidance is out of order. ISO 30111 is sort of like the digestive system of bugs. Without a digestive system, you must not go to an all-you-can-eat buffet. Whether you're paying for bugs or not, the process internally is the same between vulnerability disclosure programs and bug bounties.

  In the Capital One breach, the notification occurred by a good Samaritan hacker and that report was closed by a HackerOne triage person and caused a delay of reporting that breach. It is 45 times more expensive to deal with vulnerabilities after you have released them. If you are putting your resources towards vulnerability disclosure processes before resources towards secure development, you are doing things in a very inefficient and costly order.

- **Best Practices: Resource Allocation for VDPs**
  The key engine of vulnerability disclosure and bug bounty programs is the second layer of operational maturity. This is where the case management happens. If you are only fixing that one bug, you're playing whack a bug, and this is a completely inefficient system. Where you absolutely need the most resources is your security engineering process. VDPs accelerate the need to improve this whole area, not just the engine that runs VDP, but the security engineering process.

  The BOD provides an organizational commitment to respond to vulnerability reports. That would be baselining them at basic level organizationally, and then set up a point of contact. The most efficient investments are in better tools that helps close the skills gap between the attacks.

- **Recommendations**
  - Do a maturity assessment first
  - Use the assessment and set realistic goals
  - Create a roadmap for building compliance with ISO 30111

- **Recommended Order of Operations:** Assess; Close holes in software and process; Equip and train; Roll out VDP; Incorporate into SDL

  Ideally you want to create an environment that's running smoothly and then use bug bounties to direct eyeballs to where you need them most. Bug bounties are bad if they're your first external bug reports unless you are a tiny organization.

In the end, we really need to create balance in the labor workforce and understand that the majority of the workers that we need are not more people pointing out problems, it's people who understand problems.

- **Q&A**

Ms. Hallawell said there really isn't that much focus around security testing and asked if Ms. Moussouris had input around testing and how to better think about security testing as it relates to bug bounties and VDP.

Ms. Moussouris said security testing is part of the secure development lifecycle. The verification steps ideally come after you have implemented as many design-level checks as possible. The emphasis should be way earlier than the testing part. There's often a missing link – it's a combination of testing and, more importantly, it is secure architecture guidelines, design principles, and bringing in experts to evaluate the secure design.

Ms. Hallawell said secure architecture and design is harder to evaluate than security testing. How do you make security architecture and design review easier from a marketplace perspective?

Ms. Moussouris said we still have unaddressed market spaces for a lot of these things. There are no magic bullet answers about ways to make this more scalable.

The Chair thanked Ms. Moussouris for her presentation and invited her to return to answer questions during the final session of the meeting.

Quantum Computing; Current State and Cryptography

Dr. Barbara Goldstein, PML, NIST; Dr. Dustin Moody, ITL, NIST

Dr. Goldstein said there are a lot of opinions on where the state of the art is in quantum technology. Her presentation focuses on three general buckets of quantum technologies – quantum sensing, quantum computing, and quantum communications and networking – and on the Quantum Economic Development Consortium

- **Quantum Sensing**
  Dr. Goldstein manages a program called NIST on a Chip, where they are developing a suite of quantum-based sensors. The advantage of sensing is that we can use quantum tricks to help lower the noise limits of conventional sensing technologies. Applications include biosensors and other health-related applications, gravimeters, and accelerometers for navigation in GPS-denied environments. Broadly speaking, sensing is probably the closest to maturity out of the three major buckets. One of the kick-off applications was the chip-scale atomic clock. There is a commercial product on the market being sold and a lot of other sensors in the works.

  What is needed is a new metrology culture. When we talk about shrinking precision measurement technology down to chip-scale, and then trusting it out in the wild where it can be embedded directly into products, it's a whole new world in the metrology community. We need to develop trust mechanisms for shifting over to that.

  Sensors being developed within the NIST on a Chip program include the chip-scale atomic clock. John Kitching, in the Time and Frequency Division, came up with the idea that you could take a lab full of equipment that took a bunch of PhDs to run, and shrink it down to something that's basically the size of a grain of rice, put that out in the field, and trust it to behave in a reliable, reputable manner, which he did.

  Another forerunner of quantum sensing at NIST is voltage sensors. They have the world's most precise voltage sensors available, which costs a quarter of a million dollars. They are working on mechanisms for making them more affordable –good enough for a lot of applications.

