Internet of Things Advisory Board (IoTAB) Committee

Established by 9204(b)(5) of the William M. (Mac) Thornberry
National Defense Authorization Act for Fiscal Year 2021 (Pub. L. 116-283)

January 18-19, 2023

Virtual Meeting Platform: Webex

MEETING MINUTES

Board Members	**Board Chairs and NIST Staff**
• **Michael J. Bergman**, Consumer Technology Association • **Dr. Ranveer Chandra**, Microsoft • **Nicholas Emanuel**, CropX • **Steven E. Griffith**, National Electrical Manufacturers Association • **Tom Katsioulas**, Global Semiconductor Alliance • **Prof. Kevin T. Kornegay**, Morgan State University • **Debra Lam**, Georgia Institute of Technology • **Ann Mehra**, Splunk • **Robby Moss**, TGL Enterprises LLC • **Nicole Raimundo**, Town of Cary North Carolina • **Maria Rerecich**, Consumer Reports • **Debbie A. Reynolds**, Debbie Reynolds Consulting • **Dr. Arman Shehabi**, Lawrence Berkeley National Laboratory • **Peter Tseronis**, Dots and Bridges LLC	• **Benson M. Chan**, Strategy of Things Inc. (Chair) • **Daniel W. Caprio Jr**., The Providence Group (Co-Chair) • **Barbara Cuthill**, NIST (Designated Federal Officer) • **Jeffrey Brewer**, NIST (Designated Federal Officer Backup) • **Katerina Megas**, NIST (Federal Working Group Co-Convener) • **Alison Kahn**, NIST (Federal Working Group Co-Convener) • **Greg Witte**, NIST Contractor, (Report Editor) • **Brad Hoehn**, NIST Contractor (Report Editor) • **David Lemire**, NIST Contractor (Scribe) • **Wendy Szwerc**, NIST Contractor (Scribe)

Action Items Over Both Days

*Note: Names and roles are **bolded** to show ownership.*

General:

- **All IoTAB members** to submit presentation files to Ms. Cuthill if they have not already done so.
- All presentations can be found on the NIST website at: *https://www.nist.gov/itl/iot-ab-january-2023-meeting-minutes-and-presentations*

Report Outline and Initial Discussion:

- Regarding the drafting of the report, there were several related sub-actions:
  - **Mr. Chan** to lead the IoT Advisory Board (IoTAB) in more discussion on creation of a list of topics for the report to organize thinking in context of initial proposed outline.
  - **Ms. Lam** to provide draft of graphic to show horizontal / vertical landscape; also, to consider aspects of scale (e.g., from personal / wearable up to Smart Cities);
  - **Mr. Bergman** to provide draft scope proposal as it might appear in the report.
    Mr. Griffith volunteered to support Mr. Bergman on providing scope definition.
  - **Mr. Chan** to indicate specific items to be considered in the report outline:
    - Suggests agriculture, smart traffic, and critical infrastructure as initial topics.

  - Device ID information was discussed by Ms. Mehra, Mr. Bergman for Mehra's definition, and Mr. Katsioulas' perspective.
  - Ms. Mehra points out that report needs to include Recommendations as key section.
- **Ms. Reynolds, Ms. Raimundo, Ms. Lam** volunteered to develop personas (i.e., categories and lifecycle of IoT as examples)

IoTAB Sub-groups:
- **Chair and Vice-chair** to establish and coordinate **with the Designated Federal Officers** subgroup meetings for the purpose of collection and consolidation of information to be provided at the next full IoTAB meeting to make discussions and deliberations at those meetings. Subgroups can gather and consolidate information for the purpose of preparing for meetings of the full IoTAB. This information will be part of the IoTAB website.

Schedule:
- **Ms. Cuthill, Chair and Vice Chair** will work on meeting arrangements and send out confirmation for the following agreed upon IoTAB meeting dates:
  - 7 March: 1-day virtual meeting
  - 18-19 April: 2-day, hybrid meeting
  - 16-17 May: 2-day virtual meeting
- Request by IoTAB Members to plan dates for the rest of the year and develop timeline for accomplishments.

Speaker Invitations:
- **Chair and Vice Chair**: Identify potential speakers for understanding the focus of critical infrastructure for IoT.

Information Sharing:
- **NIST**: Provide background on the Developing and Growing the Internet of Things (DIGIT) Act estimate of 125 billion devices.
- **NIST**: Provide information on the availability of resources for market research.
- **Chair, Vice Chair and Sub-group leads:** Requested by IoTAB members to share information about subgroup meeting schedules ahead of time and for an information sharing mechanism to be established.

Meeting Recording:
- **NIST** will post to the IoT Advisory Board website.

Day 1 – IoTAB Meeting on Wednesday, January 18, 2023

Opening and Welcome

Introduction of the Chairs/Open the Meeting

Ms. Cuthill, Designated Federal Officer

- The Designated Federal Officer (DFO) opened the meeting at 11:04 a.m. ET and welcomed everyone to the call.
- Introduced the IoTAB Chair and Vice Chair.

Mr. Chan, Chair

- Welcomed the IoTAB members.
- Mr. Chan noted that the IoTAB is an impressive group and that he was looking forward to contributing to the work of this board.

Mr. Caprio, Vice Chair

- Thanked to the NIST staff for putting this together.
- Mr. Caprio noted that this is a momentous occasion in IoT.
- Mr. Caprio further noted that the IoTAB can all learn from each other and that our experiences complement each other.
- Mr. Caprio shared slides which can be found here: PowerPoint Presentation (nist.gov)

Mr. Chan, Chair

Mr. Chan shared slides, which can be found here: IoT Advisory Board Report Outline - Draft (nist.gov)

- Mr. Chan discussed expectations for the board and this initial meeting.
  - Importance of being strategic and proactive with developing the report
  - Reviewed the agenda.
  - Began team introductions.
  - Noted that on day two, the IoTAB would get into the details of the major topic areas.
  - Encouraged feedback.
  - Reminded the board that there would be three speakers toward the end of the second day.

NIST Introductions

Ms. Cuthill, Designated Federal Officer (DFO)

- NIST employee for 30 years.
- Introduced Jeff Brewer as the backup DFO who has several years' experience as a DFO of the Information Security and Privacy Advisory Board (ISPAB).
- Introduced Ms. Kat Megas as the lead of the IoT for Cybersecurity Program at NIST. Ms. Alison Kahn and Ms. Kat Megas are the Co-Conveners of the IoT Federal Working Group (IoTFWG).

Ms. Kahn, Federal Working Group Co-Convener

- Works within the NIST Public Safety Communications Research (PSCR) Division.
- Ms. Kahn also introduced Mr. Greg Witte and Mr. Brad Hoehn as members of the contractor team supporting NIST, who will be helping to provide writing support to the IoT Advisory Board.

Board Member Introductions - Each Member

Mr. Benson Chan, Chair

- Chair of the IoTAB.
- Based in San Francisco, working with IoT in various capacities.
- Co-founder and CEO of an innovation company called Strategy of Things Inc., which brings science technology and strategy to help cities, communities, and businesses. It operates within these communities to solve complex problems.

Mr. Dan Caprio, Vice Chair

- Worked as a senior official at the Federal Trade Commission (FTC) and then as a senior official at the Department of Commerce where he was acting Assistant Secretary for Technology Policy and the Chief Privacy Officer of the department.
- Worked on IoT and technology policy for 20 years.
- Has served on a number of expert groups on IoT, including trans-Atlantic with the European Commission.
- Has also worked on several advisory committees while at FTC and have been on three since leaving the federal government.
- Co-founder of Providence Group, which advises boards and senior level executives on data risk. This includes focusing on privacy, cybersecurity, and IoT.

Dr. Ranveer Chandra

- PhD from Cornell in Computer Science.
- 18 years' experience.
- Published more than 100 papers.
- At Microsoft for the past 8 years where he leads industry research and work on different areas, including agriculture and supply chain.
- Started a project FarmBeats for data driven agriculture, which was featured by Bill Gates to become a Microsoft product. Also have partnered with USDA and various companies.
- Also served on the Federal Communications Commission (FCC) technical advisory council and taskforce working group

Ms. Debbie A. Reynolds

- Data Privacy Officer and founder of Debbie Reynolds Consulting.
- Works at the intersection of privacy, law and technology.
- Started over 20 years ago working with companies on digital transformation.
- Works on technology issues as it relates to emerging technologies and how that impacts humans. This includes issues such as privacy by design, smart cities, and how companies can use technology and tools to collect and retain data.
- Serves on advisory boards doing privacy work around topics such as the metaverse, virtual reality, augmented reality, mixed realities – also connected systems.

Prof. Kevin T. Kornegay

- Director of the Cyber Security Assurance and Policy Center at Morgan State University and a Professor in the Electrical and Computer Engineering Department at Morgan State.

- Berkeley graduate PhD with a background in devices circuits and systems, which was the focus of the early part of career.
- Designing the fabric that is are used to implement and construct IoT devices.
- In the last 10 years moved into the security space to work on reverse engineering techniques, which is the inverse of the design to address vulnerabilities.
- Interested in the intersection of 5G technology and the impact it has across the entire ecosystem.
- Has worked with 32 PhD students. Over 200 publications. Several blockchain patents.

Ms. Nicole Raimundo Coughlin

- Chief Information Officer (CIO) for town of Cary, NC, which is located in the Research Triangle area.
- Worked in the IoT smart city space for about the last six years.
- Recently deployed a LoRaWAN network.
- Strong interest in security.
- Working on a regional level. Mother Nature knows no boundaries, with prediction, building models.
- There's an opportunity here for education and standardization.

Mr. Michael J. Bergman

- Vice President at the Consumer Technology Association (CTA).
- Worked on the technical side of the trade association, which is also associated with the Consumer Electronics Show (CES).
- Worked in the technology industry for more than 30 years.
- Led work on cyber security and on internet standards.
- Currently working on helping to set up a national cybersecurity label for consumer connected devices. The White House announced this on October 19th.
- There is a public-private effort going on and this was a central role on the public side and CTA.

