\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)

May 16 & 17, 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 Support

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

- **Donald Davidson**, Synopsys
- **Syed Hosain,** Aeris
- **Jeff Jockisch**, Avantis Privacy
- **Colby Scullion,** Avantis Privacy
- **Harvey Reed,** MITRE

Action Items Over Both Days

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

In General - Members of the Board requested clarity on the following topics for the next meeting:

- User Protection would need more definition and should be discussed in more depth.
- Smart Cities would need more definition and **Ms. Coughlin** indicated she would provide input.
- The Board requested if the IoTFWG could review recommendations for Agency Coordination and provide suggestions for greater specificity regarding agency collaborations or barriers.

For Subgroups:

- Personas - **Ms. Reynolds** to send the chair an update on the drafted section on personas.
- International - Mr. Katsioulas proposed an action to consolidate recommendations related to international matters from other subgroups under the new International Engagement subgroup being started. **Mr. Caprio** will lead the International Engagement subgroup.
- Spectrum - **Mr. Bergman** will lead a new subgroup "Spectrum/Connectivity".
- Sustainable Infrastructure - The sustainable infrastructure subgroup will be split into smart cities and sustainability.

For the Report:

- Overall:
  - The Board agreed that related material from existing subgroups should be contributed to the new subgroup sections of the report where there is overlap.
  - The Board and the secretariat will start to look for common areas in recommendations.
  - The Board emphasized the need to provide the editor with input so that the draft report can be circulated ahead of the July meeting to permit member review before and during Board-level decisions at that meeting.
  - The Board suggested having a complete draft of one section that could make it easier for everyone to have a better sense of where and how to contribute and better place recommendations in context.
- Specific Topics:
  - On the topic of Consumer, Smart Home Regulation, Standards, Personas, **Mr. Bergman** to send an email. **Mr. Witte** to add as commentary sections to report by May 31.
  - On the topic of Skills, Education, Workforce recommendations, **each subgroup** is to send their recommendations to Mr. Chan. **Mr. Witte** to add a section into the report by May 31.
  - On the topic of User Protection and Agency Coordination, **Mr. Witte** to add commentary sections to the report by May 31.
  - On the topic of Emerging Technologies, NIST suggested that **the Board** should consider a discussion of the connections among IoT, AI, and digital twins, as a topic where the expertise of the Board could be looking to the future potential for IoT.
  - On the topic of Recommendations, the Board agreed to proceed on agreeing on recommendations as they were presented and that Board consensus (i.e., lack of objection) was sufficient for a recommendation to move forward in principle.
    - **Subgroups** to update recommendations for those not advanced by June 15
    - **Subgroups** to update recommendations/wording for those that are advanced (and require it) by June 15

On the Schedule:

- Review the draft IoTAB timeline.
- Upcoming meeting dates:
  - The July meeting dates are set (18-19 July).
  - The discussion confirmed meeting dates for August (22nd-23rd) and September (26th-27th).
- **Mr. Witte** stated that the target date for the draft report was 30 June, and that updated recommendations are needed by mid-June to support that target.
- **Ms. Cuthill** said that she would begin working on Federal Register Notices for the future meetings.
- As has been previously discussed – the IoTAB is looking at a one-year timeline with milestones:
  - By the May meeting, all material would be received from the subgroups and the IoTAB would need to identify any additional content or attention to areas of the report.
  - By the end of the July meeting, plan to have complete initial recommendations and use the July meeting to discuss/fill in any gaps.
  - By November, have a near final draft so that the time between November and January which includes holidays is available to refine content to final.

IoTAB Meeting on Tuesday, May 16, 2023

Welcome and Agenda Review

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

Slide deck: Agenda Meeting Slides (slide 1-4)

- Mr. Chan reviewed the agenda including the speakers and subgroups presenting for the day and expected key outcomes. These outcomes included reviewing recommendations, knowledge transfer among members, insights from external speakers, planning for future meetings in July, August, and September.
- After brief discussion, the IoT Advisory Board agreed to proceed on agreeing on recommendations as they were presented and that Board consensus (i.e., lack of objection) was sufficient for a recommendation to move forward in principle.

Invited Speaker – Syed Hosain, Aeris

Mr. Syed Hosain, Aeries

Slide deck: Aeris Presentation

- Mr. Hosain summarized his experience as having been involved in IoT since the mid-1990s, with a focus on devices using cellular communications and supporting enterprise customers and applications.
- His presentation's focus was on barriers to IoT growth, with security, scale, technology, resources, and regulations as the key topics.
- With regard to security Mr. Hosain stated IoT cyber-attacks are growing rapidly, that devices are generally vulnerable, and that most do not use encryption. He said the cost of attacks is very impactful, citing IBM reporting a cost of more than $4M for each event. He acknowledged that security and privacy are receiving attention.
- Regarding cellular technologies, Mr. Hosain explained that many enterprise IoT devices are long-lived, with a useful life far greater than consumer cellular handsets, and as a consequence, cellular IoT devices must either evolve or be replaced as cellular technology changes. He provided several examples of cellular technology "sunsets" in the U.S., and the resulting need for IoT device replacements. He also said that the impending sunset of 4G LTE networks in the U.S. later this decade will create another such event. He also explained the cost and complexity of replacing hundreds of thousands of enterprise IoT devices. He noted that the potential for similar sunsetting of some satellite IoT communications.
- Mr. Hosain described the challenges associated with assigning dialable numbers to cellular IoT devices in large numbers, especially for highly mobile applications. He explained that part of the problem is outdated assignment and allocation policies. He said that the stopgap solution that exists is insufficient, and that while the FCC is aware of the issue it is not being addressed.
- Mr. Hosain discussed the evolving regulatory environment from regulation oriented toward individual privacy protection to an orientation toward protecting infrastructure and addressing cyber warfare issues. He pointed out the challenges of dealing with different regulations in different states that are relatively general and abstract, and that the regulations were often too vague for state attorneys general to enforce. Mr. Hosain said he sees the need for federal regulations, consistent with actions other nations have taken. He specifically noted a Malaysian proposal to require all devices use open-source software as an example of a regulation that applies to architecture.

- Mr. Hosain concluded by noting the availability of a free guide describing what is required to get an application deployed for business IoT users.[1]

Group Discussion

- Mr. Caprio noted the Board's tasking to identify barriers to adoption, and asked Mr. Hosain if he had any recommendations to share.
    - Mr. Hosain repeated that his viewpoint is cellular IoT, with devices often deployed in locations that aren't human accessible. Consumer IoT will have different issues, such as healthcare environments. From a cellular perspective, technology sunset is very important. He noted that the U.S. needs to treat IoT as a national resource that the government needs to support, as has happened in other countries. Different regulations in different states also create a barrier to national adoption.
- Mr. Caprio asked, in term of the IoT market, what Mr. Hosain foresees as IoT adoption over the next five years, and what might the Board do to help drive that.
    - Mr. Hosain responded that more specific regulations driven by understanding of the issues would be beneficial, citing California's SB-327 as being too abstract to be enforceable as a counterexample.
- Mr. Tseronis noted that Mr. Hosain's presentation emphasized the importance of resilience for IoT devices and applications, the need to manage and architect the use of spectrum, and the potential for economic benefits from the application of IoT.
    - Mr. Hosain provided some supporting examples, noting IoT devices that could have worked "for decades", and some of the applications his company supports monitoring solar panels in Africa and tractors in India.
    - Mr. Tseronis concurred, noting the need for secure communications and customer data protection, along with the potential for real time decision making.
- Mr. Bergman mentioned the forthcoming national label program and his expectation that it would extend beyond consumer products to industrial and government applications. He then asked about state laws, noting that SB-327 had been amended to offer safe harbor to manufacturers offering "reasonable security", and asked about initiatives in other states.
    - Mr. Hosain said he had as list of about 14 other states that he would supply.
- Dr. Chandra asked Mr. Hosain's view of the differences in urban vs. rural deployments of IoT, and any special considerations.
    - Mr. Hosain noted that some rural IoT deployment have similar requirements to urban ones. He acknowledged that cellular IoT is "piggybacking" on a human-oriented infrastructure because it exists, and that there are applications where other technologies, such as satellite communications could substitute.