  Another one is E-field sensing, which is based on taking the outermost electron of an atom and putting it into a tortured state pulled far from the nucleus. You create what's called a Rydberg atom that has a large macroscopic footprint, making it exceptionally sensitive to electric fields.

- **Quantum Computing**
  A lot of companies are in some stage of technology development with quantum computing. Quantum computers are well-poised for optimization problems and rapidly solving the kinds of problems that would otherwise be intractable. The buzz is that they could do things like break current cryptography. That is why there's the whole quantum-safe cryptography effort that ITL is spearheading.

  There is a lot of technology development needed to scale down the cryogenics and the environmental controls that it will take to have a successful quantum computer. We need better and more robust ways to transduce this fragile quantum information between a variety of physical modalities,

including microwaves, vibrating membranes, RF signals, etc. We need to be able to read out these signals at room temperature, even if we have to process them inside of a cryostat.

There is a lot of hype around quantum computing and the number of qubits, but to get to the end goal, which is a full-scale, error-corrected, gate-based quantum computer, we are decades away. Also, to error-correct, you must have an enormous number of error correction qubits on top of the qubits that you're expecting to actually do your work.

What's available now are quantum annealers. This is a very specific kind of quantum computer that's geared towards optimization. D-Wave is the company that's best known for quantum annealing.

Another area in the works involves quantum computers available via the cloud, called NISQ, Noisy Intermediate-Scale Quantum systems.

NIST has a long, rich history in developing the baseline and fundamental enabling technology that's helping this market grow. They have a world-leading program in ion trapping, and this is famously what Dave Wineland got his Nobel Prize for advancing in terms of manipulating and controlling qubits and single trapped ions. They also have a program in using Josephson junctions, which, if successful, is easier to scale up.

- **Quantum Communication and Networking**
  The third large bucket is communications and networking. Ideally, this will provide the advantage of eavesdrop-proof communications. Quantum-based sensors are using quantum tricks to make better sensors.

  Another application people are looking forward to is blind quantum computing. Eventually, when we have more powerful computers available via the cloud, you'd like to have some sense that the information you're feeding into that computer and the results you're getting back are secure. You want to know that whoever's hosting that computer is not eavesdropping.

  This is widely thought of as the least mature of the three buckets of quantum technologies. We need quantum repeaters, memories, and interconnects. We need robust, reliable, single-photon sources and detectors, and compact cryogenics.

  We are looking at implementing networks, both ground-based and space-based, so there's lots of technology to develop there. A functional, entanglement-based quantum network is a long way off.

  The Chair noted that he has read in the trade press about quantum networks and municipal scale quantum communications and ground-to-space quantum communications. It is a little bit of a surprise to hear that that's the least mature. Are the press reports just marketing hype?

  Dr. Goldstein said that the least mature doesn't mean the least hyped. Another thing many people talk about in quantum networking is quantum key distribution, and that is one of the most mature quantum technologies. You can buy QKD, quantum key distribution products on the market. That is technically a network, but all it does is secure the channel by which you would send a key. This is really an international battleground. China has a very aggressive strategy for initiating lots of standards activities. It is a way to assert dominance in the field, which is widely thought to be the foundation for the next wave of economic growth. People are posturing.

  To highlight a very simple system, NIST is still aiming to just put together a very small, couple-of-node network. They also kicked off the Quantum Network Grand Challenge.

- **Joint Institutes**
  NIST has played a role in the development of the quantum research community from the very beginning. They have three joint institutes involved in quantum research. One in Boulder that was

established in 1962 started with astrophysics but now is a world leader in AMO and quantum many-body physics. They have two joint institutes with the University of Maryland – one that is doing fundamental research, well-known for quantum simulation. Bill Phillips, one of our Nobel laureates, has a research group there. And the other, QuICS – Center for Quantum Information and Computer Science, brings in a lot of IT and computing capability to study questions on complexity and integration of classical and quantum computing.

- **Quantum Economic Development Consortium**
  The goal of QED-C is to develop a community of suppliers that will turn good ideas into an actual marketplace that scales to commercial levels. Its mission is to create a robust supply chain for the United States. It is called out in the National Quantum Initiative Act and is a key part of our national strategy. It is industry-driven and run by SRI. There are participation agreements ready for companies to sign. Up until last month, people could only sign letters of intent, and they had 180 different organizations that signed those. Now they have over 100 signed participation agreements, and they're still coming in.