Mr. Robby Moss

- Supply chain IT solutions consultant currently advising a couple of companies including a supply chain planning and analysis startup.
- Implementing systems that use IoT at the edge to bring data into supply chain systems, whether it is supply chain production control or manufacturing execution.
- Interested in use cases and efficiency gains that can be brought about by doing data collection or enabling the workforce with inventory management efficiencies.
- Focused on organizational change management and how new technologies effect operations.
- Previous work includes private sector logistics operations, working at Transport Security Administration (TSA) and then some work in government consulting.
- Working during the past eight years in mobile workforce solutions.

Mr. Steven E. Griffith

- Executive Director for the National Electrical Manufacturers Association (NEMA) - an industry association of over 325 manufacturers.
- Focus is on intelligent transportation systems, electrified transportation infrastructure, and all aspects of fleets, busses, and rail.
- Lead for NEMA's broader cybersecurity activities.
- NEMA's members provide the products and systems that go in various aspects of critical infrastructure and are moving towards the Internet of things in the manufacturing space.

- Focus on the IoTAB will be on industrial IoT (IIoT).
- Project and program management experience with over 20 years for the Department of Defense and TSA.

Ms. Debra Lam

- Based at Georgia Tech, leading a statewide public-private partnership called the Partnership for Innovation, which is a cross between a foundation and an action tank. It uses financial and social capital to invest in innovation solutions for shared economic prosperity.
- Have been doing work in the smart cities IoT space, both at Georgia Tech and prior to that for the city of Pittsburgh as the Chief of Innovation and Performance.
- For the city of Pittsburgh, experienced with public-private partnerships between higher education, corporate, and the university sector.

Mr. Nicholas Emanuel

- From Omaha, Nebraska.
- Working in the agriculture sector.
- Worked at John Deere and their advanced engineering department developing agriculture technology.
- Saw a disconnect from what we were providing from the corporate world and what the agricultural producers and farmers were able to adopt and utilize.
- Left John Deere and started a company to help service growers and support them on the data connectivity and software.
- Started having sensors in the field to measure quantities of moisture and irrigation events related to water utilization for egg producers. This company was acquired by CropX.
- Maintains advisory product development role that is ongoing.
- Took over family farm in Nebraska.

Ms. Maria Rerecich

- Senior Director of product testing at Consumer Reports, based in Yonkers, New York.
- Responsible for the teams who generate evaluations and ratings of consumer products, covering the areas of appliances, home health and outdoor products and consumer electronics.
- Have a team responsible for testing the security and data privacy of these products across all these product areas.
- Background is in Electrical Engineering.
- Went to M.I.T. and spent many years doing integrated circuit chip design and product engineering in the semiconductor industry.
- Been at Consumer Reports for ten years.

Mr. Tom Katsioulas

- Started in Digital Equipment [Corporation] in Massachusetts and did everything in the value chain from chip design to manufacturing.
- Has helped numerous startups in Silicon Valley involved in maritime, agriculture, and weather.
- Got into IoT through a gaming startup company that began looking at the chips through the connected ecosystem of IoT.
- Went to the Global Semiconductor Alliance and created a group of companies with expertise from end-to-end to promote trusted utilization solutions and a scalable business model.

Mr. Peter Tseronis

- Went to Villanova University and Johns Hopkins.
- Worked in the federal government for 25 years.
- Chief Technology Officer of the U.S. Department of Energy and U.S. Department of Education.
- Launched Dots and Bridges seven years ago.
- Led an IoT infrastructure working group for a non-profit here in Washington.
- Leader on a Control Systems Working Group through the energy sector ecosystem.
- Led a utility supercluster associated with energy, water, and waste management, which ties into the world of smart cities.
- Interested in the emphasis today on critical infrastructure and how technology impacts humanity. Trust is needed and keeping data safe.

Ms. Ann Mehra

- Harvard graduate working with Professor George Church, the father of synthetic biology at Harvard Wyss Institute, which has the mission to transform health care and the environment by developing innovative technologies that emulate and accelerate the way nature works.
- Started working on IoT during the dot-com era, leading Java programming while working in industry and government, and most recently guiding and advising the Chief Information Officer (CISO) of the Veteran Affairs and several health care institutions including the Mayo Clinic, Stanford Health, UCLA and others.
- Specifically, focused on addressing vulnerabilities in IoT devices, including Operational Technology (OT) and the Internet of Medical Things (IoMT). IoMT as within hospitals but also a focus on patients' homes where there is a vital and critical need to monitor patients and deliver therapies to save lives.

Dr. Arman Shehabi

- Staff scientist at Lawrence Berkeley National Laboratory.
- PhD from U.C. Berkeley in environmental engineering focused on lifecycle assessment, which is energy and environmental systems modeling.
- Author of some of the most widely cited journal articles on global data center energy use
- Lead the Advanced Manufacturing Sustainable Analysis Team, which supports the strategic Analysis Group at Department of Energy and advanced manufacturing office.
- Looking at IoT across the manufacturing sector and what the energy and environmental implications will be for manufacturing IoT devices.
- Work looks at emerging technologies and tries to predict what sort of issues might arise to enable a smoother transition to a new technology.

Review of IoTAB Charter, Scope, Expectations

Presentation for this section can be found on the NIST website at: PowerPoint Presentation (nist.gov)

Ms. Kahn, Federal Working Group Co-Convener

- The IoT Advisory Board (IoTAB) and the IoT Federal Working Group (IoTFWG) are submitting reports to Congress. The IoT FWG will include the group's response to the recommendations in the IoTAB report.
- The authorizing legislation for the IoTAB is Section 9204 of the William Thornberry National Defense Authorization Act (NDAA) Public Law 116-283, which calls for the creation of the Internet of Things

advisory board committee and the Federal working group. The bill tasks both groups with examining barriers, to adoption of IoT devices in a variety of civilian use cases and gaining the economic benefits of those IoT devices.

- Ms. Kahn indicated that preceding the NDAA was the Developing Innovation and Growing the Internet of Things Act ("DIGIT ACT") which cleared the Senate in January 2020. Key points from the legislation:
  - The introductory language (Section 2) identifies a growing economy of IoT across market sectors and a focus on furthering innovation with a convergence on emerging technologies like AI to position the US to lead in the development of technologies for IoT.
  - Specifically, the bill calls out "the appropriate prioritization of a national strategy with respect to the Internet of Things [that] would strengthen that position" and through which "the Federal Government can implement this technology to better deliver services to the public."
  - This remainder of the bill identifies language similar to the NDAA in the responsibilities of both groups.
- Ms. Kahn indicated that it is important to look at policies and regulations that may be impacting the widespread adoption of IoT. At how IoT can be secured in order to make sure that we are utilizing it both federally and publicly. It is important to look at how IoT adoption is happening in both the public space and in the federal space.
- Ms. Kahn noted that the DIGIT Act identifies the fact that IoT is growing exponentially. Although this is from a few years ago, we are coming across a time when we are seeing the impact of devices.

Ms. Megas, Federal Working Group Co-Convener

- The IoTFWG is examining the federal side of things.
- The IoTAB is tasked with examining barriers in a wide range of industries and enablers that promote the use of IoT in those industries.

Ms. Kahn, Federal Working Group Co-Convener

- Ms. Kahn reviewed at a high-level Section 9204 of the NDAA on the IoT Advisory Committee duties and discussed the IoTAB Charter.
- Link to the Charter can be found here: **https://www.nist.gov/system/files/documents/noindex/2021/12/20/IOT-Board-Charter-20211215.pdf**

Designated Federal Officer (DFO)

Ms. Cuthill, Designated Federal Officer

- Designated Federal Officers (Ms. Cuthill / Mr. Brewer) will call all Board and subcommittee meetings; prepare meeting agendas as they are set by the Board; attend all Board meetings.
- The charter calls for the IoTAB to meet at least three times each year at the call of the DFO in consultation with the IoTAB Chair.
- The IoTAB is expected to complete the report to the Federal Working Group within one year.
- While IoTAB is not set up for formal subcommittees, the IoTAB can have informal subgroups that meet to gather and consolidate information to present to the broader IoTAB. The subgroups cannot engage in deliberations but only preparation of materials for meetings in which the actual deliberations and decisions will take place in a public setting.

- DFO also prepares Federal Register Notices, which explain the agenda, making sure it gets up on the website and working with the chairs to formulate the agenda.

Questions on the IoTAB Report:

- Mr. Bergman asked who has the authority over the publications of the report? Who has the approval over publication?
  - Ms. Cuthill responded that it is the IoTAB's report once the IoTAB reaches consensus. Then, the IoTAB report is delivered to the IoTFWG. There is no government official who reviews or approves the report. It does not go through an agency or inter-agency approval process.
- Mr. Bergman recommended the working group formulate a schedule to complete the work in one year.
- Ms. Megas added that the IoT FWG will absolutely have the interagency process for its report, and we will have to ensure that our IoT FWG members go back to their respective federal agencies and have that buy in, but this does not apply to the IoTAB report.
- Mr. Chan asked if the IoTFWG wants interim inputs?
  - Ms. Kahn replied that the IoTFWG does not require an interim report beyond the final report.

Question on Recommendations to the IoTFWG:

- Mr. Katsioulas asked if there is something that we can recommend earlier than the final report?
  - Mrs. Megas said that there will be published minutes at the end of these meetings. There is nothing to stop the group from saying, 'We have this recommendation'. The IoTFWG would like to encourage this so that it can begin considering those recommendations.

IoT Federal Working Group Overview & Relationship to IoT Advisory Board

Ms. Kahn, Federal Working Group Co-Convener

- The IoT Federal Working Group (IoT FWG) is comprised of seventeen Federal Agencies:
  - National Institute of Standards and Technology
  - Department of Homeland Security
  - Department of Energy
  - Office of Management and Budget
  - National Oceanic and Atmospheric Administration
  - Food and Drug Administration
  - Department of Agriculture
  - National Telecommunications and Information Administration
  - National Science Foundation
  - Consumer Product Safety Commission
  - Environmental Protection Agency
  - Federal Communications Commission
  - Department of Transportation
  - Federal Trade Commission
  - Department of the Interior
  - Office of Science and Technology Policy
  - General Services Administration
- Ms. Khan noted that lots of entities are talking about federal IoT usage.
- While the federal government is trying to broaden IoT adoption, agencies do not talk about IoT inhibiters for several reasons.

