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)

July 18 & 19, 2023

Virtual Meeting Platform: Webex

MEETING MINUTES

Board Members

- **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**
- **Robby Moss**, Moviynt
- **Nicole Coughlin**, 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

Board Chairs and NIST Staff

- **Benson M. Chan**, Strategy of Things Inc. (Chair)
- **Daniel W. Caprio Jr.**, The Providence Group (Vice Chair)
- **Barbara Cuthill**, NIST (Designated Federal Officer)
- **Jeffrey Brewer**, NIST (Alternate Designated Federal Officer)
- **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)

Speakers:

- **Chris Autry**, CEO, Iothic
- **Sven Dharmani**, Ernst and Young
- **Paul Eisler**, Vice President, US Telecom, The Broadband Association
- **Mei Lin Fung,** Chair, People Centered Internet
- **Christopher Moore**, President, Mission Critical Insights, LLC

Action Items Over Both Days

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

Report

- Overall
  - **Mr. Witte** will provide an updated draft IoTAB report post-meeting.
    - The path forward is to revise the structure as discussed, harmonize the final recommendations, and add additional content. Removing recommendations is still under review.
  - **IoTAB members** should consider begin to consider graphics for the IoTAB report to visually convey information. Mr. Witte will help to format graphics, so they look similar.

- Executive summary
  - **IoTAB members** should think about what other information should be included.

- Recommendations
  - **IoTAB subgroups** that are reworking recommendations should be addressed in the next meeting for board consensus.
  - The **Board** must work to make recommendations actionable (e.g., currently there are no KPIs in the recommendations) and the IoTAB report will need specific, actionable, and measurable recommendations.
  - On the topic of a legend:
    - **Mr. Witte** was asked to provide a specific proposal so that the board can make a determination. The board suggested a legend that would indicate both prioritization and levels of funding associated with individual recommendations.
  - On the topic of ordering the recommendations:
    - **IoTAB members** should come to consensus on the ordering of recommendations. Consensus on order of recommendations was discussed but not agreed upon. Recommendations are provided in thematic groups rather than strict numerical order. IoTAB members discussed a way to order it, possibly by NDAA language.
- Conclusion of the report
  - **IoTAB members** to determine if recommendations should be included in the introduction or the conclusion of the report.

- References
  - **IoTAB members** should identify references. Few references have been suggested so far and need to be identified by the Board. References should relate to things for the IoTFWG to inform Congress about. Also, the presentation of references should be determined by board consensus.

Subgroup Considerations

- Considerations for future meetings or gaps that need to be addressed were identified:
  - Intersections with the AI and other areas.
  - Concerns about coverage for legacy data and legacy devices including handling data from end-of-life devices, which is a huge issue.

  - Environmental monitoring needs to include other use cases.
  - Connectivity discussion and recommendations need more coverage. Dr. Chandra offered to join the Connectivity team on connectivity recommendations.
  - Supply chain had a discussion that the IoTAB may want to address the challenge of "white boxing", as it relates to labeling, how it relates to manufacturer responsibility.

Speakers

- **IoTAB members** should provide suggestions for invited speakers to Mr. Chan for upcoming meetings.

Schedule

- Review the draft IoTAB timeline.
- Upcoming meeting dates:
  - August (22nd-23rd)
  - September (26th-27th)
  - Future meeting dates will be provided
- The IoTAB is looking at a one-year timeline with **updated** milestones:
  - **August**: Board will be identifying remaining gaps to discuss prioritization for next steps.
  - **September**: Board should target having all recommendations complete by end of this meeting.
  - **October**: Board will review summaries and prioritizations.
  - **November**: Board should target having a final draft report by the end of the meeting with some final adjustments being made in December.

IoTAB Meeting on Tuesday, July 18, 2023

Welcome and Chair's Opening Remarks

Ms. Cuthill welcomed the attendees, opened the meeting, and introduced the chair, Mr. Benson Chan.

Mr. Chan went over the agenda and goals for the meeting.

Slide deck: Chair Discussion Slides

- The discussion reviewed the expected outcomes for the day, the agenda, and the logistics.

Invited Speaker – Chris Autry, CEO, Iothic

Mr. Chris Autry, CEO, Iothic

Prepared remarks: Concise Version / Detailed Version

- Mr. Autry stated he has been working on IIoT for several years, with an emphasis on the security and interoperability aspects of IIoT networks. He has been addressing the challenge of decentralized authentication in disparate networks, framing the problem as, for example in a smart cities' environment, how can a device authenticate other devices entering from another network in real time, without relying on a third party. He stated that the US Navy and UK MoD have done work on this problem, as it relates to authenticating military personnel disassociated from their central command.
- Mr. Autry described authentication as the foundation of any cryptosystem, and central to security and trust. Authentication, he said, leads to authorization. He noted that the vast majority of network authentication today is based on PKI, with third party involvement and static certificates.
- Mr. Autry identified three big technological hurdles regarding this problem, which he said applied regardless of application; in no order of importance, he listed them as:
  - The existing infrastructure, especially for operating technology, which can be 20,30, or 40 years old;
  - Interoperability, noting that getting point-to-point authentication within a network is often a huge issue, even when endpoints are from the same vendor; and
  - Security.
- Mr. Autry said the security problem in IoT/IIoT is so large it is "the elephant in the room" and stated that cybersecurity conferences don't discuss solutions but focus on mitigation and detection techniques, often leveraging AI for detection. He described this as trying to use existing, centralized client/server solutions that aren't appropriate for dynamic operating models.
- Mr. Autry described networks across a spectrum of complexity from highly static / single owner to highly dynamic / multi-owner (owner here means whoever is controlling or responsible for the network), and provided examples:
  - A static building network with hundreds of nodes, internal interactions, and a single owner;
  - Multi-owner, highly dynamic networks that change over time and interact with multiple other networks.
- Mr. Autry stated that networks in 2023 look more like the multi-owner / dynamic networks, but the industry is trying to address the security of these networks problems using an old, static (client / server) model of computing. He described the promise of IoT / IIoT as high fluidity, with lots of connections in "real time" between things, and lots of data transmitted, and referenced discussions circa 2015 of

smart cities and a 4th industrial revolution. Mr. Autry declared this hasn't happened as expected largely because of the three technological hurdles he had listed.

- Mr. Katsioulas asked about how to get suppliers of IIoT products to improve their security, noting the current security deficiencies of OT systems.
    - Mr. Autry concurred about the security challenges of OT systems and their evolution to IIoT, saying he had spoken to vendors who describe the problem as complicated, particularly regarding the security of PLCs.
- Mr. Autry referred to the huge cost of replacing existing infrastructure to build security into the network, and said because of that cost, a desirable solution would be one that can be easily deployed on existing network infrastructures, either directly onto a network asset or via a physical or virtual entity fronting the asset. He indicated this solution could directly affect the TCP/IP layer, integrating post-quantum security and interoperability onto existing systems, and stated this was "not theoretical".
- Mr. Autry described the need to permit ongoing operations while introducing these new security protections ("keep everything you have on").
- Mr. Katsioulas asked about the impact of vendors being unable to track or connect to deployed devices.
    - Mr. Autry acknowledged that customer organizations often lose track of their deployed assets, which complicates deploying code or fronting elements to provide the security capabilities. He said this created expensive and time-consuming challenges.
- Mr. Autry described that some companies have had spiders crawl networks to identify and map what is there, and associate function, serial number, and MAC address, thereby creating a functional inventory. He said that what he described as "more progressive companies" have built this into digital twins, which he called hugely valuable. Mr. Autry stated that it is possible to deploy a solution if you have a reasonable picture of what you have. The operator needs to allow for parallel systems, and the ability to easily create subnetworks if things get left out.
- Prof. Kornegay asserted that, assuming the deployment will be fully automated, there is a challenge for the IT workforce knowing how to respond when things break.
    - Mr. Autry responded that there are two times when central connectivity is required in the proposed solution. The first is during initial deployment, after which automated operations occur. The second is in the scenario Prof. Kornegay described. Mr. Autry described a need for the solution to include a "profound reporting mechanism" and noted that most organizations have systems and event management protocols and reporting systems. He stated the proposed solution can trace connections in a detailed manner.
- Mr. Autry described characteristics of the solution as using standards when deploying on TCP/IP, providing full reporting all the time, and being transparent (to understand what connections happen).
- Prof. Kornegay asked about decommissioning and residual data.
    - Mr. Autry replied that the system handled commissioning and decommissioning the same, and that residual data from decommissioning was "not particularly relevant".
- Mr. Autry describe the goal of the solution as creating a "low level, live, semi-intelligent network that has partially shared secrets that change", where components are aware of one another. He said that current authentication mechanisms authenticate the certificate the thing has, rather than "the thing", but if you are able to authenticate "the thing" — knowing what it is, where it is, what has it just done — with certificates generated new on-the-fly each time, the result is that decommissioned assets can't participate.

- Prof. Kornegay asked how this differs from zero trust, and Mr. Autry stated this is a zero-trust solution.
- Mr. Autry described the value of applying AI to dynamic networks, saying it is closely connected with IoT, and it is possible to place established machine learning models at the network edge to analyze and act on data.
- Mr. Autry stated that quantum computing poses a greater threat, especially if combined with AI, where it can speed up model execution. He described quantum as one of the most "potentially precarious technologies that will be released on humanity" and described a characteristic of his proposed solution as negating the quantum risk by eliminating permanent, static certificates.
- Mr. Autry presented three recommendations:
  - Invest in integrating quantum-safe solutions directly into the network to future proof existing and future networks on existing infrastructure. This future proofing protects IoT.
  - Invest in relatively autonomous, intelligent networking capabilities that require minimal human involvement once the technology is deployed. This reduces the potential for human error to enable security breaches. The goal is to make networks as automated as possible while maintaining transparency, which brings enormous cost savings potential (e.g., by eliminating the overhead of managing cryptographic keys, and reducing errors).
  - Invest in decentralized, dynamic networks that can adapt in real time. He stated that IIoT / IoT are "designed precisely for this", and that it is nearly impossible to properly integrate dynamic IoT / IIoT devices into current static networks.
- Mr. Autry acknowledged that dynamic networks introduce a lot of challenges we don't appreciate today and will support unanticipated use cases.
- Mr. Katsioulas ask about a potential strategy for identity and cybersecurity labeling in the industrial context.
  - Mr. Autry said he doesn't believe the solutions currently proposed by industry are the right solutions, and there is a need to wait for solutions such as he described to be deployed.
- Mr. Autry summarized his key take-away as to stop thinking about solving problems using a client/server model of computing, which is misaligned with IoT / IIoT, and described his recommended solution as having "no kingdom to get the keys to". He identified the technology as "dOISP"[1].

Invited Speaker – Paul Eisler, Vice President, US Telecom, The Broadband Association

Mr. Paul Eisler, Vice President, US Telecom, The Broadband Association

Slide deck: Report to NIST Advisory Board

- Mr. Eisler described the focus of US Telecom as "creating international harmonization and building economies of scale", with a strong interest in standards, especially for security, which they see as a driver for adoption across different customer bases. He described the creation of the Council to Secure the Digital Economy (CSDE) and the broad support it had received. He stated that the CSDE's C2 Consensus document had informed the ANSI/CTA 2088 security standard.
- Mr. Eisler then presented several key points.