  We don't have the workforce we need, and so there's a lot of effort in building quantum education into the pipeline.

  The consortium is beginning to fund research that it prioritizes, and there was recently a call for proposals in the area of cryogenics.

- **USG Policy and Investments**
  The national strategy around quantum includes building up a quantum-smart workforce, engaging with industry, and focusing on economic security as a key component of national security. The National Quantum Initiative Act authorizes almost $1.3 billion in new investments. NIST has received about $10 million, and they are hoping that their share will grow in these next few years.

  The National Science Foundation is targeted to double its quantum investment, and the DOE is also expecting healthy increases to its quantum-related budget. As part of those NSF and DOE investments, they are required by the National Quantum Initiative Act to stand up centers, which both have done in the last couple months. NIST is also a lead on the Q-SEnSE center that the NSF recently announced. The private sector is making significant investments as well, and there is a huge amount of global investment. NIST's quantum researchers always feel sort of outspent, especially by China.

Dr. Goldstein turned the floor over to Dr. Dustin Moody, who is in charge of the post-quantum cryptography project at NIST.

- **The Quantum Threat**
  In terms of cryptography, there is the threat that a large-scale quantum computer would break the public-key cryptosystems that we use today. NIST has three public-key crypto standards that involve public-key encryption or public-key establishment as well as public-key digital signatures. If a large-scale quantum computer were to arrive, we would no longer use the crypto algorithms that are standardized. The post-quantum crypto project is looking for new cryptosystems to standardize.

  The threat to public-key cryptography is much more than the threat to symmetric-key cryptography. While public key would be completely broken, with symmetric-key cryptography, we would need to use longer keys and longer hash function output, and that's much more manageable.

- **NIST PQC Milestones and Timelines**
  Around 2016, they announced a worldwide competition, organized into two rounds. They asked people to design new quantum-resistant cryptosystems and then they would select the best ones for standardization. They received 82 submissions. The first round of evaluation and analysis went on for roughly a year, and they looked at security, performance, and some of the particular individual

characteristics. They selected 26 algorithms to move into the second round. They issued a report, NISTIR 8240, documenting the decision process and reasoning.

Two or three months ago, they announced the algorithms that would move into the third round. They selected two tracks of algorithms, with seven finalists and eight alternates. NISTIR 8309 explains it.

During the third round of analysis, they will hold another workshop. The round will last probably about a year and a half, and then they will select algorithms to standardize. They expect to issue the draft standard around 2022, and then it will probably take a year or two to write the standard, put it out for public comment, address the comments, and finalize it.

They will likely do a fourth round to continue looking at the alternates, and likely select a few of the alternates to standardize at that point.

- **Q&A**
  Mr. Venables asked if they are also publishing performance profiles, power consumption, key size, or ciphertext expansion.

  Dr. Moody said that in the specification all teams must make it clear what their key sizes, signature, and ciphertext sizes are. There are outside websites that have put them all in tables that are easy to see. As for performance profiles, they compute some internal benchmarks, which they publish and make known in their presentations. There are websites that have much more widespread performance testing so that people can see the performance of these algorithms.

  Mr. Venables asked if they are comfortable that it is correlated with power consumption. Is there any kind of weird power consumption profile on any of the algorithms?

  Dr. Moody said there is also work being done on power consumption. The algorithms are a little bit different in their own way, but none of them are notably strange.

  The Chair said his cryptographer friends seem to worry about side channels in the algorithms. What has NIST done about that area?

  Dr. Moody said they want to make sure it is looked at. They called that out in their report. Internally they don't have anyone who is a great expert in side channels so they are trying to stay in close contact with the experts they do know.

  The Chair said he also worries that this shapes up to be an enormous transition. Standards will have to accommodate multiple algorithms. For somebody who comes from the software security world, this seems like a prescription for potential bugs or oversights that could creep in and last for years. Is anyone thinking about that?

  Dr. Moody said there are a lot of people worrying about that. The NCCoE started a lot of work in this area to help give guidance to companies to start preparing for the transition and develop a playbook. They held a workshop a week ago or so, and more than 300 people attended. There will be hiccups along the way.

  The Chair asked how confident they are that we need to be doing this. When he was a kid in high school, he read in *Popular Science* magazine about fusion power being the future of clean energy. A week or two ago, he was reading that a group, maybe at MIT, might have a nuclear fusion reactor available in another 10 or 20 years. Is the quantum computer threat going to be real? Making the transition is not going to be without risk.