- If the private sector is coming across things that inhibit adoption, these are important for the report.

Ms. Kahn, Federal Working Group Co-Convener

- Ms. Khan reviewed the duties of the IoTAB according to Section 9204 of the NDAA which states that the advisory board shall advise the working group with respect to
  - The identification of any federal regulations, statutes, grants practices, programs, or budgetary or jurisdictional challenges that could inhibit the development of IoT.
  - Situations in which the use of the IoT is likely to deliver significant and scalable economic and societal benefits to the United States, including benefits to smart traffic, logistics and supply chain, sustainable infrastructure, precision, agriculture, environmental monitoring, public safety and health care.
  - Whether adequate spectrum is available to support the IoT as it grows, and any legal or regulatory barriers that exist to providing spectrum in the future.
  - The identification of any policies, programs or activities that promote or are related to the privacy of individuals who were affected by IoT, activities that may enhance the security of IoT, including critical infrastructure, protect users of IoT, or that may encourage coordination among Federal agencies with jurisdiction over the IoT.
  - Opportunities and challenges associated with IoT technology by small businesses.
  - Any international proceeding, negotiation, or matter affecting the IoT to which the U.S. should be a party.
- Ms. Khan reviewed the interaction between the IoTFWG and the IoTAB. The IoTFWG will provide the following inputs to the IoTAB:
  - Consult with the IoTAB regarding expertise needed for the FWG report (NDAA Section 9204 b(4)(A))
  - Provide suggestions on topics or items for the IoTAB to study (NDAA Section 9204 Section b(5)(E)(ii)
- The IoTAB will provide the following inputs to the IoTFWG:
  - Recommendations related to the Duties as specified in the FY21 NDAA—details in the IoTAB Charter (NDAA Section 9204 b(5)(B))

Questions about the final report and the IoTAB meeting schedule:

- Mr. Chan noted that the IoTAB has one year to write the report and asked what the Advisory Board will do once that is submitted?
  - Ms. Kahn replied that, according the NDAA, this group will stay intact until the IoTFWG report is finalized and submitted. There will be no further meetings.
- Mr. Chan asked if there will there be more than three IoTAB meetings?
  - Ms. Cuthill said that the charter calls for a minimum of three meetings and noted it would likely be challenging to do more than six meetings in a year.
- Mr. Chan asked if there would be any in person meetings?
  - Ms. Cuthill said that hybrid meetings would be possible. They would have to be held in a space that accommodated public in person attendees as well

Question about inviting speakers:

- Mr. Tseronis noted the value of having speakers who could discuss smart cities and suggested that there was a lot of activity in the DC area and experts who could come and speak about these challenges.
  - Ms. Cuthill confirmed that the Advisory Board members can identify experts to speak to the Board at any time. Members should work with the Chair and Vice-Chair to add speakers to the agenda.

NIST can help to support this effort by identifying subject matter experts in particular areas that the Board has identified as important. The Chair and Vice-Chair need to set priorities, balancing the time for speakers and the time required for discussion.

Questions about global IoT:

- Mr. Katsioulas recalled the earlier discussion on building trusted networks, noted that devices have chips from abroad and asked if the Board was going to focus on the global aspect of IoT, including collaboration with allies in the European Union, the Pacific.
  - Mr. Caprio agreed that IoT's impact is global and suggested that he looks forward to working with other members of the AB to look for opportunities to amplify our work internationally.
  - Ms. Cuthill noted that the legislation refers to an international component and pointed out that virtual meetings made the inclusion of international speakers much easier if they could work around the time zone issues.

Federal Advisory Committee Act (FACA)

Ms. Cuthill, Designated Federal Officer

- This Federal Advisory Committee came about as a result of the Federal Advisory Committee Act (FACA) of 1972 (Public Law 92-463). The U.S. Congress was trying to provide a consistent framework for federal advisory committees.
- Congress sought to assure that advisory committees provided advice that would be considered relevant, that the process would be reasonable and transparent, and that it would provide consistent record keeping.
- The Government in the Sunshine Act of 1977 made some amendments to the FACA. GSA now manages the whole process across the federal government (GSA Federal Advisory Committee Management Final Rule).
- This process is to be transparent and open to the public. Detailed meeting minutes will be taken and published. Any slides presented during meetings, and all comments submitted by the public will be part of the official meeting record and will be publicly available on NIST's website.
- There is a Designated Federal Officer (DFO) who manages the Secretariat side of this process. The DFO makes sure that the Board stays within the framework; calls meetings and posts them to the Federal Register; provides recordkeeping; keeps track of NIST's costs; and publishes all documents. The DFO provides copies of reports, which ultimately go to the Library of Congress.
- The committee has to be chartered, and that charter must be registered with GSA before the Board can meet. The charter provides the scope, and it is a very important foundational document for the work of the IoTAB.
- The Advisory Board must be balanced and diverse.
- The Board must be independent. The advisory committee is providing independent advice to the Federal Government, and it should not be influenced by any special interest.
- Meetings are announced in the Federal Register 15 days in advance and are required to be open to the public. This advisory board does not meet any of the exceptions to this rule, so all of our meetings, for the entire meeting, are open to the public. Both virtual and in-person meetings must include the public virtually and in person also.
- The IoT Advisory Board provides that transparent participation from citizens outside the Federal Government which improves trust, and the actions can then be easier to implement because there's clear outside expertise that has developed those recommendations.

- GSA maintains a database of all federal government committees, showing how much each agency is spending on each one of these committees: the time that we spend and the contractor support in order to make sure we are efficient.
- All meeting documentation will be posted to the NIST website within 90 days of each meeting.
- Preparing information for meetings can be done outside of meetings, which may involve people talking to each other. The question has come up regarding "what can be done outside of meetings?" You can prepare for meetings; you can prepare documents for the meeting, but the work itself and the key discussions that need to take place must take place in those public meetings.
- Advisory Board members may not speak on behalf of the Advisory Board unless authorized and Board members may not use their position for their own personal benefit or promotion or engage in "grass roots" lobbying.

IoTAB Operating Model discussion

Mr. Chan, Chair

Mr. Chan shared an initial version of a framework to guide the discussions. Framework

- Mr. Chan emphasized that:
  - The IoTAB has only one year to write the report and send it to the IoTFWG.
  - The members need to identify speakers that the IoTAB needs to bring in to further this effort.
  - This high-level outline is offered as a starting point for what the report could look like.
  - Feedback is always appreciated.
- Mr. Bergman asked if challenges could include things that need to be done to take advantage of opportunities?
  - Mr. Chan noted that it could include challenges. The IoTAB has complete freedom. The IoTAB could say these are challenges, and these are opportunities for those particular challenges. Mr. Chan asked how the IoTAB would want to organize it?
  - Mr. Caprio said that there is a lot of attention on this and the IoTAB doesn't want to give short shift to the challenges, because there are some, but we really want to highlight the opportunities.
- Mr. Bergman stated that his reaction comes from seeing the detail under the section, 'key challenges'. The opportunities and value of IoT could be a couple of paragraphs. Infrastructure standards may need some elaboration. Opportunities could get similar treatment as the challenges.
- Mr. Chan reminded the members that this was a way to give an idea of what is inside the sections.

Question on efficacy of existing policies:

- Ms. Lam asked how much the IoTAB is assuming that certain plans and policies are in place that would address some of the challenges? How much are we incorporating some of the ongoing efforts and polices - inequalities across the country? Connectivity is still an issue in different parts of the country. The Inflation Reduction Act would address some of the inequities.
  - Mr. Chan replied that there may be shortcomings in some of those policies and asked if members could identify where those policies fall short. The bipartisan infrastructure law is supposed to address some things, but it is lacking broadband, for example. For farmers, the broadband connection goes to the farmhouse, not the field, for example.
- Mr. Caprio reminded everyone that this was intended as an exercise to lay out an approach. Beginning with the end in mind. This can be tweaked, revised, extended.

Sector specific verticals/horizontals:

- Mr. Bergman pointed out that the topic specific challenges are sector specific:
  - Vertical challenges are healthcare and agriculture - top to bottom.
  - The horizontal challenges are cybersecurity, privacy, and international proceedings. May want to separate out and treat these as non-sector specific with the option of suggesting topic specific challenges.
  - Suggest topic specific challenges be called sector specific challenges. Need an equivalent one for cross sector challenges.
  - Mr. Katsioulas concurred and noted that data supply chain security across the horizontal issues tend to be applicable to many verticals.
- Ms. Raimundo stated that her work is to support government deployments and how to make them work in communities. The challenge is the gap in skillsets and education, especially in public sector and rural communities.
- Ms. Mehra said that given the number of touchpoints across industries and the 16 critical infrastructure sectors, education is the entire gamut. A framework is going to include some type of a dashboard that provides a methodology to look across these individual components and show the current state and the prioritization.
- Prof. Kornegay stated that he would also like to add the socio-economic impact of the digital divide, the growing aging population with regards to technology adoption.
- Mr. Chan noted that in his smart city work one of the big gaps is that the user experience is terrible because it is designed for people who are digital savvy and presents problems for a lot of people don't have mobile phones, or are vision impaired, or don't speak English, or work two jobs. The last thing such users want to do is go onto a website and look for something or call into customer support.
- Mr. Katsioulas asked how the Board could come up with a methodology to be able to structure between vertical markets and the horizontal issues that we have to worry about in order to convince the government to invest in this very important opportunity? Essential for competing with adversaries.
- Prof. Kornegay mentioned how crucial the notion of bias is in the discussion of equity, particularly in health care. Using IoT devices and AI you can come up with an incorrect diagnosis. This could lead to a fatal consequence. This should be included across all sectors. He acknowledged that he was not sure if this issue is horizontal and vertical or if there's an opportunity for a 3D perspective.
- Mr. Chan added vendor algorithm bias under cross-sector challenges for now.
- Dr. Chandra suggested including innovation and where things are heading. This is related to a previous comment. How do we accelerate these innovations to get these to market? Make sure we are ahead of the curve in the adoption of IoT.
- Ms. Lam noted that there are verticals and some horizontals in terms of larger crossover but what pulls it all together is some sort of place based IoT at whatever scale that you're talking about.
- Mr. Chan suggested that it could be along a vertical or along some more issue based specific term but at the end of the day it is about application to the place and to the people.
- Mr. Bergman noted his interest in putting it after the sector specific challenges.
- Ms. Lam suggested that this goes towards the end with things that go beyond the specific silos into something that's more cross integrated as a whole category, a comprehensive viewpoint.
- Mr. Chan added this suggestion of a potential feature speaker topic.
- Mr. Bergman suggested that the IoTAB look at the scope that the IoTAB is addressing. One definition is an IoT device is one that is connected to the internet, or it has a sensor and an actuator. Well, a sensor is a camera, and a laptop has a camera, so is that an IoT device?
- Prof. Kornegay agreed that the Board needs to be on the same page about what an IoT device is.