[1] decentralized Open IoT Security Protocol: https://ieeexplore.ieee.org/document/9988136

  - Point 1: IoT can rely on existing security policy principles. Mr. Eisler stated confidence in the quality of ANSI/CTA 2088 but expressed a preference for an international security standard for IoT because member organizations operate around the world.
  - Point 2: Leverage existing consensus-based standards and best practices on IoT security. Mr. Eisler said that standards need to make technical sense, but also have a legal component, in which they are being used by legislator and regulators as the basis for rules that have to be adopted. He described this as increasingly an issue, creating a need for lawyers alongside technologists, and asserted the value of providing legal protections ("earned safe harbors") for businesses responsibly adopting accepted standards.
  - Point 3: Risk analysis approach. Mr. Eisler said the applicability of IoT security capabilities varies a lot based on context and encouraged flexible adoption of standards based on risk management principles. He said the CSDE C2 Consensus is an example of what it looks like to apply NIST concepts to a particular environment and suggested other sectors would benefit from a similar approach. Mr. Eisler said he favors a voluntary, industry-led model while acknowledging that industry needs to "step up".
  - Point 4: Leverage public/private partnerships and multi-stakeholder efforts. Mr. Eisler described the value of such partnerships and stated they would like to see better partnership with Europe, saying companies both in the US and in Europe have interests in avoiding disharmonization. He acknowledged the cultural challenges associated with building relationships.
  - Mr. Caprio asked about examples of bi-lateral and multi-lateral gatherings that are particularly effective.
    - Mr. Eisler replied that there are no perfect examples, and that governance issues often prevent direct participation in EU government meetings. He suggested that having a number of US and European companies presenting a consensus to regulators could be helpful and noted that EU regulators care about European companies.
  - Point 5: a thoughtful and holistic approach to device security. Mr. Eisler noted the diversity of the IoT landscape, and a need for policies that "comport with" security of underpinning domains. He expressed the desired to work with NIST on the announced router profile. He said that while the US labeling program equates to meeting certain technical requirements, he sees opportunity for industry certification programs, and a need for industry input for certification and labeling to be successful.

- Mr. Eisler then discussed recommendations endorsed by six trade organizations:
  - Host standards body meetings in the US to facilitate great industry and government involvement. He noted the need to address visa processes and restrictions that complicate foreign participants entering the US, saying this resulted in fewer US participants engaged and fewer like-minded countries sending representative here, and cited the specific example of example of 3GPP meetings being moved away from the US due to pressure from China.
  - The US should work with like-minded countries to reform standards body governance and processes to maintain focus on the appropriate scope of their work.
  - Provide targeted financial incentives to support industry participation in standards, particularly to help in getting small companies to engage, send their experts to standards making activities.

- Mr. Caprio asked about the challenge of conformity assessments, especially internationally, related to the announced US labeling effort and any suggestions on promoting that.

  - Mr. Eisler suggested beginning by identifying countries most likely to be open-minded to working with US, then examining the legal implications for parties in those countries to engage, saying that a voluntary labeling program might have a totally different set of considerations for a European lawyer. He noted that lawyers are often serving as gatekeepers, saying there is a need to eliminate excuses to say "no". He stated there are significant differences among countries, and a need to engage policy makers. He concluded this will have to be built out gradually.

Informal Feedback from IoT Federal Working Group

Mr. Witte, Editor

Mr. Witte started the discussion with feedback from the IoTFWG meeting held on June 24, 2023.

- Some IoTFWG members have been attending our meetings here and expressed appreciation for "immense amount of work the board has done". He said there's a lot of commonality.
- The IoTAB materials provided independent confirmation of items they've seen in their agencies.
- They liked the idea of a framework that can cover both data protection & privacy and are supportive. This could help to organize and communicate about data protection and privacy.
- On standards, they emphasized needing a better way to use the standards that exist and how to explore achieving that. The IoTFWG is focused on interoperability, particularly across vendors, avoiding vendor lock-in and want the best tools for the job. Along these lines, the IOTFWG wants to encourage voluntary adoption of standards-based approaches.
- Mr. Witte pointed to the implementation plan for the recently released national cybersecurity strategy[2] and that it encourages shared responsibility with a shift toward greater vendor responsibility.
  - A link to the national standards strategy[3] is shared for additional guidance.
- Mr. Witte noted that the IoTFWG discussed secure operation of IoT in addition to securing the data and the notions and difficulties of safe harbors.
    - Mr. Caprio: A shining example of this is the Credit Card Reporting Act (circa 1970). Basically, this act holds the consumer harmless for fraudulent use of the card. It does allow for lots of information to be collected by credit reporting agencies. Is there some expertise around that law that could be accessed? The Credit Card Reporting Act has led to economic growth.
    - Mr. Witte: The Act didn't come up by name, but definitely that example was definitely used. The IoTAB can reach out to agencies or the IoTFWG for clarifications.
- There is a need to determine how to incentivize organizations to share accurate information. There is also a need for international cooperation on cybersecurity. Everything has international connotations. Indicated that privacy was a concern. IoTAB has been discussing setting new criteria, which would apply to new devices. IoTFWG suggested keeping in mind legacy devices and what can be done with those.
- Indicated that the IoTFWG acknowledged the challenges in smart transportation, especially the privacy trade-offs.
- On the topic of Connectivity: The IoTFWG discussed the national spectrum strategy. Issues that come up deal with prioritizing needs and the potential for dynamic management and use of spectrum that the IoTAB could consider.

[2] https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf
[3] https://www.whitehouse.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf

- On Sustainable Infrastructure: The IoTFWG would appreciate more specifics on what to measure and why, and how the data could be used.
- On Workforce: There is strong support for workforce discussion and potential to revitalize some areas. The IoTFWG reminded the IoTAB that "digital natives" don't necessarily have all of the skills and knowledge needed. There are opportunities for inter-generational collaboration.
- On Smart Traffic / Transportation: Department of Transportation has been in conversation with the General Accountability Office (GAO) and Congressional committees. The IoTAB could ask questions or get information on specific matters discussed or review public records since there have been hearings.
- On Supply chain: A need to be distinct about cyber supply chain risk vs. reliable / resilient supply chain. Might want to reach out to Federal Maritime Commission regarding their work on supply chain.
- The IoTAB may want to address the challenge of "white boxing", as it relates to labeling, how it relates to manufacturer responsibility.
- On Healthcare: On HIPAA protection regarding medical data in mobile IoT.
- Mr. Witte will forward a few questions from the IoTFWG to Mr. Chan:
  - To what extent does the IoTAB believe adequate spectrum is available?
  - Are there opportunities and challenges for small businesses related to IoT adoption?
  - What are the international proceedings that affect IoT?
  - And how can we understand where to engage or disengage internationally?

Group Discussion

- Mr. Katsioulas: Comprehensive "fly by"; pleased IoTFWG is considering all these issues. There is a need to better educate by looking ten years out at the opportunities for IoT to have substantial impact to the economy.
- Mr. Tseronis: Agrees with Mr. Katsioulas. Thinks the opportunity and challenges are the owners and operators of legacy infrastructure starting to connect to IoT / Industrial IoT (IIoT) There is great promise but enhances risk. How are we keeping situational awareness in play (when data is siloed off)? There is a need to consider where the data is and what will be different in ten years (e.g., regarding the cloud or how the Federal government is involved when 90% of the devices are privately owned).
- Mr. Chan asked the IoTAB what their overall sense was on the IoTFWG reaction.
  - Mr. Witte responded that we are on the right track with some areas still needing actionable recommendations (e.g., don't have KPIs in our recommendations) and will want specific, actionable, and measurable recommendations.
  - Mr. Katsioulas: Started by talking about opportunities and barriers and emphasized the need for recommendations plus the context to develop KPIs.
  - Ms. Kahn: Seconded Mr. Witte's description on the enthusiastic group with lots of brainstorming and an overall positive discussion.
- Mr. Chan: What happens when IoTFWG gets this report? How does this align with IoTFWG activities?
  - Mr. Witte indicated that he had looked at all of the recommendations from the May meeting and started considering how agencies might respond to the recommendations. The IoTFWG has already recommended better interagency coordination. IoTAB recommendations will also be reflected in the IoTFWG report to Congress. The IoTFWG won't write the national strategy but will provide input to it.
  - Ms. Cuthill indicated that responses were provided by individual agencies that were present and able to get information back to this group. She indicated that this group would see more responses

over time. There's an appreciation for agencies and their working relationship. Ms. Cuthill stressed the informality between the back and forth of the IoTAB and the IoTFWG. This is a process of the IoTFWG commenting as individual members on what they see from the publicly available material from the last meeting.

Discussion on Report of Draft Recommendations

NOTE: all document references in this section are to the July 18, 2023, draft of the IoTAB report[4].

- Mr. Witte discussed the informal draft development, emphasizing this is a work-in-progress draft and considerable more work is needed.

Executive Summary

- Mr. Witte described the expected content of the executive summary, which he said would be filled in at the end of the process. He anticipates an introduction from the chairs, and background on the purpose for the IoTAB and the report. Mr. Witte suggested that the IoTAB members should think about what other information should be shared here.

Overview of Report Organization

- Mr. Witte walked through the next several sections of the report: information about the charter, a table of the summary recommendations (on completion), description of the methodology, and meetings held by the IoTAB and subgroups to share information.
- For the commentary section (section 6), Mr. Witte reminded the members of earlier IoTAB discussions that could be included in the executive summary:
  - What is IoT? Not a definition, but what we considered to be relevant for our work here.
  - Describing the current state and envisioned future state of IoT: where is it going in 5, 10, 20 years?
  - Adjacent technologies and subtopics: how does this relate to AI? How does it relate to different individual components such as consumers, regulations, smart homes?
  - Personas - who are we talking about? Who would be affected by the recommendations?
- Mr. Witte highlighted other sections of the report and the content they would include:
  - Section 7 will summarize the findings of the IoTAB, including barriers and opportunities, summarized by topical area, presenting both what the IoTAB is seeing and why. Mr. Witted pointed to the Section 7.1 outline as an example of the section layout that will be used throughout.
  - Section 8 will discuss the cross-market and development topic specific areas, including cybersecurity, privacy and data ownership, and others. He described this section as an opportunity to share the IoTAB's hopes and dreams, challenges, opportunities, and barriers.
  - Section 9 will provide the recommendations, starting from the recommendations that the IoTAB reviewed and approved at the May meeting. Mr. Witte noted that the draft included recommendations the IoTAB had concluded needed more work, with highlighting to distinguish them.
  - Section 10 will present conclusions, describing how the recommendations help achieve a desired state for IoT.
  - Remaining sections will present references, acknowledgements, and a compliance matrix indicating how the guidance from the NDAA is addressed.