[1] https://www.aeris.com/iotguide

Action Item Review

Mr. Chan, chair

Slide deck: Agenda Meeting Slides (slides 6-9)

- The sustainable infrastructure subgroup will be split into smart cities and sustainability
- The Board and the secretariat will start to look for common areas in recommendations
- The July meeting dates are set (18-19 July)
- Discussion confirmed meeting dates for August (22nd-23rd) and September (26th-27th)
    - Ms. Cuthill said that she would begin working on FRNs for the future meetings

New Subgroups –Connectivity/Spectrum & International Engagement

Mr. Chan, chair

Slide deck: Agenda Meeting Slides (slides 9-10)

- Mr. Chan began the discussion of new subgroups by sharing Mr. Bergman's table from the April meeting. He identified leads for two new subgroups:
    - Mr. Bergman will lead the Connectivity/Spectrum subgroup
    - Mr. Caprio will lead the International Engagement subgroup
- Mr. Bergman explained that he'd tried to show that Board activities that map to the charter, and highlight activities that are optional, and can be addressed if time and resources permit. He summarized the results:
    - Subgroups to close and move to commentary section on important sectors:
        - Consumer
        - Smart Homes
    - Subgroups to close and include discussion under broader themes:
        - Standards
        - Skills, Education, and Workforce Development (after discussion: the IoT Advisory Board agreed to take an action for subgroups to send their workforce recommendations to Mr. Chan for inclusion in a subgroup themed set of recommendations)
        - Regulations
    - Topics from the charter not currently assigned to subgroups
        - Spectrum: Mr. Bergman will lead a new subgroup "Spectrum/Connectivity"
        - User Protection: This need more definition, to be discussed at the next IoTAB meeting
        - Agency Coordination: IoTFWG could review recommendations and provide suggestions for greater specificity regarding agency collaborations or barriers
- Mr. Bergman invited discussion and stated he thought it appropriate the Board approve these restructuring recommendations.
    - Mr. Chan endorsed the recommendations, saying they bring the Board's organization closer in line to the charter.

  - Some Board members raised concerns regarding the elimination of the Skills subgroup. It was suggested this could be handled as a cross-cutting theme in the report.
  - Ms. Cuthill clarified that the recommendations in the Board's report would not be linked to subgroups, which exist as a convenience to develop input from the Board.
  - Ms. Megas noted that the IoTFWG will using inputs from the IoTAB in building a national strategy. The IoTFWG is looking for as many recommendations as possible and will define pillars of the strategy from the inputs. She noted that "themes" identified by the Board in its report would be helpful in identifying areas where significant focus is needed.

- Mr. Bergman noted that he didn't know what "user protection" in the charter means.
  - Ms. Megas responded by quoting from the DIGIT Act: "looking at what can be done to protect the individual in the larger IoT ecosystem, unanticipated ways consumers might be impacted" and suggested the spirit of the language focuses on safety and privacy. She encouraged the Board to think broadly about the topic.
- Mr. Chan noted that there was consensus on moving ahead with reorganization of the IoT Advisory Board's subgroups to align with the charter.

Progress and Schedule Review (AKA Report Status and Considerations)

Greg Witte, NIST Secretariat

Slide deck: Report Status Update

- Mr. Witte stated that the subgroups had produced a lot of recommendations, which the secretariat will consolidate to create a smaller set of strong proposals ("a holistic approach") in a draft report that will be ready for the Board members to review before the July meeting. Other key points:
  - He acknowledged that was still material missing, but that it could be filled in.
  - He encouraged making recommendations specific, measurable, and actionable.
  - He will begin integrating recommendations into the draft report while the subgroups and the Board work on refining them, and the results can be merged.
- He asked the Board to consider "the whole forest" as well as "the trees", saying that the report is an opportunity to do positive things for the nation and needs to tell a story about what IoT could be and do, so themes and objectives are vital content, noting the requirement to describe "significant and scalable economic and social benefits" from IoT.
- Mr. Witte reminded the members of the tasking language from the legislation and pointed out that the Board should not only consider things the nation should be doing, but also things we should stop doing. He asked particularly that Board members apply their knowledge and expertise to the various parts of the tasking with regards to subjects like agency coordination, support to small business, and international engagement.
- Mr. Witte pointed to specific areas where recommendations are needed, pointing to precision agriculture, environmental monitoring, public safety, and healthcare and as topics where there are gaps coming into this meeting. He stated that he would be reaching out for clarifications to better understand some of the recommendations.
- Mr. Katsioulas asked for clarification on how the secretariat would integrate recommendations across groups and optimize common theme.

  - Mr. Witte replied this will have to be an iterative process and involve some use of "artistic license" to pull the material together. He also said there would efforts to coordinate with the Board members ensure the report is correct and accurate.
  - Ms. Megas explained that the IoTFWG would prefer to hear recommendations sooner, even if they are still rough, so they can begin to evaluate and respond to the IoTAB's input. She said the IoTFWG would see the current set of recommendations at their meeting on May 23rd but would want some sense of the consensus for those recommendations. She emphasized that having a July draft IoTAB report would allow time for conversation.

- Ms. Reynolds asked how much content was expected from the subgroups? Would two pages per recommendation be appropriate?
  - Mr. Witte replied that more content would definitely be helpful and give the subgroups the opportunity to ensure their key points are communicated. The secretariat's job will be to smooth all of the inputs make one voice. He concluded that more prose is helpful but not at the expense of delaying inputs for the report.
- Ms. Mehra asked if July would be the first time the IoTFWG will see the preliminary recommendations?
  - Mr. Witte replied that the IoTFWG meets monthly and would be seeing the recommendations at their next meeting in about a week.
  - Ms. Megas stated that the IoTFWG is ready at any time to review recommendations, and cited Mr. Chan's description of having "no sustained disagreements" about recommendations as sufficient for the IoTFWG to consider them. She noted there are 18 federal agencies on the IoTFWG, and they can reach out to others, and IoTFWG will need some time to react to recommendations.
- Mr. Bergman noted that the Board was trying to avoid mandates to implement these technologies and recommended reviewing the language in the subgroups to ensure that there aren't mandates associated with the agency descriptions.
- There was some concern that some recommendations were written as execution plans, instead of describing desirable outcomes.

Sustainable Infrastructure Subgroup Discussion

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

Mr. Tseronis and Mr. Chan presented for the Sustainable Infrastructure recommendations

Slide Deck: Sustainable Infrastructure Presentation

Draft Text of Recommendations: Sustainable Infrastructure Draft Recommendations

Sustainable Infrastructure Background

- Key Questions addressed in Sustainable Infrastructure:
  - How do we enable and enforce a sustainable infrastructure?
  - What's the nexus for different levels of government who don't have the funding to be able to create a resilient infrastructure?
  - How do we get there without the funding or resources to implement?

- The team noted that context was necessary to understanding the recommendations.

Sustainable Infrastructure Recommendations

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

Smart City Implementation Recommendations:

ID: SUS-R01	The federal government should consider the development of Smart City and Sustainability Extension Partnerships (SCSEP).
Status: Moving Forward in Principle	Issues: None identified at this meeting

- Intent is to leverage existing infrastructure; for example, USDA infrastructure
- NIST's Manufacturing Extension Partnership (MEP) can serve as a model. Regional centers can make expertise available to smaller cities.
- Resource constraints are a key issue
- Concerns about government procurement considerations were also raised since being on "preferred vendor lists" or other mechanisms can be required and take time. The concern raised here is that while some cities may have the budgets and can acquire resources and expertise through contracting (e.g. hiring consultants, etc.), the process to procure those services are onerous, take a lot of time, and are not agile. Getting on a "preferred vendor" list simplifies these processes but is a difficult qualification process, and the opportunity to apply to get on these lists occur once every three or four years.

ID: SUS-R08	The Federal Government should establish a Smart City Officer (SCO) within each of the twenty-four (24) CFO Act agencies.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: More research needs to be done on how a "Smart City Officer" would fit into federal government organizational structures.

- Questions were raised about the nature of the "Smart City Officer" position and whether this office would be focused on agency (internal) adoption of IoT or promoting adoption of IoT broadly (external).
- The relationship of a "Smart City Officer" to a "Chief Technology Officer" or "Chief IOT Officer" was another issue needing additional consideration. There were questions about the focus and breadth of the proposed office.

ID: SUS-R11	The Federal Government should establish a Smart Cities 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.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: More research needs to be done on how a "Smart City Officer" would fit into executive branch organizational structures

- This recommendation is connected to the prior recommendation and raises organizational issues that requires further consideration.

ID: SUS-R09	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.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: More information is needed to resolve the relationship of sustainable infrastructure to critical infrastructure and smart cities.

- There is continued discussion of the relationship of sustainable infrastructure, critical infrastructure, and smart cities.