- Mr. Katsioulas noted that Fostering the Advancement of IoT from 2017 defined any electronic device that is connected is an IoT device. Connectivity opens it up to security risk. Mr. Katsioulas asked if a rack server in a data center is an IoT device?
- Mr. Bergman said that he believed that it is. It is connected to the outside world.
- Mr. Chan suggested that the Board should ask NIST for a definition of an IoT device?
- Prof. Kornegay noted it depends on the application. The Board needs to spend some time on this. The Board has an opportunity to define or shape that as a group.
- Mr. Katsioulas agreed. Think of a hyper connected world, 10 years out.
- Ms. Kahn pointed out that the IoTFWG has been using the NIST definition first published in NIST IR 8259 and adopted in the IoT Cybersecurity Improvement Act. This Board needs to come up with the definition that suits the purposes of this report.
- Ms. Megas expressed concern that if the Board tries to define IoT they may spend a lot of time coming up with the exact words. The IoT Cybersecurity Improvement Act has been beneficial. To use the anti-pattern - what is not an IoT device? It may take a lot of time to hone the definition. The device is part of the technology. The desire is to look at the adoption of the technology broadly.
- Mr. Chan noted that the definition used by the Board will ultimately impact the IoTFWG report. The IoTFWG may be looking at it from a different perspective.

Analysis Framework for Capturing and Classifying Challenges

- Mr. Chan shared a slide which included a preliminary list of categories for gaps and challenges that could fall into a framework. The columns showing development, adoption and operation/use are parts of the IoT lifecycle.
- Each industry area will likely have some similar challenges, and some industry specific ones. The idea is to capture them in this framework.
- Mr. Chan invited members to provide a 10-minute speech/presentation on the benefits, opportunities, barriers, etc. of IoT from their perspective.

Board Member Statements

Mr. Tom Katsioulas

Mr. Katsioulas shared slides which can be found here: Katsioulas Presentation (nist.gov)

- Want to look ten years out. It will be a hyper connected world which will be enabled by IoT devices and fueled by chips. Everything will be connected and will be more complex.
- Society will enable connected value chains and marketplaces - drive trillions of dollars in economic growth.
- Growth will be impacted by global supply chain and cybersecurity risk vulnerabilities.
- Must take actions with international allies to create trusted networks and collaborating ecosystems. A new wave of public private partnerships that will align incentives and standards to create marketplaces for the world.
- Semiconductor enabled devices will grow to 1.5 billion by 2030. Semiconductor industry will provide the fuel for those devices.
- Good news is that the US and the CHIPS Act will increase production capacity.

- McKinsey recently revised their 2014 projection. They created 9 settings. Went through different factors from adoption rates, impact and scale. Mr. Katsioulas encouraged everyone to look at this 2022 report.
- The interconnection among different sectors is what really will create the hybrid opportunity of scaling so that a product that comes from manufacturing can connect to another product that comes from agriculture.
- Mr. Katsioulas cited an older Harvard Business Review article about how products evolve. Connected products evolve into systems and that systems essentially create platforms or ecosystems that can be monetized.
- Companies whose product systems connect to other product systems would be able to essentially capture much more value. That's where different products come together in connected value chains.
- Systems from different IoT products can connect to full ecosystems. That is extremely important because the business revolution can then follow.
- Different markets will evolve at different rates. And of course, consumers will lead the way.
- What's the connectivity impact in getting there? What is technology, performance and power in enabling that?
- Finally, the next question is how do we scale? And the only way can scale is to create trusted networks and platform-based business ecosystems. And that's where supply chain comes into play.
- Another problem is supply chain of chips going to devices. The chips, even though developed in the United States, they are manufactured somewhere else. A drone going into Ukraine territory, and you open it up and it's full of Western chips.
- Key message here is that lack of supply chain visibility and traceability threatens national security and also threatens economic prosperity.
- Question for this team. How do we scale this into the entire value chain across marketplaces?

Mr. Steven E. Griffith

- National Electrical Manufacturers Association (NEMA) represents more than 325 electrical equipment, and medical imaging manufacturers, responsible for about 1.65 million American jobs contributing more than $200 billion to the US economy. NEMA drives growth through systems development, business intelligence, and advocacy at all levels of government.
- The electric industry is evolving. Electrification, digitalization, globalization, environmental concerns, workforce development, changing business conditions are all disruptive technologies and of course, opportunities and challenges for manufacturers.
- One challenge is IoT. Harnessing IoT gives manufacturers the ability to optimize their operating efficiency by using robotics and automated machinery. They can boost productivity and streamline productions using sensors.
- Manufacturers can: gain insights into operational performance of equipment and entire systems; reduce operational and manufacturing errors; make recommendations to improve a process using predictive maintenance IOT technologies which reduce down time; incorporate sensors to bolster worker and product safety; ultimately provide cost reduction.
- One challenge is in the definition of IoT. There is consumer IoT (smart phones), and industrial IoT (IIoT), which is used for industrial processes like manufacturing monitoring supply chain. There is a tendency to place the IIoT and consumer IoT in the same category.
- Many of NEMA’s member companies manufacture industrial control systems or ICS.

- ICS uses supervisory control, data acquisition systems, and distributed control systems. Sensors can collect data from equipment and see the data analytics. Machine learning can learn from data and fine tune.
- IoT can also enable remote monitoring of systems located in harsh environments.
- One of the big challenges is data. IoT devices and systems generate a large amount of data. For IIoT, analysis of the data can be used to improve the process whereby these devices are produced.
- This is totally different from personal data that can be shared by different consumer devices, which is subject to regulations like GDPR and HIPAA. These devices are dynamic in nature, and capable of evolving into unanticipated use cases.
- One of the biggest challenges with the IoT is cybersecurity. The supply chain is facing threats from different types of malicious actors. Electrical manufacturers have voluntarily adopted industry cybersecurity standards.
- One of the standards that is used quite a lot across industry is IEC 62443. Standards offer a pragmatic approach to cybersecurity. Every stage of cybersecurity is covered from risk assessment through operations.
- NIST offers good voluntary guidance in the Cybersecurity Framework. Maybe there's an opportunity to leverage that framework in our discussions here.
- Looking at the smart home ecosystem in a household there are several smart home devices that may not always be cross compatible. There is a new open standard called Matter, which allows devices from different manufacturers to talk to each other.
- Spectrum is another focus area particularly with respect to vehicle technologies. Connected vehicles that communicate safety messages to infrastructure. Recently, the FCC reallocated a portion of the 5.9 gigahertz band. It was set aside for vehicle communications. It is conceivable that more spectrum will be needed in the autonomous vehicle space.
- When properly, responsibly governed and applied, IoT can achieve these efficiencies by enhancing workers safety and privacy.

Questions and Dialogue Post Presentation:

- Mr. Katsioulas: Mr. Katsioulas noted that automation is the biggest area for the creation of economic value. He stated that Mr. Griffith had touched all the important points. Digitalization of brownfield environments is a challenge. He recommended that the IoTAB bring in someone who is leading in that space to give the Board some insight.

Prof. Kevin T. Kornegay

Prof. Kornegay shared slides which can be found here: Kornegay Presentation (nist.gov)

- Prof. Kornegay is at Morgan State University and particularly interested in the convergence of 5G, IoT and AI. Prof. Kornegay has established an isolated infrastructure for connected devices on campus separate from the university infrastructure. This is a zero-trust software environment where hundreds of devices in an ecosystem spanning across several buildings on campus, a connected car, and a representation of a smart city.
- Prof. Kornegay indicated there are challenges going from the edge to the cloud. He said his team is taking a layered security approach – including methods such as side channel analysis, reverse engineering, and anomaly detection across layers of the stack. They are examining solutions to mitigate various attacks. From a research standpoint his team is interested in the security and privacy lifecycle.

- Prof. Kornegay discussed risk topics such as: knowing normal behavior assists in determining a deviation or an attack, the importance of provision and decommissioning devices, and the risk of legacy devices and patch management.
- Prof. Kornegay identified issues for policy such as: ownership of the data, the lifecycle of processed/collected data, profiles that could be created from understanding the data about a user from observing patterns in use.