[4] https://www.nist.gov/document/initial-draft-iot-advisory-board-report-2023-07-18

Recommendations Presentation

- Mr. Witte noted that each set of recommendations will have an overarching recommendation that summarizes the broad recommendations of the IoTAB on a particular topic, and specific supporting recommendations that would either revise or extend or be a specialized implementation of that key recommendation. He used the example of the recommendation for a National Data Protection framework, describing the need for separate supplemental implementation recommendations to enable the broader recommendation.
- Mr. Witte identified the seven topics areas to be addressed in Section 9: precision agriculture, environmental monitoring, smart cities, health care, public safety, smart traffic & transit, and supply chain logistics (both augmented logistics and supply chain traceability). For each topic there will be a key recommendation and supporting recommendation, all of which can be referenced by number.
- Mr. Witte indicated he captured recommendations as the IoTAB discussed and approved them, noting where some recommendations are being reworked and have not been approved.

Group Discussion

- Mr. Katsioulas had several points of feedback:
  - Expressed approval for a short executive summary;
  - Raised a concern about the recommendation appearing far into the document, and suggesting that they should instead appear in Section 7 where the context for each topic is presented;
  - Suggested the horizontal recommendation should appear earlier, at least in summary form;
  - Suggested that where the topics from the legislation appear they appear in matching order to the legislation.
- Mr. Witte accepted the suggestions.

Discussion of Recommendations

Note: Mr. Witte moved throughout the IoTAB Report Recommendations section when presenting material to the IoTAB for discussion. Commentary is best attributed to the supporting recommendations where possible as some discussion moved between different supporting recommendations. Following the discussion in the next section, the IoTAB determined that the report will identify the cross-topic areas ahead of the findings, so Section 7 will be cross-topic areas and Section 8 will be findings.

Key Recommendation 1.0: National Data Protection Framework

Mr. Witte led the group discussion on the recommendations in Section 9 of the report.

- The initial approach is to present a recommendation for a single framework with certain characteristics rather than a set of frameworks (i.e., data use, privacy, security).
- Mr. Witte proposed the use of NIST SP 800-60 to help characterize the information types of a system as a starting point for how data should be protected. Direction from the IoTAB included the need for a better taxonomy of standards rather than another standard. A framework can organize the various elements to make sure there is standards coverage.
- The IoTAB was interested in also connecting this starting point to organizing disclosure for privacy policies (for how a type of data is defined/used).

Supporting recommendation 1.1	The federal government should facilitate/support the development of a National Data/Privacy Framework that clearly delineates the different aspects of data (i.e., machine versus personal) and how they should or shouldn't be utilized in smart transportation technologies.

Group discussion:

- Suggested the example of data "subject to privacy" vs. "machine data" (e.g., traffic) and the importance of capturing the distinction.
- There was a clarification question for the IoTAB on whether the information presented here does not already exist for IoT, to which Ms. Reynolds clarified that from examination of related frameworks they do not capture what the IoTAB is working on, and the intent is to think about what the gaps are and whether that is a separate framework or an augmentation to an existing framework.
- Mr. Witte made a reference to aligning this information in earlier chapters 7 and 8 of the report, giving the example that for smart transportation we could say a framework would help and we could add a note to say that these recommendations were covered in the umbrella topic.
- The IoTAB directed that the supporting recommendations be presented in the order of the topics in the.

Supporting recommendation 1.2 (under review)	The government should examine opportunities to use the notional IoT Data Framework to support and document privacy considerations

- Mr. Witte pointed out that at a minimum the framework covers smart transportation components and could be used to support and document privacy considerations. He said that one of the recommendations from the privacy team is that we're not trying to address all privacy, but the concerns from IoTAB about what data will be produced and will be consumed. Privacy considerations go both ways. For example, data use basics that could be included in data policies.

Supporting recommendation 1.3 (under review)	Federal agencies can establish templates for clear and robust policies regarding data sharing and data usage involving third parties in the IoT ecosystem.

Supporting recommendation 1.4 (under review)	The government could incentivize the creation of trusted data marketplaces where data producers and consumers share information about data

- Mr. Witte asked the IoTAB to consider how to incorporate sufficient trust into any approach to incentives?

Supporting recommendation 1.5	The government can encourage and foster data policies that drive economic growth, such as through this framework.

- Mr. Witte pointed out that data policies came up with several the topics. The federal government doesn't always have a say in how data is produced or used. The focus is on collect, protect, and share data and how to represent that in a framework in ways that maximize value and protections.

Key recommendation 2.0 Standardize IoT Implementation

This key recommendation focuses on methods to foster interoperability and security for IoT technology.

Supporting recommendation 2.1	The government should promote standards and protocols for IoT technology in supply chain management to provide assurance of interoperability, reliability, and security across various IoT systems and devices.

- Mr. Witte pointed out that standardization goes back to interoperability and the need to invest in technology that will be around for a while. He pointed out that in the past industry groups came together to simplify complexity for interoperability. Examples include for Wi-Fi and cellular technology.
- The government could foster and encourage voluntary industry collaboration.

Supporting recommendation 2.2	Agencies can support research and industry-led standards in areas such as telematics and sensor technologies for autonomous vehicles.

- Mr. Witte here incorporated the IoTAB's recommendation that it would be helpful if agencies could just perform a survey of available and relevant standards, protocols, and models. Government and industry need to understand what is available and what supplementation, if any, is needed. This provides confidence in the standard and can encourage dialog about standards.

Supporting recommendation 2.3	The federal government should promote and adopt industry led standards for minimum baseline interoperability and cybersecurity requirements for smart transportation technologies and corresponding transportation infrastructure (i.e., sensors in roads, cameras at intersections).

- Mr. Chan pointed out that government is used broadly and that the IoTAB may want to put placeholders to talk about specific agency impact or implementation. He further added that adding a table tying supporting recommendations to agencies may be helpful.

Supporting recommendation 2.4	The federal government can facilitate and support the adoption of smart city and sustainable infrastructure standards.

- Mr. Witte pointed out that trust came up often and has two dimensions. Can we trust the data and the devices?

Supporting recommendation 2.5	Federal agencies can help support existing industry standards development activities with respect to energy efficient technologies used in sustainable infrastructure.

Supporting recommendation 2.6	Agencies should advocate for the implementation and adoption of interoperable data standards for public safety IoT.

Supporting recommendation 2.7 (Under Review)	Agencies can promote and, if necessary, develop a protocol for data exchange standards for IoMT (Internet of Medical Things) for interoperability, and promote the adoption of these standards.

- Mr. Witte pointed out that there should be a follow-up on healthcare to determine the extent to which data used by IoMT devices are covered by existing regulations.

Supporting recommendation 2.8 (Proposed)	The federal government should promote and adopt industry led standards for minimum baseline interoperability and cybersecurity requirements for smart transportation technologies and corresponding transportation infrastructure (i.e., sensors in roads, cameras at intersections).

Key recommendation 3.0 IoT Cybersecurity (including critical infrastructure)

- The Federal Government should provide specific and consistent guidance for providers and adopters to ensure secure operations.
- Mr. Witte explained that he had placed the recommendation to continue to look to NIST for their expertise in developing cybersecurity guidance in the supporting text for the cybersecurity key recommendation.

Supporting recommendation 3.1	The Federal Government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems.

Supporting recommendation 3.2	The government should strengthen cybersecurity measures focused on IoT across supply chain networks to address concerns around data privacy, security, and potential risks associated with increased connectivity and interdependence of IoT systems.

Supporting recommendation 3.3	The government should prioritize broad and active industry engagement when developing and maintaining the government-sponsored portion of the U.S. national cybersecurity label for connected devices.

- For supporting recommendations 3.1, 3.2 and 3.3, Mr. Witte pointed out there is a back and forth between security and cybersecurity and "cybersecurity" is most used in industry. NIST uses the terms as equivalent and is using cybersecurity in the report because it is more common in industry.

Supporting recommendation 3.4 (Under Review)	The Federal Government should update Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience requiring a sector-specific Internet of Things (IoT) data strategy.

Supporting recommendation 3.5	The Sector Risk Management Agencies (SRMAs) should collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience.

Supporting recommendation 3.6	The federal government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems.

- Mr. Chan was interested in the notion of government leading by example which could be a common tactic of these recommendations, either doing it themselves or doing it as procurement. He indicated this could be a separate recommendation or an overarching.
  - Mr. Witte indicated an icon or visual tag could help indicate it consistently.
  - Mr. Chan included that the IoTAB is going to have all these different recommendations and there's a need to make sure the government does something and that all categories must be consistent across different recommendations.

Key Recommendation 4.0: IoT Connectivity Improvement and Expansion

Mr. Witte indicated that the key recommendation text is still being developed.

Supporting recommendation 4.1	The federal government should consider increasing funding and accelerating implementation of broadband deployment across rural America.

- Mr. Witte started by indicating that connectivity came up frequently in recommendations across different sectors. Devices are connected using different broadband technologies.
  Mr. Witte pointed out that various recommendations included improving connectivity under the different conditions and constraints of specific environments (e.g., rural farmland) and that offering challenges to industry to address could be an approach.

Supporting recommendation 4.2 (Under Review)	The federal government should actively promote and support the adoption of satellite narrowband IoT systems.

- Mr. Witte talked briefly to satellite connectivity when Mr. Chandra recommended including dynamic spectrum access for IoT for broadband systems. He pointed out that the FCC published new regulations in 2020 and 2022, but more for TV spectrum. And that it's great to see satellite narrowband mentioned as well.
- Mr. Chan followed on that a comment regarding the possibilities of other potential recommendations can be added and the IoTAB can build out the recommendations from the placeholder comment.
- Mr. Chandra added that there is a national spectrum strategy being discussed, but it doesn't include IoT. The IoTAB here can flag the need to have IoT discussions regarding dynamic spectrum access.
- Mr. Chan also added in that from the last meeting about the sufficiency of connectivity services for agriculture, there is a need for more uplink than downlink to support future agriculture. And there was a discussion on creating a network like a FirstNet equivalent. Mr. Chan informed the IoTAB that Chris Moore speaking on Day 2 was one of the architects of FirstNet.

Key Recommendation 5.0: Address Privacy Considerations for IoT

Mr. Witte indicated that the key recommendation text is still being developed.

- Mr. Witte pointed out that privacy would be discussed in more detail on Day 2 and pointed out that the IoTAB can advocate for appropriate protection / data use basics.
- He indicated that this recommendation would be broadly drawing on what we have learned around IoT protection and privacy and that some privacy recommendations point back to others.

Key Recommendation 6.0: Sustainable Infrastructure

Mr. Witte indicated that the key recommendation text is still being developed.

- Mr. Witte indicated that there is recognition that the US is lagging in reducing impact on the environment. The key recommendation would be trying to lead the way and a continuation of working together to draw from supporting recommendations to drive specifics around how can we do better, around technology that will ensure sustainability and reliability.
- Mr. Griffith said the subgroup would have updated recommendations to discuss on Day 2.

Key Recommendation 7.0 Workforce

- Mr. Witte pointed out that there are a lot of opportunities with workforce. From the security side of things, we always say we need more people. If we can better describe what we need and what someone will do in a particular role, then we can train them. So, what specific tasks will they need to do? If we can provide specifics from a persona perspective, it might support the ask in the legislation.
- He pointed out that there's a lot of opportunity to supplement the workforce and that the IoTAB should be thinking about how to work with industry on what's needed (identifying target areas) and indicating how the government can specify those things. The recommendation should support an emphasis on promoting industry/academic partnership.