  Dr. Goldstein said there are people who legitimately are asking this question. There is a lot of talk about whether we are going to head into a quantum winter. Her opinion is that while the hype may ebb and flow, this technology is coming. We can be confident we are making progress toward

quantum computing. If you don't take it seriously now, by the time there's a tipping point, it's too late. We don't have the luxury of sitting on the sidelines.

Dr. Moody said we can't afford to do nothing. Even if there is a small chance that it does exist, we have to be prepared for that.

The Chair thanked the presenters and announced a 10-minute break.

Final Board Reviews, Recommendations and Discussions

The Chair opened the Board review and asked if members had any follow-up questions or comments on any of the day's presentations.

- **Quantum Transition and Crypto Agility**
  Mr. Venables said that with regard to the quantum landscape, there is a lot of awareness in industry about cipher competitions and such, but there is a lot less awareness about what needs to happen around crypto agility. The fact that the cipher text is going to be a different size, for example, is going to mean a lot of re-engineering. As we get closer to the transition, it could be useful to publish more information about how organizations can start preparing today. If, for example, an organization next year is rebuilding one of its transaction messaging systems that uses digital signatures, they should probably build it in such a way as to cope with key expansion and signature expansion. He doesn't know if people are really thinking deeply about that.

  The Chair said that the workshop Mr. Moody referred to in his presentation focused on that issue, and it was well attended. SAFEcode is starting to work on guidance for organizations that are facing the agility problem. That said, he feels like there remains a real problem, particularly considering how long it has taken to get other standards changes done.

  Mr. Venables said that we need to think about the cascading effect on other standards. The ripple is going to be much more challenging than the engineering challenge.

  The Chair said that NIST is working this problem, and he asked Mr. Scholl and Mr. Stine if they feel like NIST is doing enough and is focusing enough attention on it.

  Mr. Scholl said they certainly understand the issue and have many lessons from past experience to guide them. They do have a separate item looking at transitions and agility, which basically started with the workshop the previous week. That said, it is never a bad idea to re-emphasize the need for attention to make it a successful transition. In short, they do understand that this is an issue, but he does not think they should underestimate its difficulty.

  Mr. Stine agreed and added that there is a long road ahead on this issue, and it has to run in concert with the standardization process that is underway. They will have to double down on their collaborations with partners.

  Dr. Romine said there is no lack of will on ITL's part in engaging the community and working hard on this problem. That does not mean that there isn't value in the board redoubling their attention to this. The resources that expended on ITL activities have to be prioritized in some way. Having the board express that they believe this is of sufficiently high criticality helps him prioritize it.

  Mr. Scholl said they could tee this topic up for the next meeting if it's of interest. They have talked with people in the U.K. who are very interested in doing agility testing with TLS. Some of the folks in the E.U. are interested in doing some benching around implementations as well.

  Mr. Venables said it would be useful to think about the top five most likely areas of standardization over the coming years that will lock in something that is going to last beyond the decade. What is in

that window over the next 5 years or so of standards definition that will lock something in for the following 10 years?

Mr. Scholl agreed.

The Chair said that it might be helpful to have a briefing about the post-quantum transition at the next meeting, and then they can consider sending a letter that recommends prioritization.

- **Emphasizing Privacy Initiatives**
  The Chair reminded everyone that Mr. Groman had suggested sending a letter recommending additional emphasis on privacy to encourage NIST to keep an eye on what seems to be a growth area of security and privacy problems. Mr. Groman was unable to submit a draft letter overnight. If everyone is in agreement, they can vote to send such a letter, draft it following meeting, and then the Chair can sign it out. He asked whether that is in the scope of the Board's charter.

  Mr. Scholl said he believes it is.

  Mr. Gattoni said he sent Mr. Groman his thoughts on the topic. He moved that they proceed with writing the letter and send it after the meeting.

  Mr. Duvvur seconded the motion.

  The Chair called a vote.

  The Board voted in favor of sending the letter.

- **Vulnerability Disclosure**
  The Chair asked the Board members if they believe it makes sense to write a letter, perhaps to DHS, about the issues in vulnerability handling and vulnerability disclosure policies to make sure agencies have a complete or balanced program and not get themselves buried in vulnerability reports.