Mr. Benson Chan

Mr. Chan shared slides which can be found here: Chan Presentation (nist.gov)

- Mr. Chan presented material from IoT Technology Infrastructure Gaps Research he has been involved in over the last two and half years, under a NIST grant. He described the study's tasking and the industries they elected to analyze, saying that the industries were selected based on their contributions to the GDP, the potential for IoT to have a significant impact, and their implications for US economic security.
- Mr. Chan described five stages of IoT evolution that the study used as a framework, looking forward over a 30-year or longer period. The framework projects that improvements in IoT data and AI algorithms will enable greater automation in 5-10 years and will evolve toward a "hyperconnected autonomy" that will require an infrastructure designed to supports that. Mr. Chan observed that we are still a long way from truly "smart" capabilities, despite the use of that label today.
- Mr. Chan describe "accelerators" to move toward hyperconnected autonomy, and the various elements of the overall evolution. Some dimensions of this are:
  - Moving from vendor "walled gardens" to cross-vendor and cross-industry extended ecosystems of devices;
  - Moving to truly trusted systems; here Mr. Chan drew a parallel to the aviation industry;
  - Development and testing of ethical computing.
- Mr. Chan presented the report's draft list of technology areas for investment to enable the future of IoT he had been describing. He identified several areas of particular importance: interoperability and standards, security and privacy, and user experience. He said these topics would be mapped back to the economic analysis in the report.
- Mr. Chan then presented the potential areas for future research, noting the reports covers a broad span of items based on the input they had received. He again emphasized the importance of infrastructure, saying that our current infrastructure isn't prepared to drive adoption of massive volumes of IoT. Other areas he pointed out are sensors, chipsets and processor capabilities, and energy harvesting to reduce dependence on batteries.
- Mr. Katsioulas asked for clarification on what Mr. Chan considered the scope of infrastructure. Mr. Chan included both the network infrastructure and the compute infrastructure. He cited the potential for massive expansion in edge computing, and the challenges of power and data transfer, and said "foundational research" was needed to enable these concepts.

Mr. Peter Tseronis

Mr. Tseronis shared slides which can be found here: Tseronis Presentation (nist.gov)

- Mr. Tseronis noted the sixteen "critical sectors" the government deems vital to national security, emphasizing that these are sectors, not federal agencies, and that the definition comes from DHS. He stated that "transportation, climate, energy, the environment, and broadband" are the things that all

sixteen sectors are tied to, and that federal agencies all align to these sectors, which are generally owned and operated commercially. Recent laws have provided substantial funding and opportunity to innovate.

- Mr. Tseronis then discussed risk, stated that the mission is to mitigate risk because it cannot be eliminated. He said that risk mitigation needs to be addressed in the context of "mission", rather than technology. He then pointed to the documented National Essential Functions, which align to the critical infrastructure sectors. He said the IoTAB could address the critical infrastructure sectors and essential functions in a plainspoken way.
- Mr. Tseronis displayed an organizational chart of the federal government, and pointed out the large number of agencies, and addressed the primary role of government to facilitate improvements in infrastructure and cybersecurity.
- Mr. Tseronis identified challenges and opportunities:
  - He stated that there are enough tools, but hard work is needed to integrate them, including related workforce development, noting the goal to create "a 21st century workforce".
  - He stated that compliance is a requirement but can't be a killer of momentum and suggested that proof of concept and pilot efforts can help when standards are still under development.
  - He described "reskilling, retaining, and recruiting people" suggesting that it is important for everyone to try to understand technology and how to benefit from it.
  - He stated that the US has to deal with constant transition, noting that critical infrastructure remains a constant concern regardless of changes in political leadership. He reported the statistics that a modern car has 63 endpoints on Bluetooth, describing it as "a network on wheels" and expressing concern about its risk in the context of smart cities.

Mr. Michael Bergman

- Mr. Bergman identified his current role in the Consumer Technology Association (CTA) as Vice President, Technical Standards, and noted the breadth of connections CTA members have to different IoT-related topics, saying that CES has become "an IoT type of show". He said that CTA is an ANSI-accredited standards body, producing standards for a variety of topics including cybersecurity, health and fitness, audio/video and more. He noted that almost everything CTA works on touches on IoT in one way or another.
- Mr. Bergman noted the broad range of topics the IoTAB would need to consider, per its charter, to achieve its purpose. He indicated that CTA members have experience with most of the areas the board needs to address, and said CTA has perspectives on specific categories:
  - Recommendations in the area of augmented logistics and supply chain should not promote government mandates for "onshoring";
  - For supply chain risk management, the board should discuss developments in anti-counterfeiting and anti-tampering technologies for chip and systems; additionally, the use of hardware, software, and digital bills of materials (HBOM, SBOM, DBOM), and applications and systems that can measure supply chain, performance and increase supply chain optimization;
  - The adoption of home automation products could significantly reduce energy consumption and reduce emissions;
  - Personal safety should also be considered under public safety; the focus here is how IoT can help protect individuals including in the context of authoritarian governments;
  - The report should urge continued government release of licensed and unlicensed spectrum for IoT use.
- Mr. Bergman also presented CTA views on horizontal topics that apply regardless of sector:

- Regarding privacy, IoT should be treated no differently than other categories, except for the collection of data on hardware devices, which should be covered under cybersecurity;
- The IoTAB should support a federal baseline privacy law, based on a uniform, technology-neutral privacy framework;
- The report should acknowledge the on-going public / private effort to establish a national cybersecurity label for IoT;
- The report should support expansion of the WTO's Information Technology Agreement (ITA) and encourage plurilateral tariff elimination.

Comments and Questions Following Mr. Bergman's presentation:

- Mr. Katsioulas expressed the belief the IoT label will lead to additional labels for specific sectors. He noted the Carnegie Melon research on labels did not address SBOM and DBOM. Mr. Katsioulas believes cyber security labels need to go down to the level of BOMs.
- Mr. Bergman replied with two points:
  - The national consumer connected label is a US program primarily driven by the private sector, creating a framework using NIST consumer profile criteria. Those criteria would be joined by enterprise or other sector criteria to meet different needs and requirements.
  - SBOM and HBOM can be considered in context of those technical and non-technical requirements. One of the standards referenced by the program, CTA 2088, considers SBOM as important as soon as it is mature, which is developing under efforts led by CISA. SBOM, HBOM, DBOM, and secure provenance will become a priority as the label program evolves over time.

Ms. Ann Mehra

Ms. Mehra shared slides which can be found here: World of IoMT (nist.gov)

- Ms. Mehra focused her statement on the Internet of Medical things (IoMT). She reported there are tens of thousands of medical devices around the world, creating a significant portion of the economic activity attributed to IoT, and the US is the leading country with regard to IoMT.
- Ms. Mehra shared the World Health Organization (WHO) definition of medical devices, believing it would be helpful for the board's consideration of the definition of IoT. She also noted the existence of the WHO's Global Atlas of Medical Devices as a reference.
- Ms. Mehra described the large number of devices commonly used in different medical contexts and agreed with other members' remarks about the lack of standardization. She explained that the scope of IoMT should include the cameras that monitor medical facilities and noted the extensive amount of hacking focused on medical records and IoMT devices. She cited insulin pumps and implanted cardiac stimulators as the most hacked medical devices.
- Ms. Mehra described a Journal of Biomedical Informatics study that took an 18-year historical view on IoT's adoption into medicine and noted that the major contribution of IoMT have been in homes. She said the extensive use of IoMT in the home created another complication due to lack of standards and the large volumes of data exchanged among interested parties create a significant opportunity to intercept that data.
- Ms. Mehra made a recommendation regarding the need for Unique Device Identifiers (UDIs), based on work done under the FDA. She also suggested engaging with the FDA-associated organizations that developed related recommendations or inviting those organizations to speak to the board.

Comments and Questions Following Ms. Mehra's presentation:

- Mr. Katsioulas endorsed the device identifier requirement but stated that a digital paper trail was needed to have enough information for proper security, and that there would need to be many identifiers.
- Mr. Bergman said he thought the device identifier would make a good recommendation and noted that there are many ways to approach that need. He said he wanted to further understand the need in a medical context, and noted that the emerging technical standards for IoT cybersecurity, including the NIST consumer profile, all call for a device ID.
- Mr. Katsioulas connected the device identifier need to NDAA requirements for supply chain traceability and described it as a long-term infrastructure problem.
- Ms. Mehra suggested vaccine management, including development and distribution, as a good supply chain case to explore due to the mixture of associated requirements. Mr. Bergman requested Ms. Mehra provide a written description of that use case.

Dr. Arman Shehabi

Dr. Shehabi shared slides which can be found here: Shehabi Presentation (nist.gov)

- Dr. Shehabi said that he is a Staff Scientist at Lawrence Berkeley National Lab (LBL) who examines the implications of emerging technology using a system-wide assessment, life-cycle approach.
- He explained that in considering IoT it was necessary to consider new physical elements, the data that would be required, the equipment required to handle that data, and the variety of places that equipment might operate. He said it would be important to consider the circularity requirements for a mixture of long-lived and short-lived devices, and how IoT technology might change the environment around it.
- He described to the board a large report LBL has nearly completed for DoE looking at the implications of advanced manufacturing and the connected economy. He said IIoT is a large part of smart manufacturing, and that he believes the report will be a helpful input for the IoTAB.
- He identified challenges he believed were important for the board, citing the example of global supply chains, and suggesting the board would need to think on international level, considering equipment coming from different manufacturing stages in different geolocations.
- Dr. Shehabi believes there is great uncertainty regarding the impacts of IoT; he stated he is bullish on IoT but there can be secondary effects that must be considered.
- He summarized saying he saw the need to understand future applications at a sector level, the equipment and infrastructure to meet applications, and finally what manufacturing will be needed to meet those equipment and infrastructure needs.

Mr. Dan Caprio

- Mr. Caprio stated he has a background in technology policy and has been working for 20 years on IoT. He said his focus on the future: where do we want to be in 10 years?
- Mr. Caprio said he thinks about privacy, cyber risk, and data risk, and is hopeful there will soon be a federal privacy law, and that he hopes the board's work will lead to more secure IoT devices in the next decade, noting that we "face a very persistent adversary", so there's a need to focus on cyber security.
- Mr. Caprio stated his other focus area is international cooperation, especially with the European Commission, and that he sees opportunity for collaboration regarding standards.
- He said that while the board's charge is US competitiveness and growth, he believes they also need to consider the global economy, as we face real geopolitical risks and should work with countries with which we share common values.