Supporting recommendation 7.1	The federal government should consider "student loan forgiveness" programs in exchange for providing critical emerging technology (IoT, data science, cybersecurity, etc.) skills to state and local as well as federal agencies.

- This was especially noted as a challenge for smaller cities and rural areas.

Supporting recommendation 7.2	Agencies can support an improved Supply Chain Workforce by investing in and promoting education and workforce development for designing, implementing, and managing IoT systems in supply chain operations.

- Mr. Witte indicated that the supply chain team called out ways to invest in and promote the specialized skills needed for supply chain work.
- There is a broad general need for more trained employees across all the sectors. These needs tend to have broad commonality, but specific specialized skills are needed for each.

Supporting recommendation 7.3 (Proposed)	The federal government should invest and promote education and workforce development in smart transportation technologies.

- Mr. Witte pointed out that smart transportation also provided great ideas on why would be helpful, how to go about it, some of which may help with overarching requirement.
- Mr. Witte asked the IoTAB: does this approach to umbrella recommendations make sense?
- Mr. Chan suggested that it is generally easier to write up challenges and opportunities across sectors for overarching recommendations. He described an additional challenge beyond the lack of a skilled workforce, citing the overall US labor shortage, and explaining that the general labor shortage could limit the capacity both to manufacture IoT and to install it. He stated this as a broad challenge, noting that the related challenges in specific sectors can vary.
- Mr. Witte agreed and indicated that use cases could enhance the next set of recommendations.

Key Recommendation 8.0: Precision Agriculture

Mr. Witte indicated that the key recommendation text is still being developed.

Supporting recommendation 8.1 (Under Review)	The U.S. should create a National Strategy for Agricultural IoT.

Supporting recommendation 8.2	The federal government should consider subsidizing the use of IoT in farms.

- Mr. Witte pointed out that the IoTAB recommended subsidies and that upfront cost is a limitation on adoption, especially for the smaller farms.
- Tagging the mechanisms (e.g., staffing, funding, need for standards, need for user education/outreach) in a way that would flag certain recommendation types was recommended.

Supporting recommendation 8.3	The federal government should fund the deployment of a “farm of the future” setup in every land grant university nationwide.

- Mr. Witte pointed out that funding is related here but that this is more about deploying and integrating, and not as directly tied to grants.

Supporting recommendation 8.4	The federal government should promote adoption of Generative AI applications for Agriculture IoT.

- Mr. Witte indicated it was interesting to hear the IoTAB’s recommendation for the relationship between AI and precision agriculture. Other topics were discussed in other examples – broadband and connectivity which tie back to recommendation 4. Mr. Witte indicated that perhaps providing pointers to cross reference among places in the document could be a next step.

Key Recommendation 9.0: Environmental Monitoring

Mr. Witte indicated that the key recommendation text is still being developed.

Supporting recommendation 9.1	The federal government should establish or encourage IoT environmental data repositories in support of making environmental data open and available.

Supporting recommendation 9.2	The federal government should facilitate and support the research, development and deployment of low-cost air quality sensors.

- The supplemental recommendation for low-cost air quality sensors could be treated as an example, and the recommendation broadened to low-cost sensors. Mr. Chan and Dr. Chandra suggested water monitoring as an additional example.

Key Recommendation 10.0: Smart Cities

Mr. Witte indicated that the key recommendation text is still being developed.

Supporting recommendation 10.1	The federal government should consider the development of a Smart City and Sustainability Extension Partnerships (SCSEP).

- Mr. Witte indicated there was a lot of useful content around the proposal for Smart City and Sustainability Extension Partnerships (SCSEP).

Supporting recommendation 10.2 (Under Review)	The Federal Government should establish a Smart City Officer (SCO) within each of the twenty-four (24) CFO Act agencies.

Supporting recommendation 10.3 (Under Review)	The Federal Government should establish a Smart Cities Program Office (SCPO) within the Executive Office of the President to ensure that the federal government, state, and local government entities can effectively plan, implement, and manage smart city initiatives across the United States.

- There are two bills in the Senate that establish responsibilities in the executive branch regarding emerging technologies. Language from those bills could be adapted by the IoTAB for use in the supplemental recommendations regarding a Smart Cities Officer (10.2) and Smart Cities Program Office (10.3). This would aid the IoTAB both in ensuring these topics are brought to federal agencies' attention and in fostering inter-agency collaboration.

Supporting recommendation 10.4	The federal government should consider the specification and utilization of IoT and "smart" technologies into infrastructure and other projects that are funded in full, or partially, with federal funding.

- The concept of using federal procurement requirements to promote the use of IoT can be broadly applied and could also bring IoT costs down due to the government's substantial buying power.

Supporting recommendation 10.5	The federal government should consider funding models for sustaining and support beyond the initial acquisition and building of new projects.

Supporting recommendation 10.6	The federal government should facilitate and support the development of smart city and sustainable infrastructure reference architectures.

- Recommendation about specific reference architecture would be helpful, similar to the recommendation that the government. should create the "farm of the future" model.

Supporting recommendation 10.7	The Sector Risk Management Agencies (SRMAs) should collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience.

- The report would benefit from statistics and pictures. For example, a simple graph that will illustrate that the majority of cities are "small cities". Mr. Chan suggested similar data for other areas: in agriculture, 98% of farms are family farms, and 2-3% are corporate farms; in manufacturing, most business are small (75-80% have 50-100 people).

Key Recommendation 11.0: Healthcare

Mr. Witte indicated that the key recommendation text is still being developed.

Supporting recommendation 11.1 (Under Review)	Raise Priority for IoMT to Healthcare Facilities' Executive Leadership Team.

  - This section is largely still to be developed; the meeting agenda calls for discussing healthcare recommendations on Day 2.
  - The proposal to stockpile IoT devices (section 2.8) might also be applicable to healthcare.
  - The proposal to promote interoperability of healthcare IoT could appear in healthcare, in standards, or both (with appropriate cross references).

Key Recommendation 12.0: Public Safety

Mr. Witte indicated that the key recommendation text is still being developed.

Supporting recommendation 12.1	The federal government should create a stockpile of public safety IOT devices that is available for immediate access.

  - Public safety recommendations have mostly focused on first responders; there is potential for a broader range of recommendations.
  - Mr. Griffith noted that many building sensors are relevant to public safety, such as fire and occupancy sensors.

- ○ An icon in the proposed legend could be used to call attention to public safety-relevant recommendations.

Key Recommendation 13.0 Smart Traffic and Transit

Mr. Witte indicated that the key recommendation text is still being developed.

- ○ The IoTAB has provided "lots of great data" about smart traffic and transit.

Supporting recommendation 13.1	The federal government should consider developing programs and grants to allow underserved and less developed communities as well as rural areas.

Supporting recommendation 13.2	The Federal Government should provide overarching regulatory guidance for the drone industry.

- There may be conflicting regulations in development regarding the drone industry. This could be an area to respond to the charter's call to identify where existing regulations are an impediment; an example is a regulation limiting each operator to a single drone.

Key Recommendation 14.0: Supply Chain Logistics

- Mr. Witte presented an overview of the Supply Chain and Logistics section.
  - He highlighted some specific areas including supply chain logistics themselves, a national strategy, incentivizing adoption, partnerships, international collaboration, and measuring progress.
  - Mr. Witte needs to confirm he has preserved the evolutionary order that they were presented.
  - Mr. Moss noted that the IoTAB had supplied a substantial amount of content that was not represented in the draft report. He also expressed concern about the input being rewritten.
    - Mr. Witte responded that was a result of time constraints and the material would be added to the post-meeting update.
- The following recommendations were approved at the May IoTAB meeting for inclusion in the report's Supply Chain Logistics section:
  - Supporting Recommendation 14.1: National Strategy for IoT In Supply Chain Logistics
  - Supporting Recommendation 14.2: Incentivize Adoption Of IoT in Supply Chain Logistics
  - Supporting Recommendation 14.3: Federal entities can also help establish and foster public-private partnerships (PPPs) focused on IoT adoption to facilitate collaboration and knowledge sharing between government agencies, businesses, technology providers, and academia
  - Supporting Recommendation 14.4: Promote international collaboration in IoT adoption across global supply chains to share knowledge, best practices, and resources between countries & regions, driving innovation & accelerating widespread adoption of IoT technologies in supply chain operations worldwide.
  - Supporting Recommendation 14.5: Monitor And Evaluate IoT Adoption Progress in supply chain logistics
  - Supporting Recommendation 14.6: Sustainable, Scalable Manufacturing Growth
  - Supporting Recommendation 14.7: Trusted Architectures for Provenance & Traceability

- ○ Supporting Recommendation 14.8: Incentivize IoT Systems Supply Chains to Adopt Trusted Traceability
- ○ Supporting Recommendation 14.9: Promote traceable and trusted IoT network ecosystems made of devices, systems, networks, and personas operating in connected IoT environments
- ○ Supporting Recommendation 14.10: Accelerate Evolution of Trusted Digital Threads Across Value Chains
- ○ Supporting Recommendation 14.11: Subsidize Digitalization of Enterprises in the Value Chain
- ○ Supporting Recommendation 14.12: Promote Creation and Orchestration of Trusted Value Chains
- ○ Supporting Recommendation 14.13: Subsidize Orchestrated Public-Private Partnerships Across Value Chains
- ○ Supporting Recommendation 14.14: Facilitate Creation of Data-driven Business Ecosystems (Could move to Recommendation 1)
- ○ Supporting Recommendation 14.15: Evaluate Opportunities, Risks of Using AI in Supply Chains

(Section 10 Conclusion to Report)

- Mr. Witte stated that the IoTAB can provide recommendations to be included in either the introduction or the conclusion of the report.

(Section 11. References)

- Mr. Witte reported that very few references has been suggested so far. He suggested references should relate to things for the IoTFWG to inform Congress about.

Reminders

- Ms. Cuthill emphasized that IoTAB members should provide their inputs to Mr. Witte so that the report correctly reflects the IoTAB's intent.
- In response to a question about government action on the recommendations, Ms. Cuthill reminded the IoTAB that Congress will receive both the IoTFWG and the IoTAB reports and that the IoTFWG is required to explain in their report how they have implemented the recommendations or why they are not implementing them. The presumption is that the recommendations will be implemented.
- Mr. Katsioulas asked whether all references would appear at the end, or whether they should appear closer to the relevant subject matter.
  - ○ Mr. Witte expressed flexibility on presentation and suggested that references should provide support for what the IoTAB is saying.
- Mr. Katsioulas suggested having references at the end of each section.
  - ○ Mr. Witte indicated that is up to the IoTAB.

Group Discussion on Report Follow-up

- Mr. Mehra inquired about the procedure for IoTAB members to provide edits.
  - ○ Ms. Cuthill explained that comments could come in from external parties via the website and would need to be consolidated with IoTAB member comments for action and discussion. She said the expectation is to receive comments in the form of marked-up documents.
- Mr. Katsioulas stated his intent to circulate the updated draft to colleagues and consolidate their comments.

- ○ Mr. Witte emphasized that those comments will still need to be reviewed and any changes approved by the IoTAB.