  Mr. Gattoni said he heard the comments expressed during Ms. Moussouris' presentation on order of operations. He is not an expert in that, but his read of the VDP is that it has progressive milestones in it. He doesn't know whether a formal letter is needed. He can take comments back to the senior staff meeting at DHS. There are forums for these kinds of discussions, and he can create the conversation loop at the CISO level.

  Mr. Venables added that if it isn't necessary to do something formal, then he doesn't see the need to.

  Ms. Moussouris offered a clarifying comment about her presentation. She said they found that when people jump into this area and expect to build out the metrics, they are already so far behind. There are a lot of missing assumptions in terms of skills and tools. This isn't something you can walk into and measure as you go along. It is important to understand what your metrics are currently.

  Mr. Gattoni asked Ms. Moussouris if she had an opportunity to participate in the BOD process.

  Ms. Moussouris said that she and her co-researchers submitted a comment, and one of their recommendations was accepted. CISA understands that this is something that will cause discomfort. They don't understand that there is a skills, tools, and process gap. It is not a resource re-allocation issue. Right now, we are not training for the expertise because it is an unrecognized blind spot. We need another intermediate layer of expertise for case history over time, for spotting patterns over time. It needs to be a specific function. Not having it is like throwing an anatomy book into the wilderness and hoping surgeons will emerge.

  The Chair asked if board members were comfortable with proceeding without a formal letter for now and maybe revisiting it at the next meeting.

Mr. Gattoni said the meeting following the next one might be a good time for an update from CISA.

The Chair agreed.

- **Topics for the next meeting**
  The Chair asked if there were any additional items to queue up for the next meeting

  Mr. Scholl said another possible topic is hardware and supply chain security. The next meeting is tentatively scheduled for March 3 and 4. He invited the Board to offer suggestions on conferencing platforms because they might use a different one.

The Chair thanked everyone for their participation and adjourned the meeting at 3:30 p.m. ET.

REGISTERED ATTENDEES		
Last Name	**First Name**	**Affiliation**
Agnes	Anna	Zeichner Risk Analytics
Bagley	Drew	CrowdStrike
Baker	Brett	U.S. Nuclear Regulatory Commission
Benack	Donald	DHS
Benzina	Kamial	Wiley Law
Boutin	Chad	NIST
Brewer	Jeff	NIST
Brewer	Tanya	NIST
Brown	Peter	European Parliament
Carlson	Caron	G2
Cichonski	Jeff	NIST
Dixon	Cameron	DHS
Doyle	Harry	HD Healthcare, LLC
Duffy	Mike	DHS
Duvvur	Akilesh	IBM
Fagan	Michael	NIST
Fatty	Lamin	Cfpb
Feola	Alyssa	GSA
Friedman	Sara	Inside Cybersecurity

Garriott	Boyd	Wiley Law
Gatton	Brian	DHS
Geller	Eric	Politico
Goldberg	Jodi	Wiley Law
Goldstein	Barbara	NIST
Golmie	Nada	NIST
Groman	Marc	Privacy Consulting
Hallawell	Arabella	NETSCOUT SYSTEMS
Harris	Maranda	Deloitte & Touche
Hatzes	Laura	G2
Heyman	Mat	Impresa Management Solutions, LLC
Iacobucci	Erin	Stroock & Strook & Lavan LLP
Kerben	Jason	Department of State
Kiesler	Aaron	Lewis Burke
Kimberly	Armeni	GSA
Lemire	David	Huntington Ingalls Industries, TSD=MDIS
Lipner	Steve	SAFECode
Maughan	Doug	NSF
McConnell	Andy	G2
Megas	Katherine	NIST
Mitchell	Charlie	Inside Cybersecurity
Moody	Dustin	NIST
Moussouris	Katie	Luta Security
Newhouse	Bill	NIST
Polania	Boris	Honda North America, Inc.
Ranganathan	Venugopal	Google LLC
Rodriguez	Tina	CFPB
Romine	Chuck	NIST
Scholl	Matt	NIST

Scott	Kat	Wiley Law
Sokol	Annie	NIST
Stine	Kevin	NIST
Suh	Paul	USPS OIG
Tabassi	Elham	NIST
Tehranipoor	Mark	University of Florida
Tupitza	Charles	Americas SBDC
Vagoun	Tomas	National Coordination Office
Velasquez	Evangeline	Yap
Venables	Philip	Goldman Sachs- NEEDS UPDATED NOV2020
Weinberger	Peter	Google, Inc
Yaniv	Orlie	Gigamon