ID: SUS-R10	The Sector Risk Management Agencies (SRMAs) shall collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: As SRMAs are associated with critical infrastructure sectors, the resolution of questions around the relationship of sustainable infrastructure to critical infrastructure is needed to resolve how this recommendation applies.

- This recommendation is connected to the prior recommendation and raises organizational issues that requires further consideration.

Operationally Oriented Recommendations:

ID: SUS-R02	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.
Status: Moving Forward in Principle	Issues: May need to be reconciled or combined with SUS-R12.

ID: SUS-R12	The federal government should specify and utilize energy efficient and sustainable technologies into infrastructure and other projects that are funded in full, or partially, with federal funding.
Status: Moving Forward in Principle	Issues: May need to be reconciled or combined with SUS-R02.

- It was noted that SUS-R12 is a variant of SUS-R02 and the two may need to be reconciled or combined.

ID: SUS-R03	The federal government should consider models to help select adopting organizations sustain and support beyond the initial acquisition and building of new projects incorporating IoT technologies.
Status: Moving Forward in Principle	Issues: This recommendation potentially overlaps with SUS-R06.

- Grants could be available to obtain the IoT technology but not to sustain it over time and the costs to support over the long term can be difficult for local government to support without a new revenue source.

ID: SUS-R06	The federal government should consider offering grants to support smart city projects that target small and midsize cities and agencies.
Status: Moving Forward in Principle	Issues: This recommendation potentially overlaps with SUS-R03.

- This is a different emphasis from recommendation SUS-R03 in the targeting of smaller cities; however, the recommendations are overlapping and may need further work to reconcile.

ID: SUS-R04	The federal government should consider "student loan forgiveness" programs in exchange for providing critical emerging technology (IoT, data science, cybersecurity, etc.) skills to municipalities and agencies.
Status: Moving Forward in Principle	Issues: None identified at this meeting

ID: SUS-R05	The federal government should facilitate and support the development and use of smart city and sustainable infrastructure reference models.
Status: Moving Forward in Principle	Issues: This recommendation has some overlap with SUS-R07.

ID: SUS-R07	The federal government should facilitate and support the adoption of smart city and sustainable infrastructure IoT standards.
Status: Moving Forward in Principle	Issues: This recommendation has some overlap with SUS-R05

- It was noted that this recommendation has some overlap with recommendation SUS-R05.

ID: SUS-R13	The federal government supports existing industry standards development activities with respect to energy efficient technologies that are used in sustainable infrastructure.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: None identified at this meeting

Supply Chain Subgroup Discussion

Supply Chain team members: Robby Moss, Tom Katsioulas, Steve Griffith, Mike Bergman, Ann Mehra.

Mr. Moss and Mr. Griffith presented the Augmented Supply Chain recommendations.

Mr. Katsioulas presented the Supply Chain Traceability recommendations.

Slide deck: Augmented Logistics and Smart Supply Chains

Draft text of the Augmented Logistics recommendations: Supply Chain Logistics Recommendations

Draft text of the Smart Supply Chain (SSC) recommendations: Supply Chain Traceability Recommendations

Supply Chain Background

- Mr. Katsioulas began with pointing out how supply chains connect with smart manufacturing, smart-connected cities, and critical infrastructure. He suggested that if the Board members engaged in some outreach, it would be possible to increase the visibility of the Board and attract a larger audience.
- Mr. Katsioulas presented their subgroup's definitions of augmented supply chain and smart supply chains traceability as a refresher.
    - *Augmented supply chains:* refers to the integration and use of emerging technologies such as IoT, AI, 5G, blockchain, and other digital technologies into traditional supply chain processes. This

integration aims to enhance visibility, improve operational efficiency, reduce costs, and provide greater transparency throughout the supply chain. Augmented supply chains use real-time data and analytics to monitor and track goods from suppliers to end customers, making it easier to identify bottlenecks, optimize operations, and improve overall performance.

- *Smart supply chains:* Smart supply chain refers to a network of interconnected enterprises in a value chain that use digital technologies to exchange information deliver products or services to end-users. Smart connected value chains leverage advanced technologies and digitalization infrastructure to make intelligent decisions by establishing provenance, traceability and market preference through trusted digital thread and data analytics. They adapt quickly to customer needs by anticipating demand, inventory levels, and logistics for assured supply. They enable marketplaces by leveraging the digital thread of data to manage vulnerabilities, establish market preference and create data-driven ML/AI applications and IoT services to maximize security and economic growth.

Augmented Supply Chain Logistics Recommendations

ID: SSC-R01	Establish a comprehensive national IoT strategy that outlines clear goals and objectives for IoT adoption in supply chain management.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- It was noted that this is a very general recommendation that could potentially be applied across multiple subgroups or used as a broad draft recommendation.

ID: SSC-R02	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.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- This recommendation focuses on critical areas of device and data interoperability and security needed for scalability.
- Mr. Chan suggested the subgroup may need to list some examples of areas where this would apply, and of either standards that should be adopted or gaps in available standards.
- Mr. Bergman asked what the deliverable would be from implementing this recommendation. What specific action? And noted that there are already regulations that require government to use industry standards.

ID: SSC-R03	Establish and provide financial incentives aims to encourage adoption of IoT technologies in supply chain operations by reducing initial investment costs and perceived risks associated with implementation of IoT solutions.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- This recommendation can easily span multiple federal agencies.

- Potential implementation mechanisms could include grant programs, tax incentives, and loans and requires more consideration and discussion. The implementation would need to focus on how to identify right beneficiaries of incentives, as there is a potential to create market distortion.
- Mr. Chan noted that the first three recommendations are linked, all are aimed at driving adoption, but there's a feeling of being overly focused on financial incentives. He suggested there may be an over-arching recommendation of which this is one implementation piece.

ID: SSC-R04	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.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- The recommendation emphasizes "fostering", rather than creating, PPPs and emphasizes looking for large projects and other initiatives to use as a basis for public / private collaboration.

ID: SSC-R05	Invest in and promote education and workforce development focused on IoT to address growing demand for skilled professionals capable of designing, implementing, and managing IoT systems in supply chain operations.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- This recommendation cuts across different subgroups. There is a need to identify specific skills for certain types of devices, systems, and networks.
- Technology changes challenge workforces, and often segments of the workforce move on rather engaging with changes in process. Need to think about the necessary skills earlier in education systems, but also plan for continuing education.

ID: SSC-R06	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.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- This may be a cross-cutting recommendation and requires both technology investment and training. Given that DHS has focused on supply chain risk management, they seem like a good candidate as a lead agency. This recommendation is still high-level and needs more detail.
- This topic and supply chain traceability present an opportunity to work with the cybersecurity subgroup, which may lead to several combined recommendations.

ID: SSC-R07	Promote international collaboration in IoT adoption across global supply chains to facilitate sharing knowledge, best practices, and resources between countries and regions, driving innovation and accelerating widespread adoption of IoT technologies in supply chain operations worldwide.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- This recommendation recognizes the global nature of supply chains. In addition to the agencies on the side, it might be possible to involve international bodies like APEC. There's also the potential to participate in international forums and organizations and develop best practices. Some of this is already happening, but the recommendation is to place more emphasis on these efforts. More research is needed on identifying gaps in these efforts.
- Mr. Katsioulas proposed an action to consolidate recommendations related to international matters from other subgroups under the new International Engagement subgroup being started. Mr. Bergman supported the proposal.

ID: SSC-R08	Monitor and evaluate progress to provide assurance that IoT adoption efforts in supply chain logistics are on track, effectively addressing identified challenges and opportunities, and delivering desired outcomes.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- The recommendation focuses on instituting some means to monitor the adoption of IoT as a means to assess the effectiveness of federal efforts. This recommendation is still high level. Its implementation may relate to program offices established in various agencies.

ID: SSC-R09	Select mix of policies, incentives and requirements to support sustainable, scalable growth in domestic IoT manufacturing supply chain. The recommended policies, incentives and requirements are relevant to the transportation sector as it becomes increasingly connected, integrated, and ultimately autonomous. Rapid technological advances are further augmented by communication and IT, including IoT.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- This recommendation focuses on support for domestic manufacturing. Issues with global chains have meant manufacturers have missed goals. Procurement rules can be made more consistent across federal agencies regarding "domestic content", and those rules could be adjusted to expand the scope of what meets that requirement. These changes will ease current constraints associated with meeting "domestic content" requirements during the period required to develop domestic manufacturing capabilities.
- Mr. Katsioulas commented that this could be viewed as an opportunity to establish provenance of digital thread of data in design and manufacturing. The government could then use that provenance as a point of market preference for suppliers to use our manufacturing. He stated government support can make a huge difference in shifting market share.