- Mr. Caprio concurred with other panel member statements that he sees IoT as building block to Artificial Intelligence.

Comments and Questions Following Mr. Caprio's presentation:

- Mr. Katsioulas suggested that an important question was what percentage of the global economy can the US command, and how can we take advantage of the capabilities of leading innovation companies based here.

Ms. Debbie Reynolds

Ms. Reynolds shared slides which can be found here: 20230118_IoT-AdvisoryBoard_Reynolds_Statement (nist.gov)

- Ms. Reynolds said she has been a technologist for more than 20 years and works with companies engaged in digital transformation and extensive use of data. She cited a number of statistics regarding the exponential growth in data and connected devices, and the rapidity with which devices are attacked. She also noted that a significant number of countries (128 of 194) have legislation protecting data and privacy, and the concerns consumers have about losing civil rights because of IoT, including both consumer and industrial IoT applications.
- Ms. Reynolds described the "two major sticking points" regarding data privacy are collection and retention, noting the interactions that can happen among organizations involved, and the value of data encouraging its collection. She observed that many devices are designed without consideration of privacy or cybersecurity, something she described as a "wait until something bad happens" approach. She also described a concern that consumers lack means for adequate legal redress in the case of harm from data collection and misuse.
- Ms. Reynolds identified other concerns:
  - The increase of risk to consumers created by the expanding capabilities from IoT innovations combined with the use of AI. She said she was in favor of cybersecurity labels for IoT devices.
  - The concern of bias in automated devices, and the potential for inaccuracy in operation dependent on race (e.g., with medical diagnosis devices).
  - The challenges of interoperability with large numbers of devices operating in more decentralized architectures.
  - Appropriate access for IoT users to understand what devices are doing and how that may change over time, the impact of a security label getting out of date, and the lack of universal customer access to smart phones to access updates and updated information.
- Ms. Reynolds described her professional areas of focus as data collection and use, privacy by design (including associated standards) starting at device inception, technology development; technology adoption, and customer education at all levels.
- Ms. Reynolds emphasized the need for the board to think in strategic terms, think proactively about risk, anticipate the potential for harm, and anticipate the future to maximize the value of the board's report.

Ms. Maria Rerecich

- Ms. Rerecich described her role at Consumer Reports (CR) as evaluating the data privacy and security for consumer IoT devices and identifying challenges in that space. She emphasized that with regard to privacy the concerns were not only about risks from bad actors but also the data privacy policies and practices of manufacturers.

- Ms. Rerecich describe a set of criteria CR has developed to define "goodness" for IoT products and services, which they call "The Digital Standard" (details can be found at thedigitalstandard.org). She said the standard addresses four areas, each of which is summarized with a question:
  - Security - Is it Safe? How resistant is a product to cyber-attack?
  - Privacy – Is it private? What are the data permissions and sharing policies, and do consumers have control over their own data?
  - Governance – Are they good? Are the company's policies good for the consumer?
  - Ownership – Is it mine? This considers concepts like right to repair, and permanence of expected functionality, especially at product end of life or in disconnected situations.
- Ms. Rerecich said CR currently applies a subset of this broad umbrella of criteria to consumer product evaluation, and that she believes they can be applied horizontally across the broad range of topics for the IoTAB.
- Ms. Rerecich identified what she considered the main considerations and the principles that should apply:
  - Data privacy, transparency & control – consumers can easily know what data is collected, are given informed choice about collection, and can have data deleted when they stop using the service.
  - Data sharing: companies should be clear about what data is sold, to who, and for what purposes; she noted that only citing "trusted business partners" isn't enough.
  - Data minimization: by default, only collect what is necessary for use of product or service; many privacy policies are not specific (collect "for other purposes").
  - Right to repair / right of ownership: she noted these concepts used to be a given with consumer products, but now with integration of software have become less assured, citing the example of manufacturer restrictions on tractor repair. She reported that products have "bricked" when their manufacturers shut down service, which is contrary to consumer expectations about ownership and continued functioning without network connections.
  - Security over time: Manufacturers should commit to continue to support with security updates for a specified number of years and be clear about that.
  - Security & privacy should be designed in; consumers expect products should be safe & secure, but many are "not great"; CR has seen products send lots of sensitive info unencrypted; has demonstrated the ability to take remote control of smart TVs; and other demonstrations of security shortcomings; all problems that she believes should have been taken care of up front.
  - Privacy By Default, a product should be set to be most private by default with opt-in to greater data collection; "privacy is a right, not a setting".
- Ms. Rerecich stated she thinks these concerns and concepts apply across the big verticals, and that she looked to represent the consumer to the IoTAB and hoped that security and privacy should be a priority for the board.

Ms. Debra Lam

Ms. Lam shared slides which can be found here: Lam Presentation (nist.gov)

- Ms. Lam emphasized the importance of data and noted that other members had raised "good concerns" about that. She related data to three types of infrastructure:
  - Physical, which is the most defined and visible, and has rules, regulations and policies about it;
  - Social, which is similar in terms of how societies are governed, and
  - Virtual, which she called "a very new thing".
- She said the convergence of these is important to IoT, is "the great unknown", and is very decentralized.

- Ms. Lam then discussed the importance of data, noting there had been lots of good discussion of risks and biases. She said she likes to think about "IoT for good", and that we can think more about the power of good once we have addressed the security and bias concerns. She described the need to think about data literacy and the power of applications that go beyond descriptive to predictive and prescriptive; how can this address inequalities and empower communities with data literacy.
- Finally, Ms. Lam related the goals to the United Nations set of 17 Sustainable Development Goals (SDGs). She noted there isn't a specific IoT goal, but thinks it relates to Sustainable cities & communities, and described IoT as a tool to address that, to empower people and address inequities through data and technology, as those are at the convergence of the three types of infrastructure.

Mr. Nick Emanuel

- Mr. Emanuel stated he comes from the agricultural and agriculture technical (ag tech) realm and stated his expectation that IoT technology will be introduced into all facets of agricultural production over the next several years.
- He noted it has been about 25 years since the first self-driving tractor was released to market, which he described as indicative that agriculture is often both the most technologically advanced sector or industry and also the "most lacking". Agriculture battles a hurdle between the development of technology and its adoption throughout the sector.
- Mr. Emanuel said we are entering a new generation of robotics plus IoT allowing for full farm automation and optimization; he gave the example of robotic tractors operating without a human present. He said these advancements would be "vitally important", enabling improved forecasting and planning accuracy, increased farm productivity, greater efficiency, and reduced waste all of which improve sustainability.
- Mr. Emanuel describe the applications of IoT in agriculture technology as similar to other industries, with the potential deployment of sensors throughout the production cycle, providing the ability to monitor:
  - Inventory management
  - Machines in the field
  - Crop health and growth
  - Dynamic variables such as weather, and soil moisture
- He said using IoT in this way improves efficiency and connects the entire supply chain ("field to fork"), giving full transparency of how food was derived.
- Mr. Emanuel described Nebraska's deployment of statewide full LoRa coverage a few years ago and observed that the use of LoRa has grown beyond agriculture production to many other industries. He said Nebraska was selected for the LoRa network due to the vast network of irrigation across the state. The LoRa network has allowed development of many more opportunities for IoT.
- Mr. Emanuel discussed barriers and challenges for agricultural IoT:
  - Broadband and network coverage (cellular, LoRa, etc.), where rural infrastructure is often the most challenging aspect.
  - Reducing cost and improving ROI for sensors to permit scaling up deployment; he also noted that batteries for sensors has been a notable challenge.
  - Security, data ownership, privacy, control over data
- Integration and open frameworks to enable partnership and allow scalability and adoption to improve over time.

Ms. Nicole Raimundo Coughlin

- Ms. Raimundo stated that she is based in Cary, NC, where she is CIO.
- Ms. Raimundo noted that Cary also has a LoRa deployment. She said that having the LoRa network introduces the question of "What does it mean to have a connected community?", noting that services often go beyond the boundaries of a city.
- She said that Cary has done a lot of work trying to figure out what "smart cities" really means, using their campus as a living lab. She said that challenges of integration, proprietary solutions, and limited resource quickly became evident.
- Ms. Raimundo noted that integration and open APIs are critical for what most municipalities want to do. She described exploring working to a larger scale and connecting to nearby communities, citing the example of sharing data from storm water sensors with Raleigh.
- Ms. Raimundo identified the benefits of smart infrastructure for a community saying that IoT enables connecting manual processes to save time and lives. She said that an event touches almost every single department, and the smart infrastructure enables sharing information to the media and the community.
- Ms. Raimundo described the LoRa network as being used for most IoT communications other than streaming camera video, saying most IoT interactions involved very tiny data. She said the LoRa network is easy to manage, cost-efficient, and could be offered as a utility providing a revenue source for the municipality or small businesses. She provided the example of a hotel using the network for tracking their rental bikes, plus gaining associated data about the bikes' use, describing this as one of "tons of use cases". She also cited that the LoRa network was easy to deploy, with Cary using their expertise to assist neighbor municipalities that lack technical expertise.
- Ms. Raimundo said she thinks the US works very differently than European countries on deploying such networks.
- Ms. Raimundo sees the biggest value coming from connection and integration and hopes Cary can be a model for others to follow.

Dr. Ranveer Chandra

Dr. Chandra shared slides which can be found here: Chandra Presentation (nist.gov)

- Dr. Chandra gave a brief presentation focusing on the potential benefit of IoT in addressing challenges in agriculture today. He noted the need to achieve a 50% growth in the world's food supply by 2050 and stated that data-driven agri-food systems can help address this need. Such systems would allow every element in the food supply chain to use IoT to improve their efficiencies, especially if these entities can share data securely and privately.
- Dr. Chandra focused his presentation on the use of IoT on the farm, and described the goal here as being to augment the farmer's knowledge with data. He described mapping farms and using data to determine soil moisture and nutrient levels. Such maps and data would permit precision agriculture to improve yields, reduce cost and water use, and improve sustainability.
- He stated that the cost of precision agriculture at scale has been a significant obstacle to adoption, and then discussed some approaches to reduce the cost and address related challenges on farm. He identified three particular challenges:
    - Connectivity in the middle of the farm: while the farmhouse may have adequate Internet connectivity the farm itself is at a distance, making connectivity to the cloud problematic. He described using the spectrum from unused TV channels to send data between fields and farmhouses, and noted the FCC has passed related regulations. Other communications options include private 5G and satellite communications.