- Mr. Witte stated that IoTAB members should wait for the updated post-meeting report for detailed review and feedback.
  - Mr. Chan told Mr. Witte not to work further on the unapproved recommendations that were included in the pre-meeting draft. Ms. Mehra requested the removal of those recommendations, saying their presence was confusing. She suggested they could be placed in a separate document.

Discussion on Adding a Legend

- Ms. Cuthill asked whether there was IoTAB consensus for including a legend, as had been suggested.
- Ms. Mehra suggested that the legend could indicate both prioritization and levels of funding associated with individual recommendations.
  - Mr. Witte agreed that was possible.
- Ms. Mehra expressed concern that presenting recommendations in NDAA topic order could result in the top priority recommendations from the IoTAB not receiving appropriate attention from the IoTFWG or from Congress.
- Mr. Bergman noted that the NDAA language is often phrased as "e.g.," and he didn't believe it needed to be treated as "must haves".
  - Mr. Witte concurred that it is up to the IoTAB to determine what content to include, but also noted that the sponsors of the legislation had expressed strong interest in certain topics, hence the desire to tag those items in the compliance matrix.
- Mr. Chan requested Mr. Witte provide more a more specific proposal for a legend, so that the IoTAB could see what was requested.
  - Mr. Witte said he would work on this, but it probably would not be ready for the post-meeting update.

Group Discussion on Updates for the Report

- Mr. Witte explained that the report would be expanded from the pre-meeting draft both with content that there had not been time to include in that draft, as well as recommendations reviewed and approved at this meeting.
- Mr. Katsioulas summarized the path ahead as revise the structure as discussed, harmonize the final recommendations, and add the additional content. Mr. Witte added the need to remove requirements still under review.
- Ms. Cuthill stated that both versions of the report would be made available via the IoTAB website under meeting materials, in the interest of transparency. Mr. Witte added that versions would be distinguishable by date.

Group Discussion on Relationship of the IoTAB and IoTFWG

- Ms. Cuthill informed the members that the IoTFWG has published a preliminary update to their web page. She said the intent is to collect feedback on the work of the IoTFWG, and the preliminary update shows the direction for the road map that the IoTFWG is creating.

- Mr. Witte noted that an FRN will be published about the report and provided a link to the IoTFWG web page[5] that includes a link to the preliminary update. Ms. Cuthill noted that Mr. Witte is working on both the IoTFWG and IoTAB reports.
- In responds to IoTAB member questions, Ms. Cuthill stated that the IoTAB's report was input to the IoTFWG's work, but that members could also submit comments on the preliminary update. She stated the preliminary update has a callout box explaining how to provide feedback, or IoTAB members could direct their comments to her. She said the closing data for feedback wasn't firm but would likely be in mid-September.
- Mr. Witte said that the notion is that independent public feedback plus the input from the IoTAB's report will advise the IoTFWG on what to recommend to congress in 2024.
- Mr. Chan encouraged the subgroups to get their inputs assembled, suggesting that subgroup input was better than individual inputs. Mr. Witte indicated that either was acceptable, based on the subgroups' preferences for how to work, saying all input is welcome.

White House Labeling Announcement

Mr. Bergman provided an update from the White House event announcing the labeling program. Mr. Bergman reported:

- There was broad support from a variety of sectors: internet service providers, cloud providers, product and semiconductor manufacturers, academia, industry associations and observers, both houses of Congress.
- It was formally announced that the FCC would administer the program through industry groups.
- The label will be called the US Cyber Trust Mark and looks like a shield with a QR code which will link to more information.
- There was also an announcement that NIST will begin working on a similar set of criteria for consumer grade routers.
- The FCC will be dropping a notice of proposed rulemaking (NPRM) in two to four weeks.
- Multiple press organizations picked up the story.
- There are products ready to be certified, for example locks, washing machines, and baby monitors.
- The event was recorded on WH.gov/live.

Action Items and Wrap Up

- Mr. Chan shared the Day 2 agenda, and announced there was consensus to end the Day 1 meeting.

Closing

Ms. Cuthill adjourned the meeting at 4:22pm.

[5] https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/iot-federal-working-group

IoTAB Meeting on Wednesday, July 19, 2023

Opening Remarks

Ms. Cuthill opened the day's meeting. She thanked people for attending and turned the meeting over to the chair, Mr. Chan.

Mr. Chan reviewed the agenda and introduced the invited speakers.

- There will be three speakers: Christopher Moore; Sven Dharmani, from Ernst & Young, invited by Robby Moss; and Mei Lin Fung, from People Centered Internet, who was invited by Ann Mehra.
- Yesterday the Board finished discussing the draft report. Today we will go over the draft recommendations that didn't make it into the report.

Invited Speaker – Christopher Moore, President, Mission Critical Insights, LLC

Mr. Christopher Moore, President, Mission Critical Insights, LLC

Slide Deck: Presentation to the IoT Advisory Board

Mr. Moore briefly described his varied 31-year career in law enforcement and public safety at various levels of government from local to national, including the technology side of public safety communications and his involvement in the establishment of FirstNet. His intent was to discuss how IoT impacts public safety.

- Mr. Moore introduced what he considered the top five issues in public safety: Public Safety Next Generation 911; Public Safety Communications; UAS in Law Enforcement; School Safety; and Cyber Security.
  - Regarding 911: He explained that the US 911 system is over 60 years old and has been limited in its ability to modernize due to dependence on state and local funding. The volume of information handled by 911 dispatchers today is "overwhelming". A combination of IoT and AI can improve that process with AI identifying the more important information to push out to responders. Mr. Moore stated that urban areas are generally better served but that there needs to be equity across all parts of the nation.
  - Regarding public safety communications: drawing on the success of the FirstNet program. He noted that an important aspect of that program was requiring bidders to identify how they would market the capability to public safety organizations. He stated that similar provisions should be part of any large-scale government investment in IoT for public safety to increase the likelihood that the benefits would be realized through adoption by the community.
  - Regarding UAS (or drones) in law enforcement: UAS have proven to be "an outstanding tool" in reducing response times and providing real-time information to responders, such as information for firefighters and locating people in search and rescue operations. A number of cities have had great success using drones in incident response. Mr. Moore acknowledged the privacy and civil rights concerns associated with drone use and recommended strong community involvement and clear policies that address citizen concerns as the best approach.

  - Regarding school safety: Mr. Moore identified school safety as an area where there is rapid technology advancement but a lack of interconnection. He cited the example of panic buttons that don’t effectively connect to police departments. He acknowledged the concerns about having officers and cameras in schools but also recognized their benefits at critical times. He concluded that schools are a “great place to start” with regard to public safety, citing the availability of significant funding, adding that recommendations in this area should include requirements for coordination between departments.
  - Regarding cybersecurity: Mr. Moore noted that denial of service and ransomware attacks against cities, including 911 systems, have become more common. He acknowledged the range of abilities of different departments to respond to cyber-attacks and suggested that more funding to improve that ability would be helpful.

- Mr. Moore moved on to discuss the intersection of policy and technology in the realm of public safety.
  - He stated that public safety departments deploy large amounts of technology and are often accused of using it for unintended purposes. He cited facial recognition and license plate readers as examples of such technology, saying that both had helped in solving and preventing violent crimes while “aggressive” officers have expanded the use of the technology. The solution is to develop community guidelines based on accurate information about how it operates. The use of the technology would then be audited to address community concerns. Data retention considerations should be addressed as part of the guidelines.
  - Mr. Moore stated that privacy and civil rights are topics that apply across all of the technologies he was discussing. He stated that it was important to have information available through appropriate processes involving warrants and judicial oversight. He raised the concern of technology companies precluding access to customer information by making it inaccessible (“going dark”), describing this as “a real concern for law enforcement.”
  - Mr. Moore discussed the connection between public safety and transportation. He identified autonomous vehicles as a growing concern, saying they are “just not ready for prime time”. Mr. Moore also identified connected cars and trucks as potentially helpful with improving road safety and efficiency. He raised the concern that law enforcement has not been included in conversations regarding the maturity of the technology.
  - Mr. Moore emphasized the value of standards in promoting interoperability and driving down the cost of equipment, saying there is a need to move away from proprietary solutions for the law enforcement market. He said that the federal government is in a unique position with the ability to require open standards on large procurements and emphasized the need for interoperability in public safety communications.

- Mr. Moore provided several recommendations.
  - Vendors in grants and procurements should be required to provide a user adoption plan. Unknown or expensive capabilities will not be adopted.
  - Bidders in federal procurements should be required to provide an IoT plan, showing how they have at least considered the use of IoT in possible solutions.
  - The adoption of new technology should be supported with community engagement, the development of appropriate guidelines, and an auditing process.

Group Discussion

- Ms. Mehra: Raised the issue of crisis response and whether if there was a standardized IoT tool kit that could be applied at the time of need, packaged and labeled for addressing multiple incidents, would this be of value to public safety officials locally, regionally, internationally?
    - Mr. Moore: Right now, public safety and EMS personnel are problem solvers, and many one-off applications that have been created that address certain issues, but they are not connected. The private sector is doing a great job of developing things, but they aren't standardized; they need guidance for how to make it useful and cost effective.
- Mr. Tseronis: what metrics (e.g., coverage, connectivity, data throughput, latency, interoperability) are most important to the public safety community?
    - Mr. Moore: Our priority is always coverage, then speed, then cost. Cops need consistently working communications regardless of spectrum. Coverage is tough because it is expensive. FirstNet brought connectivity to rural areas that didn't have any. The federal investment for $42B for rural broadband is really important for the community.
    - Support for user adoption is also important: have a plan, execute to it, be held accountable provides a specific measure for contract fulfillment. It is important to show progress even if specific goals aren't met.
    - Metrics for technologies such as facial or license plate recognition are also important. It is reasonable to expect law enforcement to report how they are actually used and what results are achieved.
    - The availability of spectrum is important. Public safety usage is intermittent but critical when needed. The community has to work with the FCC to protect access to spectrum granted to public safety after 9/11.
- Mr. Caprio: Do you have any specific grant and solicitation programs in mind where IoT should be incorporated?
    - Mr. Moore: The rural broadband program is one example. Don't believe that many programs have addressed IoT/ Departments all across the government should be doing that. Each department can determine how much weight to give it, so the vendors are forced to think about it. Believes that once the capabilities are available, they will receive broad use.
- Mr. Katsioulas: Finds great value in Mr. Moore describing the use cases where we can have value in a way that brings in the economics. You are trying to raise $17 billion (for 911 upgrade), that requires some harmonization and uniformity. How do you make the justification in ROI? How would you go about creating that harmonization and make the mitigation?
    - Mr. Moore: Stories are what you need for Congress. For example, the earthquake in DC in 2010 had an impact on the network and the response was not acceptable for public safety. That message got to Congress. The whole idea is to tell a story and bring people together.
    - For next generation 911, the biggest cost savings is through consolidating centers. Labor unions have objected over limiting jobs, but there's a shortage of dispatchers. The current 18,000 call centers can be cut to one-third and be more efficient to get the job done.