Supply Chain Traceability Background

- Mr. Katsioulas presented the current list of twelve supply chain traceability recommendations, noting that these are highly connected, and it was likely that some recommendations would be combined in the long run.
- Key questions addressed for supply chain traceability:
  - What is needed to establish the foundations for supply chain traceability?
  - What contributions should government make to facilitate the development of trusted data markets?
  - What are the appropriate data policies to stimulate associated economic development?
  - What is the potential contribution of AI in smart supply chain security?

Supply Chain Traceability Recommendations

ID: SSC-R10	The Federal Government should encourage the use of Global Identifier Standards for supply chain traceability
Status: Moving Forward in Principle	Issues: None identified at this meeting

- Mr. Katsioulas reviewed the levels of identifiers needed to provide traceability and stated that he believed these need to be based on global standards.

ID: SSC-R11	Promote development and use of trusted hardware/software architectures for supply chain provenance, traceability, chain of custody and lifecycle management.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- Mr. Katsioulas said he will be refining this recommendation in concert with the cybersecurity subgroup. He said the scope covered both electronics and physical products and note the challenge of establishing trusted architectures at scale, citing the example of fleet vehicle management with thousands of end computing units (ECUs).

ID: SSC-R12	Incentivize the Supply Chains to accelerate adoption of trusted traceability to ensuring security, integrity and trustworthiness of IoT devices and systems
Status: Moving Forward in Principle	Issues: None identified at this meeting

- Mr. Katsioulas described this recommendation as focused on the IoT and the associated supply chain, to assure the trustworthiness of the parts being integrated into systems. He described the need for certifications of steps and workflows linked with identifiers, and he acknowledged that achieving this would require both protecting manufacturers' data and allowing them to monetize it.

ID: SSC-R13	Promote traceable and trusted IoT network ecosystems made of devices, systems, networks, and personas operating in connected IoT environments
Status: Moving Forward in Principle	Issues: None identified at this meeting

- Mr. Katsioulas explained that this recommendation was moving from devices to the network. He noted the variety of networks of various types that could be involved. He summarized the potential for successful intrusion and subsequent damage as the motivation for building a trusted environment, saying the environment was foundational for security and data sharing analytics.
- He said that the barriers for this recommendation are a bit different than the preceding ones, including upgrading of legacy systems and the lack of interoperability and security in existing systems.
- He stated that the FCC role in regulating communications would be "foundational" for this recommendation.

ID: SSC-R14	Accelerate evolution of trusted digital threads across value chains by incentivizing companies to digitalize their workflows and link their data IDs to marketplaces
Status: Moving Forward in Principle	Issues: None identified at this meeting

- Mr. Katsioulas stated that the digital thread was an essential requirement, regardless of value chain being considered, and noted he used the term "value chain" in relation to seeing the value that can be derived as an incentive. He noted that many companies have digitalized business workflows (e.g., for human resources), but few fewer have done so engineering design and manufacturing workflows. He said the digital thread can both fuel economic activity and provide more security and emphasized the important of public/private partnerships for this recommendation.
    - Mr. Chan stated that he believed change resistance is a huge issue for this recommendation, where the cost could be crushing for small businesses, and larger companies that have already adopted very expensive systems will be reluctant to change over. He asked Mr. Katsioulas thoughts regarding incentives for this recommendation.
- Mr. Katsioulas replied that there is both a need for incentives, with subsidies, as well as promotion of the value of digitalization, and the economic benefits a business could realize once they become eligible to join data marketplaces and monetize their data.

ID: SSC-R15	Incentivize the creation of trusted data marketplaces where data producers and consumers share information about data enabling data exchange and monetization while protecting proprietary Intellectual Property
Status: Being reworked. Further consideration necessary.	• Issues: There were concerns regarding the government's role in establishing marketplaces and concerns over the aggregation of anonymized PII in such marketplaces

- Mr. Katsioulas explained that the creation of the digital thread of information enables companies to enter a data marketplace by publishing metadata identifiers. He described this as an area where the U.S. could establish leadership by creating such a trusted marketplace that nations would want to join.
- Mr. Katsioulas noted some differences in barriers for this recommendation, pointing in particular to the challenge of educating companies about how their data is kept proprietary. He said he was working with Ms. Reynolds on the privacy implications, including international implications.
- Mr. Bergman expressed several concerns: Data marketplaces should grow organically rather than be created by the government. He noted there are companies in this space already. Current data marketplaces are doing a lot of aggregation of anonymized PII.
- Mr. Katsioulas replied that he believes the government's role is enablement and establishing market preferences.
- Ms. Reynolds stated she was happy to work on the privacy and confidentiality aspects. She said that many countries have started data marketplaces, often under the label of "open data" or "open government data", so the recommendation isn't a new idea.
- Mr. Chan noted that another tool available to the government to drive changes is procurement, which he described as a "powerful way of driving action and compliance".
- Ms. Megas agreed with Mr. Chan about the power of procurement and noted that an important precursor to being in procurement is having the right standards. She noted Ms. Reynolds comment about implementation in other countries and encouraged inclusion of that information in the report, saying it was important to identify places the U.S. should be engaging.

ID: SSC-R16	Fund digitalization of key business functions of enterprises in the IoT value chain for better visibility and ability to track products, monitor use, fix defects, and offer services
Status: Moving Forward in Principle	Issues: None identified at this meeting

- This recommendation is intended to address the costs of digitalization, especially for small business.

ID: SSC-R17	Promote creation and orchestration of trusted value chains made of entities, manufacturers, and service providers, that collaborate and drive trust and accountability
Status: Moving Forward in Principle	Issues: None identified at this meeting

- This recommendation connects to SSC-R16 and addresses the need to orchestrate the implementation of value chains, since random implementation doesn't lead to a connected value chain. To achieve value relationships among participants in the smart supply chain must be trackable.

ID: SSC-R18	Subsidize orchestrated Public-Private Partnerships working in parallel to speed adoption of traceability with consistent workflow & hand-off methods
Status: Moving Forward in Principle	Issues: None identified at this meeting

- This recommendation connects to SSC-R16 and SSC-R17. PPPs can be a vehicle for illustrating the value that can be realized from supply chain traceability.

ID: SSC-R19	Establish data policies that drive economic growth via frameworks that facilitates Data Monetization Security, Privacy, Data Sharing, Ownership, Control, Licensing etc.
Status: Moving Forward in Principle	Issues: More input is needed on the privacy implication of this recommendation and Ms. Reynolds and the privacy subgroup's input is sought.

ID: SSC-R20	Facilitate the Creation of Data-driven business ecosystems by raising awareness about the *New Gold* through mechanisms such as trusted data marketplaces, monetization strategies, platforms that maximize network effects
Status: Moving Forward in Principle	Issues: None identified at this meeting

- This recommendation connects the preceding recommendations regarding implementation and policy to use those elements to realize the desired value of the smart supply chain and its traceability capabilities.

ID: SSC-R21	Evaluate opportunities, risks and regulations for using AI to accelerate supply chain security and resilience, or prevent bad actors from tampering
Status: Being reworked. Further consideration necessary.	Issues: More information is needed on the implications of AI in the supply chain before the recommendation can be fully formulated.

- This recommendation is still under development. AI is rapidly evolving and potentially disruptive and should be considered both as a potential accelerator and as a risk.

Smart Traffic and Transportation Subgroup Discussion

Smart Traffic and Transit Technologies team members: Nicole Coughlin, Benson Chan, Steve Griffith, Kevin Kornegay, Debbie Reynolds.

Mr. Griffith presented the smart traffic and transit technologies recommendations.

Slide deck: Smart Traffic & Transit Technologies

Draft text of recommendations: Smart Transportation & Transit Technologies Recommendations

Smart Traffic and Transportation Background

Five recommendations carried forward from April meeting with updates, one recommendation (regarding drones) was new for this meeting.

Smart Traffic and Transportation Recommendations

ID: STT-R01	The federal government should facilitate/support the development 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.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- Smart traffic and transportation IoT will generate a broad variety of data. This data can be leveraged for many benefits but there's a need for clarity regarding retention, interoperability, and access considerations. There will also be a need for training regarding usage and retention. There needs to be coordination across jurisdictions, and probably some legislation, mostly at the state level.

ID: STT-R02	The federal government should support research and industry-led standards in areas such as telematics and sensor technologies for autonomous vehicles. These standards should be based on high-level safety guidelines determined by the National Highway Traffic Safety Administration.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- This pertains to the emerging market for autonomous vehicles, and the subgroup doesn't anticipate fully autonomous vehicles soon. An example of the concerns is distinguishing vehicles with and without drivers. Industry-developed standards can serve a foundation for subsequent development of policies and regulations.
- Research was added to this recommendation since it was discussed at the April meeting.