  - Dense soil sensor deployments for soil monitoring are very expensive and difficult to deploy, so his team has developed techniques to combined aerial (or satellite) imagery with AI to plan sensor location, and machine learning models to combine imagery with more limited sensor data to create very accurate maps that can guide watering and fertilization activities.
  - IoT sensors create significant volumes of data that is difficult to send to the cloud. The use of edge computing at the farmhouse can significantly reduce volume of data sent to the cloud.
- Dr. Chandra illustrated IoT benefits for agriculture with some detailed examples:
  - Use of AI for detailed predictions to permit farmers to plan activities (e.g., herbicide application at appropriate temperatures)
  - Use of drone imagery to evaluate surface conditions and livestock locations.
  - Tracking livestock movement to assess animal health.
- Dr. Chandra concluded by describing related educational efforts, including the creation of Farm Beats student kits to build technology skills by teaching data analysis and AI techniques and their application to agriculture.

Mr. Randy Moss

Mr. Moss shared slides which can be found here: Moss Presentation (nist.gov)

- Mr. Moss described his particular interests with regard to IoT. He spoke to potential benefits in the areas of supply chain management, manufacturing, and procurement.
- Mr. Moss emphasized the importance of data in achieving these potential benefits, such as information dashboards, and the ability to generate alerts.
- Mr. Moss also reviewed some challenges in the areas of implementation and change management. He noted that challenges related to training and technical expertise applied to both the public and private sectors.

Summary of Day

Mr. Chan, Chair

- Mr. Chan reviewed the activities of the day, noting that the board had reviewed the charter and rules of operations for the board, and all of the panel members had introduced themselves.
- Mr. Chan reviewed the list of action items.
- Mr. Chan reviewed the agenda for Day 2, including the invited speakers.
  - Ms. Cuthill emphasized the need to be respectful of the scheduled times for the outside speakers.

Ms. Cuthill adjourned the meeting at 5:22pm EST.

Day 2 – IoTAB Meeting on Thursday, January 19, 2023

Opening and Agenda Review for Day 2

Mr. Chan, Chair

- Mr. Chan reviewed the day 2 agenda.
  - A section was added to discuss the definition of IoT; that discussion would time limited to 30 minutes.
  - The panel would then have sector-specific discussions.
  - Mr. Chan intended to ask board members for prioritization of the sector discussions, with a goal of focusing first on the likely longest discussions.
  - The day would conclude with outside speakers, and a meeting recap.
- The members discussed and agreed that there are sectors of interest beyond the specific ones cited in the legislation.

Definition of IoT

Note: Shift from the agenda presented on NIST website to include this topic on Day 2.

Mr. Chan shared slides which can be found here: IoT Advisory Board Report Discussions (nist.gov)

Ms. Cuthill shared slides which can be found here: NIST IoT Definitions

Mr. Bergman shared slides which can be found here: CTA National Cybersecurity Label Proposal (nist.gov)

Mr. Chan, Chair

- Mr. Chan presented a Venn diagram for discussion with a proposed list of topics for the IoTAB that are in-scope, out-of-scope, and to-be-determined.
- Ms. Kahn noted that the FWG had run into a similar issue, and she concurred with Mr. Chan's notion to determine what is out of scope.
- Ms. Cuthill shared the definition for IoT device developed by NIST and codified in the IoT Cybersecurity Improvement Act of 2020, and for IoT product used in NIST IR 8425.
- Mr. Bergman reported that he had spoken to the author of DIGIT act and reported that the intended, focus was items on the left of Mr. Chan's diagram; the things we "sort of assume are IoT".
- Mr. Bergman took an action to write up scope proposal as it might appear in the report (Action: Mr. Bergman), and noted that he would like Prof. Kornegay's, Mr. Griffith's, Mr. Katsioulas' input while drafting.

Topic Discussions

Mr. Chan, Chair

- Mr. Chan opened discussions to address the sectors specifically named in the legislation and the topics to be addressed for each: opportunities, values/benefits, barriers, potential recommendations, what information might need to be gathered, which board members might take on that topic to write up for report.
- Board members pointed out that the sixteen sectors that constitute "critical infrastructure" were well-established and codified by Presidential Directive and Department of Homeland Security documents, and that the board should use that definition.

- Ms. Cuthill and Mr. Chan clarified that the list of topics was drawn directly from the legislation and are topics that specifically need to be addressed in the IoTAB's report.
- Ms. Cuthill agreed that it was appropriate for the board members to identify additional topics relevant to the board's objectives.
- The board members agreed that the list of topics in the charter included both "horizontal" and "vertical" topics, and that topics of each type should be address consistently.
- Mr. Chan recorded an action to create a list of topics for the report to organize thinking.
- Ms. Lam suggested that a graphic be created to show the horizontal/vertical landscape and aspects of scale (from personal / wearable up to Smart Cities); Mr. Chan added that to the action.

Sustainable and Critical Infrastructure

Mr. Chan, Chair

- The board initiated a discussion of sustainable and critical infrastructure; Mr. Chan stated he wanted to organize the discussion against opportunities and benefits, vs. barriers.
- Opportunities identified:
  - Potential for improvements in physical security, cybersecurity and privacy
  - Improvements in communications infrastructure (for example, funding of "middle mile" connectivity)
  - Sensors to monitor infrastructure (for example, bridges) or detect hazards from natural phenomena
  - Digital modeling and IoT technology to enhance the construction industry
  - Investment of newly available funding to improve infrastructure
- Challenges identified:
  - Improving security in "brownfield" deployments of IoT
  - Maintaining awareness and protection of privacy as the volume of IoT expands
  - Availability and reliability of connectivity for IoT across the range of possible deployments
  - Ensuring the benefits of IoT are accessible to a broad user base from small businesses through large industry organizations
  - Balancing right-to-repair concerns of IoT customers against intellectual property considerations of IoT manufacturers
  - Uncertainties regarding data ownership
- Barriers identified:
  - Liability implications of IoT and automation
  - Making the benefits of IoT and supporting infrastructure accessible to the broad range of potential users
  - Resistance to new technology due to its impact on business models and the employment landscape
  - Lack of federal standards and regulations regarding privacy, leading to an uneven market environment
- Related discussion:
  - Ms. Cuthill and Ms. Kahn clarified that the board should make recommendations as they saw fit, including future-looking recommendations, with the understanding that the report represents a point in time and future change is to be expected.

Discuss Organization / Allocation against Topics

Note: Shift from the agenda presented on NIST website to include this topic on Day 2.

Organization of the Report

Mr. Chan, Chair

- Mr. Chan noted that while his plan had been to go through discussion topic areas and discuss questions, he was seeing that many topics are going across sectors; asks membership how to proceed: discuss cross-cutting issues? High-level organization of report? The group shifted to discussing organizing to develop the report.
- Ms. Cuthill, the DFO, was asked about the use of subgroups to facilitate developing the report, and provided guidance:
  - Members can work together in small groups to prepare material for the broader meetings;
  - Subgroups cannot make decisions or finalize material in those small groups;
  - Subgroups can prepare for discussion, accumulate options; "pre-decisional / pre-deliberation" material for the meeting;
  - IoTAB as a whole makes decision on selecting options, keeping / removing material, etc.
  - Decisions must be made in public meetings; preparation outside meetings to make them more efficient is fine.
  - "Small groups" should be <50% of the board membership
- Mr. Chan led a discussion to organize topics and identify board member interest in working on the identified topics.
- Ms. Mehra proposed a 4-dimensional model for describing the problem, based on the conversation so far; and proposed merging the charter topics into the four dimensions; a fifth dimension was added as discussion proceeded:
  - All IoT types (Operational Technology, Internet of Medical Things, Internet of Drone Things, etc.) and their components (Hardware, Software, Firmware)
  - Vertical sectors (some of the Discussion topics list)
  - Horizontals (security, privacy, equity, bias, data, policies, intellectual property, adaptability)
  - Education, skills and experience levels
  - Business to Commerce, Business to Business, Business to Government
- Mr. Chan repeated the importance of ensuring that the charter topics are addressed.

Initial Allocation of Board Members to Topics

Mr. Chan, Chair

- Mr. Chan captured a draft organization of board members against report topics:
  - Sub-sectors identified from the legislation:
    - Smart Traffic and Transit Technologies: Mr. Griffith, Ms. Reynolds, Ms. Raimundo, Mr. Chan, Prof. Kornegay
    - Augmented Logistics and Supply Chains: Mr. Moss, Mr. Griffith, Mr. Katsioulas, Ms. Mehra, Mr. Bergman
    - Sustainable and Critical Infrastructure: Dr. Shehabi, Mr. Chan, Ms. Raimundo, Mr. Griffith, Mr. Katsioulas, Mr. Tseronis
    - Precision Agriculture: Dr. Chandra, Nick
    - Environmental Monitoring: Dr. Shehabi, Dr. Chandra, Nike, Mr. Bergman
    - Public Safety: Ms. Raimundo, Mr. Bergman, Ms. Rerecich, Ms. Mehra

- Health Care: Ms. Mehra, Ms. Rerecich, Mr. Bergman

- Sectors added from the discussion:
  - Smart Homes: Mr. Bergman, Prof. Kornegay, Ms. Mehra, Mr. Griffith
  - Consumer: Ms. Reynolds, Ms. Rerecich, Mr. Bergman
  - Manufacturing: TBD. This may be folded into the supply chain and critical infrastructure topics.