Invited Speaker – Sven Dharmani, Ernst and Young

Robby Moss introduced Mr. Sven Dharmani and indicated he would talk about real world examples of IoT usage in managing supply chains. Sven works with clients every week on how they are using IoT.

Mr. Sven Dharmani, Ernst and Young

Slide deck: Future of Supply Chains & IoT / Sensor Data Use

- Mr. Dharmani leads the automotive and advanced manufacturing supply chain team at Ernst & Young, with a recent focus on Industry 4.0, which includes GPS tracking, RFID, and IoT/sensor data. His subject is the future of supply chains, including describing some digital supply chain use cases.
- Mr. Dharmani described supply chains from the late 1980's to 2015 as "fairly linear" and designed to be low-cost and efficient, saying these linear and lengthy supply chains typically included offshore manufacturing and at least one ocean lag and were not resilient. He said the environment changed with Brexit in 2015-16, followed by changes US/China trade policies and other political change, and as a consequence those supply chains fell apart. He said this led to disruptions, and then supply chain failures during the COVID pandemic, driven by capacity issues, and lack of resiliency and alternate sourcing, with most companies relying on single source products.
- Mr. Dharmani stated that the current direction is toward resilient, transparent supply chains. He said these changes include a big focus on sustainability, which is now a goal rather than a reporting item. Mr. Dharmani stated supply networks have replaced linear supply chains, leading to companies having to collaborate in some areas and compete in others, and provided the example that LG is now a supplier to Sony.
- Mr. Dharmani said that companies are looking for transparency and agility in their supply networks, so that if there is an event they can respond quickly. He stated that digital supply chain capabilities such as IoT sensor data are key to creating transparency and agility, saying they have been able to leverage IoT sensor data to save customers hundreds of millions of dollars.
- Mr. Katsioulas asked if supply chain resilience includes security?
  - Mr. Dharmani said yes, explaining that they define resiliency as the ability to recover after an event; prevention of the event is the security element, including cybersecurity. He said that as the supply chain becomes more digital there are more entry points that can disrupt the network, citing the example of an automotive plant shut down for four weeks due to a cyberattack. Cyber and security is an element to prevention, but resilience is more the ability to recover from an event, which could be any of cyber, physical, supply chain disruption, or natural disasters, and could be short or long term.
- Mr. Bergman asked if traceability includes carbon footprint.
  - Mr. Dharmani answered that it does. He stated that European companies are far ahead in terms of considering carbon emissions and other regulations to create visibility both their own supply chain and their supplier's supply chains, in part to determine the environmental impact of their choice of suppliers.
- Mr. Bergman described a HBOM proposal published by DHS. Carbon footprint is one of the fields proposed but not yet added, to enable building up the carbon footprint of a products components.
  - Mr. Dharmani said his focus today is sensor data, but that he could return to discuss other elements.

- Mr. Dharmani's first case study discussed the optimization of maintenance activities through data-driven scheduling decisions and ML-driven reliability improvement:
    - He described a federal agency responsible for maintaining older aviation equipment. The agency was performing routine on-site inspections, requiring substantial travel to the equipment's location. The agency also had an overload of sensor data that they were not harnessing.
    - Dr. Dharmani said the staffing impacts of the COVID pandemic created an expectation for massive failures and a drop in availability that did not happen. This led to the question of whether they had been over-maintaining the equipment, and an inquiry into determining the right amount of maintenance.
    - Mr. Dharmani described the process developed to ingest and analyze the available IoT sensor data, maintenance logs and other data to identify events that indicated equipment failures. The approach used a ML model to identify the variables that were the most effective indicators. He said these models were then compared to historical data, allowing continuing improvement in the ML model. The result was the ability to predict failure days in advance with high accuracy, saving unnecessary travel and enabling the agency to support the systems despite a shrinking workforce.
- Mr. Dharmani's second case study described the benefits of collecting GPS data on returnable ISO tanks mounted in frames used in shipping hazardous chemicals. The benefits included higher asset utilization, reduced inventory, and stable supply. Due to the large expense of establishing a chemical plant they are few in number and strategically located so that the materials are shipped to where they can be processed. The associated supply chains are long and extend around the world.
    - Mr. Dharmani explained that the customer was experiencing a very low rate of turns (i.e., trips for each tank), typically about two per year compared to an industry benchmark of four. Equipping the ISO tanks with GPS tracking permitted creating a global inventory of tank locations; GPS data collection rates are adjusted for the tanks circumstances, with less frequent collection during ocean transport and more frequent collection during land transport. This data enabled applying analytics to tank movements.
    - The first result Mr. Dharmani described was the detection of inefficient supply routes. Analysis across all of the company's routes, leading to a "double-digit millions" in cost savings.
    - The second result Mr. Dharmani reported was associated with evaluating situations where ISO tank locations were static for excessive periods. He described several variations:
        - A long lead time for returning a tank was due to the customer using the tank as storage while gradually emptying it, leading to return times of 18 days rather than 3. This enabled the tank owner to coordinate with the customer, charging additional costs for holding the tank for extended periods.
        - Tanks sitting in customs holding for more than 3 days, which is indicative of problem with the bills of lading, shipping manifest, or other administrative information. The use of GPS location data and geofencing enable the creation of alerts for this situation, permitting a response in days rather than weeks. This, in turn, avoided expensive and time-consuming plant shutdowns due to lack of raw material.
        - The third result was identifying tanks with no movement, being used as storage. This enabled the tank owner to recognize the need to classify when an ISO tank is being used for storage, versus transport, charge appropriate leasing fees, and procure additional tanks in order to maintain transport capacity.
- Mr. Dharmani summarized that these case studies illustrated the potential for supply chain improvements driven by GPS tracking data and associated analytics. He described this as a combination

of technology (the GPS location sensor), combined with analytics and process improvements based on the analytic outputs.

Group Discussion

- Mr. Katsioulas thanked Mr. Dharmani for a use case illustrating the "three pillars" of technology, analytics, and workflow, with the goal of optimizing the supply chain for timely delivery. He asked about the semiconductor supply chain and Mr. Dharmani's view of how to remove the barriers to adoption and accelerate the digitalization of enterprises and the front-end (materials to fabrication) and back-end (fabricated chips) supply chains?
  - Mr. Dharmani replied that it is necessary to focus where it possible to drive value, saying it is hard to drive value if you attempt too much at once, which leads to a loss of executive support. He said it was necessary to look at pain points in the business and find opportunities to address them with digital capabilities. He added a couple of examples:
    - Example 1: the use of ML/AI in supply chain forecasting and planning. Mr. Dharmani said we have better techniques now to create more accurate models that can incorporate outside factors (climate, other related production, etc.). He said they have achieved >90% accuracy with models (up from 70%) in forecasting the next 6 months, leading to the ability to carry less inventory, do less "firefighting".
    - Example 2: a "control tower" that looks at inbound supply to plant so that the business can factor in disruptions; he used the example of an Interstate highway crash delaying supplies. Mr. Dharmani said this allows a business to rearrange activities in response to the disruptions (e.g., reschedule maintenance, adjust labor schedules). He observed that there is a cost associated with processing the data, and emphasized that people, process, and technology need to work together to enable people to respond to problems.
  - Mr. Dharmani concluded that the results have to drive value, and create tangible savings or operational improvements, or the business won't proceed past a pilot effort.

Invited Speaker - Mei Lin Fung, Chair, People Centered Internet

Ms. Mei Lin Fung, Chair, People Centered Internet

Ms. Mehra gave an introduction. Co-founder of PCI, envisions a people-centered sustainable future where digital systems serve people, communities, planet. Visionary / luminary / international researcher. Co-Chairs TC on sustainability; author of UN report on digital innovation; contributor to Think7 think tank of G7; leading people-centered science / transformation work; leads a UNDP / ITU org; works on Internet and IoT. Focusing on barriers to adopting IoT.

Slide deck: Can Internet of Things be of the People, by the People, for the People?

- Ms. Fung introduced her topic as how we can have Internet of Things that is of, by, and for the people? She said this meant advocating a way for people to be involved not just in use of IoT, but in adapting it to enable us to flourish as humans and steward the planet.
- Ms. Fung identified three barriers to global adoption of IoT:
  - Security & privacy, noting the lack of assurance and update by IoT makers;
  - Identity, explaining that devices don't have specific identity to track through their life cycle, including disposal;

  - Lack of standards, which she said causes expensive custom devices that inhibit widespread use. She described standards as enabling increasing functionality and the creation of digital building blocks that could reduce up-front and operating costs and increase reliability and functionality.

- Ms. Fung introduced the acronym LLII, which stands for License, Label, Identity, Interoperability, as the approach to address these barriers. She mentioned her involvement in the IEEE Standards Association's Planet Positive initiative, which she said is focused on green, resilient technology development. She cited a "responsible tech checklist" from that initiative, which she claimed can help with labeling efforts, and read the checklist elements.
- Ms. Fung presented a cycle with four components, and described each:
  - 1. People consume tech 24/7 and it affects our health and lives. We have nutrition and food labels because they affected our health and lives. This is why we need to do licensing and labeling because of the effect on our health.
  - 2. We should keep improving the design, development, use, and disposal of technology in an iterative, cyclic, dynamic process; Ms. Fung said continuous improvement was required.
  - 3. We have to get feedback by the people who designed it and the developers, but also the public interest advocates and citizen users, to identify harms and respond to them and detect unforeseen consequences, some of which may only emerge over time from research.
  - 4. An adaptive IoT licensing and labeling process which allows evolving, appropriate, timely response at each stage of a device's lifecycle.

- Ms. Fung pointed to the need to support the cycle with mechanisms for rapid feedback, describing voice-enabled conversational AI as a way to provide immediate feedback. She described this concept as "licensing and labeling at Internet speed and scale".
- Ms. Fung said that licensing and labeling for IoT should learn from drug and nutrition labeling. The described this as a need to alert people to how they are affected by what they consume. She said we consume technology today and so need to do labeling. She said that licensing can allow for appropriate and timely response to both positive and negative impacts, noting that we want things that work to spread and people to have confidence in them.
- Ms. Fung stated that we cannot expect innovations and beneficial outcomes automatically, but rather that licensing and labeling requires quick human intervention but enables dynamic systems that allow us to respond, rather than waiting for a problem to appear followed by a backlash and responding with regulations.
- Ms. Fung said that it is up to technologists to decide how technology is designed and developed, and whether we believe that technologies that are being built to work and serve are in the best interests of humanity.
- Ms. Fung expressed support for the U.S. Cyber Trust Mark announcement and the range of industry support and stated that PCI recommends it be supported by a participation and feedback process enabling iterative improvement. She said the technology exists for that process, but the institutional will is needed.
- Ms. Fung presented the IEEE Planet Positive list of guiding principles, noting that principle #9 calls for responsible use of technology and technology labeling. She explained the point of that principle is to get and track feedback throughout lifecycle at clear checkpoints from design through end of life. She acknowledged that there can be different maturity levels but stated a desire to recognize the efforts of those (vendors/providers) who are more responsible.
- Ms. Fung added a recommendation to bring the marketplace in to by inviting insurance companies to participate in standards development, licensing, labeling design and operation. She said their

involvement would enable more affordable insurance of IoT and allow the market to expand as more people will be "confident they will be taken care of".