ID: STT-R03	The federal government should consider developing programs and grants to allow underserved and less developed communities as well as rural areas to adopt smart transportation technologies.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- Recognizes the uneven accessibility of IoT. One goal of expanded access for IoT is to provide support for private investments and job growth.

ID: STT-R04	The federal government should support 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).
Status: Moving Forward in Principle	Issues: None identified at this meeting

- Interoperability and cybersecurity are big concerns, especially across jurisdictions. There are also many start-up businesses in this market so standards can encourage innovation and reduce fragmentation.
- This recommendation could be merged with some of the other recommendations.
- Mr. Bergman suggested one approach to achieve this recommendation's goals would be to establish a profile for cybersecurity requirements, against which industry can define appropriate standards.

ID: STT-R05	The federal government should invest and promote education and workforce development in smart transportation technologies.
Status: Moving Forward in Principle	Issues: Needs a stronger outcome orientation.

- IoT education for the workforce is a broad topic, but there are some unique challenges in smart transportation, as there is a huge skills gap between traditional ("concrete and asphalt") and smart transportation engineering. Currently the civil engineers in this field do not have background in smart technologies, and the smart technology companies do not know transportation applications. Data

science and analytics associated with smart technologies requires a different skill set from traditional engineering mathematics.

- Mr. Griffith said that certain sectors of transportation have successfully used an outcomes-based approach: define the problem to solve, then let the vendor community build a solution. He suggested that outcome-based contracting in surface transportation could be a solution to the workforce gap.

ID: STT-R06	The Federal Government should provide overarching regulatory guidance for the drone industry. The Federal Government should also provide funding for the drone industry for additional research in order that existing technical obstacles can be overcome.
Status: Moving Forward in Principle	Issues: Additional research on several aspects of the drone industry is needed.

- There is a lot of conflicting legislation and regulations regarding the drone industry. There is also significant diversity, including contrasts between recreational and commercial pilots, different airspaces, remote ID, and location requirements; differences between line-of-sight and over-the-horizon operations. There seems to be uncertainty about regulatory responsibility and there are significant associated safety issues.
- Mr. Bergman stated that CTA has been involved in several topics related to this recommendation and volunteered to assist with refining it.

Closing

- The Board reviewed the agenda and made adjustments to the day 2 schedule.

Ms. Cuthill adjourned the meeting.

IoTAB Meeting on Wednesday, May 17, 2023

Ms. Cuthill opened the day's meeting and turned it over to Mr. Chan.

Mr. Chan reviewed the agenda and introduced Jeff Jockisch and Colby Scullion

Public Speakers – Jeff Jockisch (Avantis Privacy), Colby Scullion (Avantis Privacy)

Mr. Jockisch and Mr. Scullion presented on location data privacy.

Slide deck: Avantis Presentation (slides)
Speaker Notes: Avantis Presentation (speaker notes)

- Ms. Reynolds introduced the speaker: Mr. Jeff Jockisch. She invited Mr. Jockisch and Mr. Scullion to address the IoTAB based on their experience around third-party data collection and location data. She described third party data collection as a barrier to adoption of IoT devices and said there is a need to find ways to make sure that this data collection is a benefit to the individuals.
- Mr. Jockisch is Chief Privacy Officer at Avantis Privacy. His primary role is as a data privacy researcher investigating data brokers. Mr. Scullion is CEO of Avantis Privacy.
- Mr. Jockisch shared the history of Amy Boyer, who was killed in 1999 by a stalker that obtained information about her from a data broker. Mr. Jockisch stated location privacy has gotten worse since 1999, reporting that a 2019 investigation found that AT&T, T-Mobile, Sprint, and Verizon are selling customer's location data to data brokers.
- Mr. Scullion explained how our phones leak location data, much of which feeds into the advertising ecosystem. There are also other sources of location data such as onboard GPS and Wi-Fi in automobiles, and automated license plate readers deployed across the nation.
- The Mobile Advertising ID (MAID) is the easiest way for advertisers to connect you to your location data. Mr. Scullion described MAID as "like a SSN that you didn't know you had", and said advertisers link everything possible to your MAID.
- MAIDs track you through apps and websites. Advertisers bid to present advertisements on your phone, and bidding, whether successful or not, gives them access to location data. Some organizations deliberately underbid simply to acquire data to build profiles.
- Mobile phone users can delete their MAID, but research shows most users don't: Only 2% of Android users have disabled their MAID, and about 25% of Apple devices users have opted in to allowing MAID access by favorite apps.
- Avantis has identified 124 location data brokers, who aggregate location data based on MAID. Mr. Jockisch explained that the location brokers' claim that your data is anonymous isn't accurate, saying 95% of Americans can be uniquely identified from only four location coordinates (i.e., latitude, longitude). He added that some data brokers advertise that they have already matched your 'anonymous' MAID to your personal data and will provide that information for a fee.
- Mr. Jockisch described this lack of location privacy as invasive and dangerous, with a meaningful risk to physical safety. He characterizes particular groups at greatest risk: people concerned with reproductive health, victims of domestic violence, military personnel (especially with regard to operational locations), law enforcement, U.S. court system, and company executives.
- Mr. Jockisch concluded by asking 'Should location data about these people be for sale? Should location data about anyone be for sale? Are marginally better ads worth the risk to physical safety?'

Group Discussion

- Mr. Chan: When Apple switched to iOS 14 didn't, they change the privacy landscape between apps?
    - Mr. Scullion: They did, significantly. Previously apps were able to pull the MAID from a device. Now app access to MAID is at the consent of the user. The problem is that once Apple introduced the new privacy settings, some apps requested the right to track you. They put their own text in the prompt with the benefits of doing this. As soon as Apple rolled that update out, most people did not have their MAID available to apps. Now more than 25% of users have their MAID completely exposed to any app that wants to access it.
    - Mr. Jockisch: MAID is the global identifier. Apple only allows apps that you give permission to. Once it's on, it's more globally exposed than they let on.
- Ms. Reynolds: We know IoT likely needs location to function. But the question is where does it go once it's collected? What do they do with the data?
    - Mr. Jockisch: If you turn that MAID on, it can go to twenty different location data brokers, and they can accumulate a history. If you turn it off the location data history doesn't go away. It is particularly insidious on the Android. When the MAID is turned off it is deleted. If you turn it back on, it generates a new MAID. You don't know what the old one was unless you recorded it, leaving the user unable to request deletion of data associated with the previous MAID.
- Mr. Chan: It can't necessarily identify you because you have a new MAID. Doesn't that make it harder to correlate?
    - Mr. Scullion: It doesn't take long for apps to share your information through dozens of channels which will quickly build a profile. Even if it was previously shielded, it can still be paired up to that MAID because it was exposed at one point.
    - Mr. Jockisch: MAID is just a string of numbers. It is possible to figure it out whose it is with a little bit of research and the right tools.
- Mr. Chan: What about Wi-Fi systems in a shopping mall that track movement, for example - are those applications safe? Are they keeping data to themselves and not selling?
    - Mr. Scullion: Location tracking by Wi-Fi doesn't have to be a Wi-Fi network that you connect to. It can be a large network (WPS) of Wi-Fi access points. If you are inside a building, the GPS can only locate you to a 50-foot circle; they'll use a WPS network to pin you down a little closer (and Bluetooth beacons as well).
    - Mr. Jockisch: This location data is associated with a machine ID, rather than your MAID, but it's still possible to connect it back to a user.
    - Mr. Scullion: There are business models being built to take "seemingly obscure" data that doesn't mean anything and then pair them together to build a bigger profile for someone. This process is much more efficient today with machine learning technologies.

Public Speaker – Harvey Reed (MITRE)

Mr. Reed presented on mechanisms for supply chain traceability.

Slide deck: Manufacturing Supply Chain Traceability

Mr. Don Davidson introduced Mr. Harvey Reed (standing in for Mr. Katsioulas).