- Additional horizontal topics resulting from the discussion:
  - Security: Prof. Kornegay, Mr. Griffith, Mr. Katsioulas, Mr. Tseronis, Mr. Bergman, Dr. Chandra
  - Privacy and Data Ownership: Ms. Rerecich, Prof. Kornegay, Mr. Bergman, Ms. Reynolds
  - Skills, Education and Workforce Development: Mr. Tseronis, Prof. Kornegay, Ms. Raimundo, Mr. Moss, Ms. Reynolds
  - Standards: Mr. Griffith, Mr. Katsioulas, Mr. Bergman, Ms. Reynolds, Mr. Emanuel
  - Regulations and Commerce: Ms. Reynolds, Mr. Moss
  - Policies: Mr. Chan, Dr. Chandra
  - International Engagement: Mr. Caprio, Ms. Mehra, Mr. Bergman, Mr. Katsioulas, Ms. Reynolds, Mr. Emanuel

Questions from Board Members

- Ms. Mehra asked NIST if there is there any backup data for the number of devices the DIGIT Act indicated would be deployed by 2030?
  - Ms. Cuthill and Ms. Kahn said they would need to investigate this.
- Mr. Katsioulas asked NIST if the IoTAB budget permits acquiring formal market research reports, such as are published by firms like Gartner.
- Ms. Lam asked what would be the relationship of IoTAB report to IoTFWG report?
  - Ms. Cuthill responded that the IoTAB report will be attached to the IoTFWG report, in its entirety, and both will be submitted to Congress.
- Ms. Mehra asked if IoTAB report elements be extracted?
  - Ms. Cuthill responded that the IoTFWG has to comment on the IoTAB recommendations and how they will be implemented. This IoTFWG response is called for in the legislation.

Invited Speakers

Justin Sherman / Patrick Mitchell - Atlantic Council

Justin Sherman / Patrick Mitchell shared slides which can be found here: Security in the Billions (nist.gov)

- Two representatives from the Atlantic Council presented the results of a year-long study into IoT security guidance and regulations around the world. They explained that they examined: Four country case studies (AU, UK, Australia, Singapore)
- Industry and private sector efforts
- Three verticals (smart homes, networking gear, consumer health)

- They developed a mapping of how the various guidance applies to the lifecycle phases of IoT products, which showed the preponderance applied to design, with roughly equal smaller shares applying to development, sales and setup, and maintenance, and minimal guidance directed toward device sunsetting.

- Their study identified recommendations in three areas:
  - Tiers of security measures
  - Country-agnostic implementation recommendation
  - US-specific implementation guidance
- The study suggests that the widely used approach of a minimum baseline set of requirements focused eliminating "the lowest-hanging fruit", and having higher targets that manufacturers are encouraged to attain don't need to be mutually exclusive
- The speakers noted some other takeaways from their study:
  - Security guidance should focus on full product lifecycle, including maintenance and sunset
  - The portion of a product lifecycle where a product, particular an appliance, works fine but is no longer receiving security updates represents a challenge that deserves careful consideration
  - Governments should engage with their international peers regarding what works and align their approaches without seeking wholesale agreement on every provision, and find ways to have mutual recognition of security labels
  - Define & measure success, which is often difficult for cyber; the speakers noted that their report proposed some potential metrics in report

Questions from Board Members

- Mr. Caprio asked the speakers to discuss further the inspiration they drew from ETSI's work, as well as other standards they considered. The speakers responded that they had considered a broad variety of standards, and that the ETSI was notably accessible. They also noted that in the convenings they held while developing the report there was openness to accepting standards that agreed on a core set of security principles.
- Mr. Bergman noted the US National Label program currently under development and expressed several points:
  - The label program's view is that federal standards are preferable to individual state laws
  - There is consensus in the program to use NIST IR 8425 as basis for a binary label with tiers on an online basis, and he appreciated the Atlantic Councils report's endorsement of that general approach
  - The program is looking at the potential for "safe harbor" features and incentives for manufacturers to adopt a higher level of security
  - With regard to international standards, the program is looking at ways to generalize the Singapore proposal into more of a global framework allowing labels based on national criteria to be compared
- Ms. Mehra asked why the effort had focused on the four particular countries:
  - Mr. Mitchell said they chose four countries based on initial relationships in research group. Singapore has taken a leading role; UK was foundational with code of practice that were more widely adopted and later fed into ETSI standard. He also stated that they would have wider scope if the effort were starting today.
- Mr. Mehra asked if the effort had considered the Drug Supply Chain Security Act, which looks across life-cycle phases, with blockchain technology to provide anonymity and eliminate need for labeling.
  - Mr. Mitchell stated that they weren't aware of the Act but was interested in the parallels across different domains.
- Mr. Katsioulas asked what were the motivations for the label? Security & Privacy? Supply chain tracking?

- The speakers said the study was primarily security-focused, with privacy considered where security had impacts on it, and there was minimal consideration of product lifecycles. The focus was more on the ability to offer a trusted device.

Public Comments

Two individuals offered public comments.

Rick Lane

- Mr. Lane stated he was speaking as volunteer for child safety groups on technology-related policy issues, and that he has 35 years' experience in this area including work in both government and the private sector.
- He expressed disappointment that child safety was not included in the board's charter and that the child safety community is not represented on the board
- Mr. Lane stated he had not heard any mention of potential impact of IoT on children, and recommended the board should solicit input on this topic from experts. He stated that governments around the world are looking at privacy for children, and this will affect IoT, given that the considerations for privacy and safety for children are different from those for adults.

Question and Comments on Mr. Lane's Presentation

- Ms. Reynolds commented that she was an expert on child safety and privacy and would be expected to address those issues as they arose.
- Ms. Lam requested Mr. Lane identify IoT opportunities specific to child well-being.
  - Mr. Lane stated that all technology has positive and negative implications. He described the convenience of connected devices as a positive and noted that is has become "embedded in [the] everyday lives" of children. He also noted that there are concerns about the exploitation of how children interact, and that expert input can help with designing approaches to reduce potential harms.

François-Frédéric Ozog

Mr. Ozog shared slides which can be found here: IoT Trustworthiness Score (nist.gov)

Mr. Ozog presented several points to the board:

- First: Mr. Ozog offered the opinion that it is important to decouple scoring the trustworthiness of an IoT device from the profile for the use of device. Mr. Ozog drew a parallel to how safety claims are handled in the automotive industry. This approach would permit a single evaluation of security claims for the IoT device, which could be manufacturer self-assessment or independent confirmation by an independent laboratory, while allowing potential customers to evaluate whether the claims are sufficient for their use of the IoT device. This would permit, for example, different acquisition policies for consumer and federal government applications from the same set of claims.
- Second: Mr. Ozog warned against the potential where individual security mechanisms are functioning correctly, but the combination of those mechanisms fails to provide a desired security outcome.
- Third: Mr. Ozog emphasized the importance of mandatory disclosures (i.e., hardware and software bills of materials [BOMs]) in order for customers to not be blindsided by security problems.

- Fourth: Mr. Ozog pointed out the problem of a "combinatory explosion" of the number of compliance tests needed to evaluate hardware and software.

Question and Comments on Mr. Ozog's Presentation

- Ms. Reynolds acknowledged Mr. Ozog's points and related them to challenges with IoT change of ownership, security degradation over time, and end-of-life challenges. She noted that many IoT cybersecurity incidents were associated with "legacy devices".
- Mr. Katsioulas requested Mr. Ozog distinguish for the board the difference between security and trust, asking what does trust bring that security does not?
  - Mr. Ozog responded with an example where a "box" to create car key duplicates is authenticated by the car as genuine, but the overall process allows a thief to get a legitimate key and steal the car. He emphasized the need for a proper trustworthiness plan with use cases to orchestrate all the security measures needed.
- Mr. Katsioulas asked how to compute a trust score that proliferates the supply chain?
  - Mr. Ozog said that is his proposal for the board, and again recommended applying techniques similar to those used for automotive safety:
- Mr. Bergman noted overlap between the concerns raised by Mr. Ozog, the work underway in the national cybersecurity label program, and the provisions of NIST IR 8425, which Mr. Berman stated provided "a good starting point" for the concerns that had been raised.

Closing Remarks

Mr. Chan, Chair

- Mr. Chan moves began the process of closing the meeting; he thanked participants for their contributions, and stated some of the discussions will change the initial game plan for the report. He stated he was feeling more confident after adjustments made during the second day.
- Mr. Chan thanked Ms. Cuthill and Ms. Kahn for their guidance on problem areas.
- Ms. Mehra points out that report needs to include Recommendations as key section.
  - Mr. Chan concurs, sees this as starting a subgroups, moving to full board for refinement and agreement.
- Mr. Bergman asked if there is a template as a starting point for the report to ease consistency?
  - Ms. Cuthill stated NIST has some templates that they have been working on for the board's content; NIST will take an action to circulate the templates and can provide editing support.
- The group discussed future meeting dates and agreed to set the dates for the next three meetings on approximately monthly intervals. Ms. Cuthill noted that the publication of a Federal Register Notice limited how soon the next meeting could be held.
- The group discussed scheduling meetings for March, April & May 2023 and agreed on:
  - 7 March: 1-day virtual meeting
  - 18-19 April: 2-day, possibly hybrid meeting
  - 16-17 May: 2-day virtual meeting
  - Ms. Cuthill will work on meeting arrangements and send out confirmation.
- Mr. Chan asked the members opinions of the two-day, six-hour format for meetings? There was consensus that the format was workable.
- There was a discussion of drafting content between IoTAB meetings:
  - Mr. Bergman inquired about subgroups drafting content, to avoid wordsmithing in full meetings.

- Ms. Cuthill stated that developing content in advance for review was fine, but that any objections should be discussed in board meetings.
- Mr. Bergman suggested that anyone is free to draft submissions with recommendations;
- Mr. Brewer emphasized that the critical point is that everything is approved by the full committee
- Mr. Chan said that a report outline will be provided at the next meeting to help guide in preparing material.
- Ms. Cuthill directed members to invite NIST to subgroup meetings so that a DFO is present.

Closing

Ms. Cuthill adjourned the meeting at 5:50pm EST.