- Ms. Fung presented a concept for IoT identity, saying it should point out the phase the device is in, and noting that identity might be different for different versions of a device. She said the PCI wants identity to exist before and after the manufacture of the device, as well as for each "field use" to support diverse multi-layered use of IoT devices through end-of-life and disposal.
- Ms. Fung described interoperability as an area that could drive US global digital leadership in IoT. She stated that interoperability is the biggest commercial barrier and is needed to increase functionality and drive down costs. She suggested that IoT meeting the broad range of needs in California agriculture can be adopted to broad range of applications, environments, and use cases, and be useful around the world. She also suggested emulating the model used by the Internet community of an interoperability event that would promote IoT interoperability.
- Ms. Fung summarized that PCI believes the four elements of license, label, identity, and interoperability can address the three barriers of security, identity, and lack of standards, supporting the concept of IoT of, by, and for the people. She added that the PCI community created the recommendations and has the ability to help achieve them, and said the presentation includes an appendix with 5 pages of input from PCI community.

Group Discussion

- Ms. Mehra stated that interoperability, standards, labeling are the key recommendation she had gathered as take-aways, that these align with key IoTAB recommendations, and that Ms. Mehra appreciated the confirmation.
- Mr. Bergman related characteristics of the U.S. Cyber Trust Mark that aligned with elements of Ms. Fung's presentation, including the use of NIST requirements as a basis, the intent of NIST and industry to iterate to higher levels of security, and the including of a device ID as a component. He acknowledged that the privacy goals of PCI were less well represented.
  - Ms. Fung noted the need for an agile adaptation mechanism, and "strongly proposed" the use of conversational AI for both citizen feedback, and also amongst designers, regulators, and legal to speed things up when danger is involved as well as speeding the production of "more useful things".
- Mr. Katsioulas noted that all of the LLII items are intertwined. He reviewed the concept of identity being evolving and asked how to track all that, and whether Ms. Fung could offer examples.
  - Ms. Fung replied that she thinks timestamp is a useful component; suggested the use of chronological time combined with a QR code pointing to the registry for devices. The timestamp could indicate where the device is in its lifecycle.
- Mr. Chan asked Ms. Fung's view situations such as smart cities that imply a user base for the IoT with broad range of technical literacy and applications often aren't usable.
  - Ms. Fung described this as an example of why voice-enabled conversational AI should be used, saying that that technology 40% of the world is left out. She described this as a big problem for global IoT adoption. She emphasized that conversational AI enables interactions with just a "dumb phone", permitting interchange between people and the cloud to get information. She described this approach as "a fantastic thing for ESG reporting". She concluded that the only way to determine if something is people-centered is to ask the people.
- Ms. Rerecich noted that Ms. Fung's presentation aligns with many of the board's conversations and asked her perception of gaps between PCI's concepts of labeling and the new U.S. Cyber Trust Mark.

  - Ms. Fung repeated the need for a dynamic feedback process. She used the example of video game makers understanding how to do dynamic response, needing to respond to how players react to the game, and suggested they could contribute to conversations about how to make the U.S. Cyber Trust Mark process more responsive.

- Ms. Reynolds expressed interested in the concept of voice feedback, noting that reliance on QR codes and smart phones are not accessible to everyone. She noted that IoT products aren't static and someone of any age should be able to get information. With regard to interoperability Ms. Reynolds pointed out that there really isn't an interoperability component to privacy.
  - Ms. Fung referred back to the cycle she had described and explained how the feedback mechanisms there can help with identifying privacy problems and making adjustments. She also mentioned the potential for doing privacy testing in the context of an IoT interoperability event such as she had described.

Discussion of Recommendations Not Ready to Proceed in May

Mr. Chan identified the recommendations not ready to proceed in May: privacy, international, healthcare, public safety, and international.

Privacy Subgroup Discussion

Privacy team members: Debbie Reynolds, Kevin Kornegay, Maria Rerecich, Mike Bergman

Ms. Reynolds presented for the subgroup.

Slides: Recommendations on Privacy

(Note: Recommendations are provided in thematic groups rather than strict numerical order)

ID: PRV-R01	Use Plain Language in Privacy Policies as part of the Federal Acquisition Regulation (FAR) requirements per the Internet of Things (IoT) Cybersecurity Improvement Act of 2020
Status: Moving Forward in Principle	Issues: None identified at this meeting.

- Researched federal mandates related to IoT cybersecurity or privacy and continue to recommend the Plain Writing Act as a model. Recommendation is to align with FAR requirements and IoT Cybersecurity Improvement Act of 2020 and ensure privacy policies are written in plain language.
- Indicated some jurisdictions (e.g., California) have done work in this area and could also be models.

ID: PRV-R02	Establish clear policies for third-party data sharing and IoT device data use
Status: Moving Forward in Principle	Issues: None identified at this meeting.

- Two previous recommendations were combined into this one. This leverages public awareness campaigns and aligns with cybersecurity strategy implementation plan elements. Also, it touches on privacy regulation at all levels of government and would be another opportunity to increase adoption, helping consumers and business understand data risk.

- Responding to a question about zero-party data, Ms. Reynolds indicated that zero-party and third party are different. Third party is transferred to another party and zero party is more like public data, has no privacy or regulator issues around it. Third party data should have associated transparency and where relevant, a consent mechanism. She indicated that third party data heightens regulatory scrutiny, is the greatest source of concern and potential liability.

ID: PRV-R03	Develop an IoT Privacy Framework for Innovation and Data Protection specifically tailored to the unique challenges posed by IoT devices
Status: Moving Forward in Principle	Issues: Adjusting the exact title of the Framework and what elements might be called out to provide context.

- Ms. Reynolds indicated this is a place to have a “big win”, where the US can lead and provide a model that might be replicated by other jurisdictions in providing guidelines around privacy that allows organizations to assess their posture / status.
  - The board discussed adjusting the title of the framework and discussed elements of what makes a framework. The board discussed calling it Data Protection over Privacy or to include “Policy” since the existing NIST Privacy framework is on privacy risk management. Some pointed out it’s about more than just policy and should include AI.
  - Mr. Witte emphasized keeping the title simple and that this became a key recommendation because it appeared that a broader framework would cover many areas – that privacy and policy should be baked in and can be part of an “IoT Framework” that would support a number of elements.
  - The Board concluded in favor of including this recommendation as is “for the moment”.

ID: PRV-R04	Add IoT Data Retention Transparency: Establish guidelines for manufacturers to establish clear policies on how long business, government, and consumer data is retained
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: Confirmation on privacy specifics with experts on specifics relating to different persona groups.

- States are passing privacy regulations because there’s no comprehensive privacy law. The American Data Privacy and Protection Act (ADPPA) has come closest to being passed. There are federal proposals floating around and seeing international tension because there’s no US unified federal privacy regulation.
- This recommendation is to include IoT in the ADPPA, specifically targeting data retention & transparency, which currently isn’t in that legislation.
  - Board suggested using “e.g.,” to allow for other laws and confirm the legislation specifics to persona groups.
  - Mike Bergman would like to run it through privacy experts and suggested deferral to next meeting.

ID: PRV-R05	Develop and implement a privacy transparency system for IoT devices, using the "U.S. Cyber Trust Mark" for business, government, and consumer data for Connected Devices and other transparency programs as a guide
Status: Moving Forward in Principle	Issues: None identified at this meeting.

- Addresses difference between cybersecurity & privacy and the potential opportunity to "piggyback" on the U.S. Cyber Trust Mark.
  - The U.S. Cyber Trust Mark isn't a privacy mark but there are privacy elements in the requirements (e.g., data deletion capabilities for redeployment and EOL). This recommendation is not specifically calling for a new label. This is aimed at starting with consumer devices.
  - Discussion on enterprise focus on company's confidentiality while users care about personal data rights (e.g., consumer data vs proprietary data). Companies could use IoT to gather data about individuals they employ.

ID: PRV-R06	Develop educational initiatives that include IoT, targeting workforce development, and enhancing business, government, and consumer data privacy and trust
Status: Moving Forward in Principle	Issues: Considerations for different personas for workforce context.

- Focus on creating IoT-focused educational initiatives for workforce development, business, government, and consumer data privacy/trust.
  - Alignment with the national cybersecurity strategy implementation plan initiative 4.6.1. Looking to see that IoT is part of workforce education.
  - Current IoTAB report talks about work roles and associated knowledge needed, aligning to NIST's education work.
  - Discussion on whether this is for the future builders or users of IoT devices. Concern about security and privacy not being built in at the design level (privacy and security by design).
  - Consideration should be given to personas since workforce is a broad umbrella. Workforce is more than users.

ID: PRV-R07	Promote the implementation of Privacy-Enhancing Technologies (PETs) in IoT systems
Status: Moving Forward in Principle	Issues: None identified at this meeting.

- The goal is to reduce privacy risk. This recommendation touches on several federal initiatives: IoT Cybersecurity Improvement Act, White House's Advancing a Vision for Privacy-Enhancing Technologies proposal, and alignment to initiative 1.2.1 in national cybersecurity strategy implementation plan.

International Subgroup Discussion:

International team members: Dan Caprio, Ann Mehra, Mike Bergman, Tom Katsioulas, Debbie Reynolds

Mr. Caprio, Ms. Reynolds, and Ms. Mehra presented for the subgroup.

Slide Deck: Recommendations on International Considerations

(Note: Recommendations are provided in thematic groups rather than strict numerical order)

- Mr. Caprio stated the group has met several times but may need more time. There is a need to consider additional language surrounding the international promotion of the U.S. Cyber Trust Mark. Mr. Caprio reminded the Board of Steve Kelly's comments in May on request for appropriations. He is interested in the work to be done at NIST, FCC, DOE, and State and for them to have the necessary resources. He is looking to make a recommendation in real time for FY24 to ensure the U.S. Cyber Trust Mark is 'fully successful'.
    - Mr. Katsioulas urged something concrete by August and noted that U.S. Cyber Trust Mark is related to SBOM/HBOM. He indicated an intersection between industrial and consumer IoT trust marks and the CHIPS Act as opportunities for big impact and that there are different needs that may take several meetings.

ID: INT-R03	Create data minimization international framework related to IoT devices, aligning with the NIST Privacy Framework principles ((Control) Disassociated Processing (CT.DP-P))
Status: Moving Forward in Principle	Issues: Explanation of data minimization for the collection and retention of PII and context in using different technologies, and what is the right balance to a justifiable collection of PII for an organization.

- Ms. Reynolds indicated the US is very active on the international scene and had a big win recently with the replacement of "privacy shield" (EU/US agreement). There has been a data sharing / data bridge agreement between UK/US and lots of progress on international agreements.
- Ms. Reynolds pointed out that a thread in these agreements is around data minimization as an international standard. International agreements show different ideas regarding privacy but data minimization answers questions around transparency and retention, which is a major risk companies face specifically with IoT devices. Focusing on a data minimization standard can minimize privacy risk.
    - Since the goal is to minimize collection and retention of PII, members of the international subgroup agreed that there may need to be some explanation of data minimization.
    - Collection and retention will be added. There are privacy issues for collection and retention of data. Need to look at the whole life cycle. Example given where IoT device is thrown out, it may still have PII on it.
    - A question regarding whether this includes data associated with, for example, collection of facial data – anonymizing the data after its collection. Ms. Reynolds indicated that yes, it depends how people use the technology and the perception of minimization to the point of losing utility – over collecting vs. justifiable collection. More companies run into issues because they over-retain information.