- Mr. Davidson: As we continue to talk about traceability identifier synchronization, digital threads, data producers, consumers and value chains, Mr. Reed will explain how to link them all together with blockchain and distributed ledger technologies based on methods and sequential transactions. The methods explained by Mr. Reed can enable end-to-end provenance and traceability during the supply chain journey and during operational use.
- Mr. Reed stated he is on the technical staff of MITRE, working on a project called Manufacturing Supply Chain Traceability, which is a follow-on to an earlier effort. Mr. Reed encouraged feedback on the project definition, via the official comment form[2] and process. He stated that he is not speaking for his role at the NCCoE at NIST.
- The focus of the project is Supply Chain Traceability, applicable to any manufacturing supply chain and the assets flowing within it, although the project is specifically taking a "deep dive approach" looking at critical infrastructure, smart infrastructure, microelectronics, and software. The approach applies to many domains including IoT and the goal of the project is producing a Minimum Viable Product (MVP) implementation with the "bare essentials" to demonstrate applicability.
- Mr. Reed identified two primary challenges, which he related to language in NIST IR 8419[3] about applying an "ecosystem perspective" to supply chain traceability to complement a "per acquirer" view:
    - Challenge#1:
        - Which acquirers have stringent traceability requirements?
        - Who drives the traceability requirements?
    - Challenge#2
        - With current per acquirer perspective: how to trace through tiers?
        - How are supply chains illuminated?'
- He noted that some of the parties driving requirements could be in the middle of the supply chain.
- Mr. Reed described the approach as a scheme based on writing records to ledgers to gain their immutability properties and the ability to trace back. He noted that the endpoint of the traceability process isn't where a product is manufactured but how it is used in critical infrastructure. He raised the possibility of linking repositories of operational data and emphasized the importance of the "Employ" record, which links the supply chain activities for producing an item to its use in operation. He cited tracking automatic software updates to self-driving cars as another example where traceability is important.
- Mr. Reed explained the traceability chain is composed of traceability records of various types, and each record when written is linked to the previous one. The different record types captured in a ledger cover manufacturing, distribution, retailing, and operations. He used the example of Mediledger, a pharmaceutical industry effort to respond to an FDA requirement to track sensitive pharmaceuticals at the individual pill level, rather than at the lot level. Mediledger is a group formed by pharmaceutical companies collecting enough information to track reverse logistics; this implementation helps illustrate the applicability to many types of goods. One benefit of reverse logistics tracking is the ability for a retailer to return excess supply while maintaining tracking. The traceability chain is written as the supply chain progresses and can be read back by an end customer for validation.

[2] https://www.nccoe.nist.gov/projects/manufacturing-supply-chain-traceability-using-blockchain-related-technologies -- comments were accepted through May 25, 2023.
[3] NISTIR 8419 - *Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability: Needs and Industry Perspectives*, https://csrc.nist.gov/publications/detail/nistir/8419/final

- Mr. Reed described the traceability chain workflow, which includes all manufacturing steps, transportation steps, and end customer use, plus connections to other systems. The blockchain ledger is storing IDs and pointers to other repositories with complete information. Mr. Reed walked through the steps of the supply chain and the types of information captured in each record type to illustrate the concept in operation. He noted that transportation and logistics firms often have their own ledger tracking.
- Mr. Reed said this concept establishes a durable traceability chain that survives the lifecycles of the companies involved. If a company goes out of business, they still have a summary record in the ledger. He noted the importance of having industry groups operating their ledgers (Mediledger is an example) and stated the use of ledgers is not a new thing. If these ledgers can be linked, then there is greater value to the supply chain and the operational customers.

Group Discussion

- Mr. Katsioulas described the approach Mr. Reed presented as "prescriptive", but that the important aspect is for organizations to follow a consistent methodology with regard to inputs, outputs, and "connecting the dots" in the digital thread. This requires the identifiers, orchestration, and inputs/outputs in the ecosystem that participate in that digital thread. This approach creates a horizontal and vertical infrastructure to support developing applications based on the digital thread data, such as monitoring or analytics.
- Mr. Katsioulas emphasized the digital thread includes both the supply chain and events that occur after device on-boarding, such as the ability to record data about device updates and other events that could involve intruders
- Mr. Tseronis noted the importance of this topic related to "smart connected things".
    - Mr. Reed: There is a preceding project, with a published paper (NIST IR 8419) done with full participation from industry. Mr. Reed emphasized input from industry groups as necessary to be "grounded in reality". The current effort is pursuing one research topics from the first project, after recognizing that industry was coordinating with ledgers and so looked into traceability and ability to coordinate among ledgers.
- Mr. Griffith agreed that blockchain has potential when we talk about supply chain and asked what is holding back ledger and traceability from mainstream adoption?
    - Mr. Reed described the challenge as getting beyond the perceived constraints of industry groups, which are accustomed to talking internally but much less so across groups. Persuading industry groups to allow linking between ledgers is needed.
    - In terms of technology adoption, the talent pools exist to implement projects with ledgers, allowing every group to form and use any ledger they want. The project is exploring the possibility of creating a very simple API (akin to HTTP) to permit moving among different ledgers to complete tracing. He described this as "a heavy lift", but not insurmountable, and that getting groups talking would be a "transformative step".
    - Mr. Bergman viewed the challenge as a "chicken and egg situation", where a customer can require traceability and gain compliance from their immediate vendors, but there won't be compatibility at deeper layers of the supply chain.
- Mr. Bergman described this traceability approach as a security solution and noted security solutions are applied appropriate to a risk analysis, where an organization will purchase a security solution appropriate to the risk. He stated supply chain traceability is a challenge in mixed risk appetites, where

the risk environment isn't easily matched to the components being tracked, such as one microcontroller that could go into a relatively benign environment or a highly secure environment.

  - Mr. Reed agreed and suggested focusing on the incentives for an organization to participate, where the marketplace, including customers, could foster and drive incentives appropriately to suppliers who might be in that mixed mode.
  - Mr. Bergman stated the incentives should be tailored to address the desired outcome compared to the risk environment, not the solution (traceability) or the implementation (blockchain). The incentives have to go back to what we are trying to accomplish with supply chain risk management.
  - Mr. Katsioulas stated a need to work on the incentives in the marketplace and suggested that the incentive is not just risk management but also the economic value, which would encourage adoption.
  - Mr. Reed agreed, noting that that is the role of the "Employ" record, capturing how the product is fielded and the potential linkage to operational data. This would be an economic driver of its own.
  - Mr. Katsioulas noted this extends into international connections, with blockchains capture data across borders.
  - Mr. Reed agreed noting that the walled garden approach is useful when the parties have aligned values. The strength and integrity of the data layer become more important once you include stakeholders who are not aligned with your values.

- Mr. Katsioulas suggested looking at the Gaia-X (EU) and Catena-X (automotive) projects, saying they are looking at ways to create data sovereignty and address the international issues associated with the data market.

Healthcare Subgroup Discussion

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

Ms. Mehra and Ms. Rerecich presented the healthcare recommendations.

Slide deck: Healthcare Subgroup

Healthcare Recommendations

ID: HCR-R01	Make IoMT equivalent in priority for all healthcare stakeholders as is IT infrastructure, cybersecurity posture, or applications. Recommend the notion of a Chief IOT Officer and a Federal program office to manage IOTs.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: More research needs to be done on how establishing a Federal Chief IoT Officer would transfer to the desired outcome in healthcare organizations

- Questions were raised about the connection between a Federal Chief IoT Officer and a corresponding response of medical organizations to raise the profile of IoMT.
- Clearer justification is needed for the recommendation of a C-Suite role. If this recommendation is retained the Board should consider if it should apply to other industries. There may be a unique need within healthcare due to IoMT devices.

- There are significant differences between the role of a federal officer (regulations) and that of a C-Suite position (risk & compliance), and the federal officer role would be much broader than healthcare unless specifically created in a department like Health & Human Services.
- Need to reconcile the slide title (which refers to "facilities") with the recommendation language ("healthcare stakeholders"), and clarify what facilities are included in the scope of the recommendation.

ID: HCR-R02	Promote and, if necessary, develop a protocol for data exchange standards for IoMT for interoperability, and promote the adoption of these standards.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: Recommendation should focus on data interoperability as a goal, rather than data exchange standards as the means to that goal

- The intent is that having a data exchange standard could create efficiencies between equipment, safety benefits; those could make it easier to move to different manufacturer's equipment; many relevant stakeholders; the goal is to promote IoMT adoption.
- The goal can be better stated as better interoperability for IoMT (device-to-device; device-to-application), making allowance for conversation between proprietary formats as a solution

ID: HCR-R03	Enact HIPAA-like protection for users' medical data in mobile applications and IoT devices. Consider medical data as a category for defined data protections.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: Need to clarify the scope of applicability and examine the potential for unintended consequences.