ID: INT-R01	Short of standards, both national and international, enable or support development of a pilot, ubiquitous IoT-Enabled Global Health Record (IoT-E GHR). DHHS FDA CDRH to fund; DHHS ONC to manage and certify IoT-E GHR.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: Strawman to be further developed.

- Ms. Mehra indicated this is an early version of the recommendation that may need more work.
    - For an IoT Enabled Global Health Record, there's a lack of getting international agencies and nations to adopt common standards. This creates an opportunity for US to take a leading role.
    - Concerns exist such as: dealing with future pandemics, being forced to migrate into safer environments and needing a GHR that an individual can carry wherever they go.
    - In healthcare, there's an advancement of the number of IoT devices that manage, monitor, and help treat by monitoring vital signs and progressions of diseases (e.g., "liquid cancers"). There's also an anticipation of new devices emerging that would benefit from an IoT-E GHR.
- Ms. Mehra also indicated that the Department of Health and Human Services (especially FDA Center for Devices and Radiological Health) is the governing authority to approve devices. Should seek proposals from industry / academia regarding design of a GHR, select teams to develop pilots working with international partners, allows for experiments, test potential for technology, and invite other nations and international bodies to participate in pilot development.
    - The group discussed additional barriers and concerns (e.g., interoperability, accessibility/cost, equity, privacy issues, consumer having a say on their health record, discrimination for a disease in the record, democratization, and anonymity). US could play a leading role in building a coalition or alliance for other nations to join.
    - Ms. Cuthill raised a scope issue that while certainly IoT is proliferating in healthcare, the charter is for IoT and not medical informatics which can be broader.
    - Several group members indicated some follow-up discussion would be needed. This recommendation stands initially as a strawman to be further developed on scope and as there are existing standards for health records which may make it difficult to exchange data.

ID: INT-R02	To give IoT the consideration and importance it deserves globally, especially given AI, Quantum Computing, and other emerging IoT technologies along with lack of standards, we recommend the establishment of an International IoT Council centered around People.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: Strawman to be further developed.

- This one was not discussed in detail but was included in the slides as a strawman to be further developed.

- In summary of the international subgroup, Mr. Caprio indicated the next subgroup meeting to consider international promotion of U.S. Cyber Trust Mark, a need to ensure US agencies get the funding they will need. He called the mark a big deal, 20 years in the making with many organizations involved. The Board will need to look at promoting internationally, provide timelines, clarify roles, and get international partners 'on board'.

Sustainable Infrastructure Subgroup Discussion

Sustainable Infrastructure team members: Peter Tseronis, Tom Katsioulas, Nicole Coughlin, Steve Griffith, Arman Shehabi, Benson Chan.

Mr. Chan and Mr. Tseronis presented for the subgroup.

Slide Deck: Recommendations on Sustainable Infrastructure

(Note: Recommendations are provided in thematic groups rather than strict numerical order)

ID: SUS-R08	The Federal Government should establish an Emerging Technology (EmT) office within each of the federal agencies.
ID: SUS-R11	The Federal Government should establish a national Emerging Technologies Program Office within the Executive office of the President to ensure that the federal government, state, and local government entities can effectively plan, implement, and manage emerging technology initiatives across the United States.
Status: These recommendations are being combined and reworked. Further consideration is necessary.	Issues: Need clarification on how emerging technologies are defined, how the definition updated over time, and the potential for redundant hiring and unbounded growth of the responsible offices.

- Mr. Chan began with SUS-R08, a recommendation for establishing Emerging Technology (EmT) offices in federal agencies. He described this as evolution of the prior recommendation for a Chief Smart Cities Officer. He described the change as inspired, in part, by the proposed Oversee Emerging Technology Act[6], introduced by Senators Bennet and Warner. Mr. Tseronis picked up the discussion, saying the recommendation incorporated some language from that bill that the subgroup supports. He emphasized the importance of having someone very focused on emerging technology as a primary responsibility, and the subgroup wants to ensure IoT is considered as an emerging technology.
- Mr. Chan noted that SUS-R08 is related to SUS-R11, which was originally a recommendation for a Smart Cities Office at the White House. This recommendation was updated based on the proposed Global Technology Leadership Act[7], with the original language extended from Smart Cities to Emerging Technologies. Mr. Tseronis said the objective was to clarify responsibilities, and noted there was potential to combine the two recommendations.
- There was consensus that these functions are needed, with several members citing other areas in government where many people are responsible but there is a lack of accountability.

[6] https://www.congress.gov/bill/118th-congress/senate-bill/1577
[7] https://www.congress.gov/bill/118th-congress/senate-bill/1873

- Mr. Bergman raised concerns over the lack of specificity about what constitutes emerging technology, and how that definition could be maintained over time. He noted that without clarity of scope, there is potential for various agencies to have different, uncoordinated definitions of emerging technology. He noted there are already some emerging technology definitions out there (such as the list in the *National Standards Strategy for Critical and Emerging Technologies*[8]) and suggested adding a process for determining emerging technologies for these EMT offices.
- Mr. Bergman also raised concerns that some agencies have already established emerging technology positions, and suggested they should not be forced to hire redundant staff.
  - Ms. Megas confirmed that a number of government officials have had “emerging technology” added to their titles, and that IoT has not been consistently included as an emerging technology.
- Mr. Caprio noted that language in the bill about protecting citizens from harm could overlap with the receptibilities of the Privacy and Civil Liberties Oversight Board (PCLOB) and suggested that organization could be referenced in the recommendation.
- The board concluded the two recommendations should be combined and the subgroup should address the concerns raised and return with a revised recommendation.

ID: SUS-R13	The federal government should promote the development and adoption of existing industry standards activities with respect to energy efficient, clean, and renewable energy technologies that are used in sustainable infrastructure.
Status: Moving Forward in Principle	Issues: A clear definition of “sustainable infrastructure” is needed.

- Mr. Griffith described this as an update and clarification of what was presented in May. The government should promote the development and adoption of industry standards, as standards can help to address interoperability, provide scalability, and level the playing field.
- Mr. Griffith acknowledged that there are some significant gaps in available standards, that standard development can take time, and that in some technology areas standards development is quite fragmented.
- Dr. Chandra asked if the board had defined “sustainable infrastructure”, and whether the definition included wastewater.
  - Mr. Chan replied there had been a definition in an early meeting, which was broad and included an environmental aspect. He added that the sponsors were thinking along the lines of environmental sustainability.
  - Mr. Griffith took a note to ensure the report includes a definition.

ID: SUS-R14	The federal government should develop and facilitate programs and grants to reskill existing workers, train future workers across manufacturing, construction, and clean tech/renewable industries.
Status: Moving Forward in Principle	Issues: None identified at this meeting

[8] https://www.whitehouse.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf

- Mr. Chan explained that renewable energy systems are closely tied to IoT, so an inability to deploy such systems is also an inability to deploy IoT, creating a need to address the labor shortage. He identified the funding in the IRA (Inflation Reduction Act) as creating jobs that will be difficult to fill, making it difficult to achieve environmental goals. Mr. Chan described this as a cross-industry problem.

ID: SUS-R15	The federal government should promote the development and adoption of procedures and methods that can accelerate and streamline planning, permitting, and interconnection aspects related to energy efficiency technology projects.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- Mr. Griffith identified the challenges of permitting and interconnections as a “huge issue” for IoT, noting that technologies that use IoT can’t be deployed without permits and saying that 78% of projects don’t get through the permitting process due to the complexity, cost, and duration of the process.
- Mr. Griffith acknowledged activity in Congress and at DOE and NEMA related to this issue, such as the concept of using existing rights of way to build transmission lines.
- Mr. Chan cited a statistic that only 21% of projects initiated from 2010 through 2017 have been built and reached commercial operation by 2022.

ID: SUS-R16	The federal government should accelerate the promotion and adoption of procedures and methods that include IoT technologies to make the electric grid more reliable and resilient. A more reliable and resilient grid can better accommodate the integration of renewable energy sources enabled by IoT
Status: Moving Forward in Principle	Issues: None identified at this meeting

- Mr. Griffith highlighted the need to make the grid more reliable and resilient to make it more amenable to integrating new energy sources, citing a number of shortcomings that are barriers to the use of IoT and where IoT could assist.
- Mr. Chan provide the example of solar generation capacity in California being shut off due to inadequate transmission capabilities.
- Dr. Shehabi suggested it would be helpful to identify specific IoT technologies held back by this issue, as well as how large a market share is involved.
- Mr. Katsioulas inquired about a recommendation related to the distinction between IoT and IIoT.
- Mr. Bergman stated the recommendation had been discussed in the cybersecurity subgroup but was deferred by concerns about giving government the responsibility of deciding market sectors.
- Mr. Katsioulas cited a GAO report that define IIoT but left out many relevant elements, such as process sensors.
- Mr. Griffith agreed that the subgroup needed to have deeper discussions and could return in August with further information.

Precision Agriculture Subgroup Discussion

Precision Agriculture team members: Ranveer Chandra, Nick Emanuel, Ann Mehra.

Dr. Chandra presented the precision agriculture recommendations.

Draft text: Recommendations on Agriculture

- Dr. Chandra reported that the Precision agriculture subgroup had incorporated the feedback they had received at the May meeting but didn't have a presentation prepared. He said they would present their updated recommendations at the August board meeting.

Healthcare and Public Safety Subgroup Discussion

Healthcare Subgroup team members: Ann Mehra, Mike Bergman, Maria Rerecich

Public Safety team members: Maria Rerecich, Nicole Coughlin, Ann Mehra.

Ms. Rerecich reported for both subgroups.

- Ms. Rerecich stated that all the updated recommendations from the Healthcare and Public Safety subgroups had been supplied to Mr. Witte for incorporation into the report and no new recommendations beyond what was discussed yesterday were presented.

Action Items and Wrap-up

Mr. Chan, Chair

- Mr. Chan listed several action items from the meeting:
    - Mr. Witte will incorporate comments and updates from today, will provide an updated draft. and raised some additional points:
        - The report needs actionable recommendations.
        - Graphics would really help to improve the paper and convey information. Mr. Katsioulas indicated he has a few graphics in mind. The secretariat will help to format graphics, so they look similar.
    - Considerations for future meetings or gaps that needed to be addressed were identified:
        - Ms. Reynolds pointed out that intersections with the AI and other areas.
        - Ms. Reynolds pointed out concerns about coverage for legacy data and legacy devices including handling data from end-of-life devices, which is a huge issue. Mr. Katsioulas suggested this issue can be used to incentive adoption of new devices.
        - Environmental monitoring needs to include other use cases.
        - Connectivity discussion and recommendations also need more coverage. Dr. Chandra offered to join the drafting team on connectivity recommendations.
        - Suggestions for invited speakers should be submitted to Mr. Chan for the August meeting.

Ms. Cuthill adjourned the meeting at 4:59 p.m.