- Consumer grade IoT devices and mobile apps collect lots of medical and PHI data, which is not protected like medical data in doctor's offices, although consumers expect it is. The recommendation is this data should be protected similarly to data that would exist in a doctor's records, including prohibitions against the sale of data.
- Mr. Bergman requested the opportunity to consult with specialists, saying there is a need to better understand the unintended consequences from a wide-ranging recommendation.
- Greater clarity is needed on the scope of devices, software, and data that would be covered by the recommended extended protection.
- There is a potential impact on medical manufacturer's business models by blocking current monetization options. There could also be access impacts for economically disadvantaged consumers.
- HIPAA isn't primarily a privacy law and has not received been updated as the technology in the healthcare sector has evolved.
- There is potential to achieve the goals through voluntary guidelines.

Public Safety Subgroup Discussion

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

Ms. Mehra presented the public safety recommendations.

Slide deck: Public Safety Recommendations

Public Safety Recommendations

ID: PSF-R01	Promote Interoperability of Public Safety IoT Data. Advocate for the implementation and adoption of interoperable data standards for public safety IoT.
Status: Moving Forward in Principle	Issues: The recommendation needs clarity on the scope of devices to be addressed. More broadly every Board recommendation may need clauses to clarify included and excluded scope; this is a topic for the chairs to address.

- The focus is achieving interoperability of public safety IoT devices for efficiencies and improved safety. The justification is enhanced incident response and coordination among responders.
- Need a recommendation to develop an assessable standard for specific categories of public safety IoT.
- Consideration should be given regarding what connections between fixed (e.g., building safety systems) and mobile (e.g., first responder communications) are needed and whether they are in-scope for this recommendation or should be addressed in the development of a new recommendation.

ID: PSF-R02	Incentivize Budget Prioritization for Public Safety IoT. Create a stockpile of public safety IOT devices that are finite in type and need but contains a medley of manufacturers to choose from rather than a single or a couple of manufacturers from which stockpiles are sourced. Refresh the stockpile per labeling requirements and best use-by date.
Status: Moving Forward in Principle	Issues: None identified at this meeting

- This recommendation is modeled on what we do when we stockpile vaccines, PPE, other "must-have" government-managed devices ready to deploy at a moment's notice for disasters, etc.
- Have some methodology around refreshing the device stockpile to respond to the speed of technological development. If accepted, the notion of stockpile for IoT devices will open the conversation for interoperability, which could be a threshold for being included in the stockpile.

Privacy Subgroup Discussion

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

Ms. Reynolds presented the privacy recommendations.

Slide deck: Privacy Subteam

Draft text of recommendations: Privacy Recommendations

Privacy Background

- Six recommendations have been refined from April and two new recommendation added.
- Refinement has been to better apply mechanisms available to government.

Privacy Recommendations

ID: PRV-R01	Advocate for the simplification of privacy policies, privacy notices, and data use policies to enhance accessibility and comprehension for users.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: Still too high level to be actionable; need clearer description of appropriate government actions

- Essentially unchanged since April, with the addition of one barrier and a broad list of federal considerations that could be applied.
- Recommendation is still very high level, needs to be refined to be "succinct yet actionable"; need specifics are behind these high-level federal considerations.
- The E-Government Act of 2002[4] should be considered as a potential framework. Should also examine the IoT Cybersecurity Improvement Act of 2000[5], which is in the implementation phase at OMB.

ID: PRV-R02	Create a set of "data use" basics that must be included in privacy policies for IoT devices
Status: Moving Forward in Principle	Issues: None identified at this meeting

- Unchanged from April, except for the addition of federal considerations; this could be part of a framework or be added to an existing framework.

ID: PRV-R03	Analyze and learn from existing privacy regulations, such as the California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR), and others
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: Unclear focus, may be multiple recommendations combined

- Only implementation barriers updated; added same federal considerations list as other privacy recommendations.
- Creating a framework may be an approach to this, or it could be a separate recommendation.

[4] https://www.justice.gov/opcl/e-government-act-2002
[5] https://www.congress.gov/bill/116th-congress/house-bill/1668

ID: PRV-R04	Develop a National Privacy Framework for Innovation and Data Protection specifically tailored to the unique challenges posed by IoT devices
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: The exact purpose and scope of the framework need to be clarified; legislative action in this area is exceedingly difficult.

- Goal is to increase confidence in IoT and highlight gaps that aren't addressed in other frameworks. Frameworks can be a resource across industries.
- This framework should be the top-level vehicle for any legislative consideration in our recommendations with regard to privacy; in digital health we have some recommendations that should reference this framework (rather than be standalone).
- Should also draw distinctions between this framework (policy-oriented, guiding legislative and agency actions) and the NIST privacy framework which is different entirely (privacy engineering); this is a top-level vehicle for any legislation that has to do with data privacy. This remains as possibly the most difficult recommendation related to privacy.
- This recommendation is oriented toward consumer privacy, not corporate confidentiality.
- Clarity is still needed whether corporate privacy for proprietary data and data governance issues are within the scope of the privacy subgroup.

ID: PRV-R05	Develop and implement a comprehensive US Federal Privacy Regulation that addresses data privacy concerns for IoT devices and services
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: Intended outcome of recommendation is unclear; need to define IoT-specific recommendations (beyond current proposed legislation)

- The proposed ADPPA (American Data Privacy and Protection Act) is a starting point for the recommendation. The Federal Privacy Regulation should be a baseline to create harmonization of terminology, not a ceiling. Implementation would require supporting legislation and regulations. The approach should include identifying and filling gaps in existing legislation and policies.
- The discussion focused on the recommendation being high-level, not adequately IoT-specific, and the general difficulties of implementing Federal privacy policies.
- It was noted that some aspects of this could be accomplished through executive branch action, but others would require legislative action.

ID: PRV-R06	Develop and implement a privacy label system for IoT devices, similar to nutrition labels on food products (similar to the White House initiative for cybersecurity labeling)
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: Recommending a specific implementation rather than an outcome;

- There is a concern that the IoT cybersecurity label doesn't provide any distinction between cybersecurity and privacy, but consumers need to be informed about both. The recommendation isn't specifically calling for a separate IoT privacy label.
- As currently envisioned, a national IoT cybersecurity label addresses some privacy issues but not the full scope of the privacy subgroup's concerns. International compatibility and mutual recognition concerns may force expansion of the privacy considerations for the label.
- There was a suggestion to focus on the outcome: "improve transparency of privacy considerations in IoT products by leveraging the cybersecurity label program either as a new label or adjunct to existing criteria in the cybersecurity label"; look for ways to improve transparency for consumers through the existing structure.

ID: PRV-R07	Formulate clear and robust policies regarding data sharing and data usage involving third parties in the IoT ecosystem
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: Scope, source, and meaning of "policies" is unclear with regard to the intended outcome; unclear whether recommending regulation and enforcement

- Could potentially be combined with PRV-02. The critical point is establishing clear policy. Goal is to create more transparency around how IoT data is accessible to third parties.
- It was suggested that the recommendation statement misaligned with intended outcomes; if proposing modifications to regulations need to be specific about what regulations and the desired outcomes from modifications.

ID: PRV-R08	Develop educational initiatives that focus on IoT, targeting workforce development and enhancing consumer privacy and trust
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: This recommendation lacks sufficient detail and is too high-level; needs to address the complete lifecycle of IoT devices;

Environmental Monitoring Subgroup Discussion

Environmental Monitoring team members: Arman Shehabi, Ranveer Chandra, Nicholas Emanuel, Mike Bergman, Benson Chan.

Dr. Shehabi presented the environmental monitoring recommendations

Slide deck: Environmental Monitoring Sub Working Group

Draft text of recommendations: Environmental Monitoring Recommendations

Environmental Monitoring Background

- IoT's potential to expanded environmental monitoring brings three significant potential changes:
  - Collection: The opportunity to collect a lot more data
  - Distribution: The ability to distribute environmental monitoring sensors widely
  - Post-processing: Improved opportunity to identify trends through analysis of expanded data sets
- There will be additional recommendations from this subgroup

Environmental Monitoring Recommendations

ID: ENV-R01	Facilitate and support the research, development and deployment of low-cost air quality monitoring sensing systems
Status: Proceeding forward in principle	Issues: None identified at this meeting

- Regulatory grade environmental sensors are very expensive, and therefore not widely deployed.
- IoT offers the potential to deploy a large number of relatively inexpensive sensors that can monitor a wider range of chemicals with greater geographic precisions (e.g., individual neighborhoods).
- Recommendation scope includes research for sensor development, access to calibration data, and connectivity in more rural areas.

ID: ENV-R02	Establish IoT environmental data repositories for privately collected data
Status: Proceeding forward in principle	Issues: None identified at this meeting

- Large volumes of data create opportunity for community research, especially with data from different sensor manufacturers and users. Publicly available repositories are needed and need to be prepared to handle large volumes of data that is anticipated. A common repository can help address harmonization of data from various sources.
- Privacy concerns need to be addressed, including the potential to reverse engineer proprietary information from shared data.
- The DoE's Energy Information Initiative (EIA) could be a model approach.

Precision Agriculture Subgroup Discussion

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

Dr. Chandra presented the precision agriculture recommendations.

Draft text of recommendations: Precision Agriculture Recommendations

Precision Agriculture Background

- Presented updates for three recommendations introduced in April, and introducing three new recommendations

Precision Agriculture Recommendations

ID: PRA-R01	The federal government should consider subsidizing the use of IoT in farms.
Status: Proceeding forward in principle	Issues: None identified at this meeting

- This would be similar to other subsidies available through USDA.
- Updated from initial presentation in April, incorporating feedback on implementation and barriers.

ID: PRA-R02	The federal government should consider fully funding the deployment of a "farm of the future" setup in every land grant university nationwide. This nationwide test-farm IoT network should span different forms of agriculture, including, but not limited to broadacre, horticulture, livestock, and aquaculture.
Status: Proceeding forward in principle	Issues: None identified at this meeting

- This recommendation would require substantial investment but should lead to better decision making.
- This recommendation would need to define the IoT-specific applications

ID: PRA-R03	The federal government should consider increasing funding and accelerating implementation of broadband deployment across rural America.
Status: Proceeding forward in principle	Issues: None identified at this meeting

- Reports are that 60% of U.S. farmland doesn't have good Internet connectivity. The US needs coverage across rural areas, especially farmland; funding is currently divided over several programs
- This recommendation may require funding energy sources as well.

ID: PRA-R04	The federal government should actively promote and support the adoption of satellite narrowband IoT systems for agricultural IoT, with the aim of improving connectivity, data collection, and decision-making in rural and remote agricultural areas.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: Government doesn't usually play a role in harmonizing standards; possibly should be broader than satellite communications;

- Satellite communications can complement LoRa for agricultural IoT for narrowband communications needs and could offer very low-cost connectivity
- There is an opportunity to harmonize the standards for satellite communications and improve interoperability

ID: PRA-R05	The federal government should actively promote and support the adoption of Generative AI applications for agricultural IoT, with the aim of improving decision-making, optimizing resource utilization, and enhancing productivity in the agricultural sector through innovative and data-driven solutions.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: Concerns regarding privacy, maturity of the AI technology; premature for government to "promote" use of this technology

- This could apply to other subgroups as well
- This recommendation needs to address privacy considerations around the training data use for large language model AI systems

ID: PRA-R06	Develop a comprehensive national strategy for agricultural IoT to establish a clear vision and roadmap for the integration of IoT in agriculture, addressing current challenges, fostering innovation, and promoting long-term sustainability and competitiveness of the agricultural sector.
Status: This recommendation is being reworked. Further consideration is necessary.	Issues: This recommendation needs refinement. While it is too generic, it could perhaps be combined with similar recommendations from other subgroups;

- This recommendation is modeled on the strategy for climate-smart agriculture.
- An example of a possible benefit is improving dynamic soil maps: existing soil maps aren't up to date; not useful for decision making; would like to integrate physical / chemical / biological data about soils;

Cybersecurity Subgroup Discussion

Cybersecurity team members: Mike Bergman, Ranveer Chandra, Steve Griffith, Tom Katsioulas, Kevin Kornegay, Pete Tseronis.

Mr. Bergman presented the cybersecurity recommendations.

Slide deck: Cybersecurity Subgroup

Draft text of recommendations: Draft Cybersecurity Recommendations

Cybersecurity Background

- Presenting updates for four recommendations introduced in April, and introducing one new recommendation
- Updates to recommendations CBY-R01, -R02, and –R04 are to make them more specific to product certification programs.
- The subgroup expects to present additional recommendation at future meetings

Cybersecurity Recommendations

ID: CYB-R01	Engage with Industry on IoT Product Certification Programs. Prioritize broad and active industry engagement when developing and maintaining the government-sponsored portion of the U.S. national cybersecurity label for connected devices.
Status: Proceeding forward in principle	Issues: None identified at this meeting

- Justification expanded to account for the impending launch of the consumer IoT cybersecurity labeling program

ID: CYB-R02	Keep IoT Product Certification Programs Voluntary. Conformance to any specific set of requirements should be voluntary.
Status: Proceeding forward in principle	Issues: None identified at this meeting

ID: CYB-R03	The federal government should continue to support NIST as the developer of outcome-based requirements that inform industry consensus standards, and industry as the developer of those standards.
Status: Proceeding forward in principle	Issues: None identified at this meeting

ID: CYB-R04	Create Further Incentives for IoT Product Certification Programs. The Administration should encourage Congressional support to deploy this program, including establishing incentives for manufacturers to participate.
Status: Proceeding forward in principle	Issues: None identified at this meeting

ID: CYB-R05	The federal government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems
Status: Proceeding forward in principle	Issues: None identified at this meeting

- There is an opportunity for the federal government to lead by example and provide credibility and assurance for IoT for the private sector
- Upgrading security could potential save on cybersecurity insurance premiums.

Overall Recommendations Feedback and Next Steps

- Mr. Witte stated that the material from this meeting would support drafting the report for review at the July meeting, and that he would work with the subgroups to solicit more detail to make recommendations actionable.
- Ms. Cuthill emphasized the need to provide Mr. Witte input so that the draft report can be circulated enough ahead of the July meeting to permit member review before and Board-level decisions at that meeting.
- The IoTFWG will have opportunity to review the draft recommendations from this meeting and may identify areas for additional IoTAB attention.
- There was a suggestion that having a complete draft of one section could make it easier for the IoTAB members to have a better sense of where and how to contribute and better place recommendations in context.

Action Items and Wrap-up

Mr. Chan, Chair

- Mr. Chan listed nine action items from this meeting:

Action	Who	When
Mr. Bergman to send email re: Consumer, Smart Home Regulation, Standards, Personas: Add as commentary sections to report	Mr. Witte – add report sections	May 31
Skills, education, workforce recommendations: each subgroup send recommend to Mr. Chan	All Mr. Witte – add section	May 31
User Protection and Agency Coordination: add as commentary sections to report	Mr. Witte	May 31
Update recommendations for those not advanced	All	June 15

Action	Who	When
Update recommendations/wording for those that are advanced (and require it)	All	June 15
Define Smart Cities and IoT	Ms. Coughlin	May 31
Consider adding section and commentary on AI as section in report, per Ms. Megas suggestion	Mr. Witte – add section	May 31
Consolidate supply chain international collaboration into International Engagement subgroup	Mr. Katsioulas Mr. Caprio	May 31
Add commentary on linkage between data, IoT systems, digital twins, vision, benefits, how does IoT enable	Mr. Witte – add section	May 31

- There are several actions related to commentary sections in the report
  - Subgroups should contribute material for those sections as it arises in their subgroup work.
  - Ms. Reynolds has already drafted a section on personas
- Ms. Megas suggested that the Board should consider a discussion of the connections among IoT, AI, and digital twins, as a topic where the expertise of the Board could be looking to the future potential for IoT.
- There was general agreement to complete action items within two weeks.
- Mr. Witte stated that the target date for the draft report was 30 June, and that updated recommendations are needed by mid-June to support that target.

Closing

Ms. Cuthill adjourned the meeting.

Additional Information for Reuse

The table below helps to visualize the 16 subgroups as they align to the 7 mandated topics in legislation.

Charter Element		Current Subgroups (as of April 2023 meeting)
i. smart traffic and transit technologies;	*maps to*	Smart Traffic and Transit Technologies
ii. augmented logistics and supply chains;	*maps to*	Augmented Logistics and Smart Supply Chains
iii. sustainable infrastructure;	*maps to*	Sustainable and Critical Infrastructure
iv. precision agriculture;	*maps to*	Precision Agriculture
v. environmental monitoring;	*maps to*	Environmental Monitoring
vi. public safety; and	*maps to*	Public Safety
vii. health care;	*maps to*	Healthcare
Spectrum	*not handled yet*	
Policies	*maps to*	Policies
Privacy	*maps to*	Privacy/Data Ownership
Security, including critical infrastructure	*maps to*	Security
user protection	*not handled yet*	
agency coordination	*not handled yet*	
small businesses	*not handled yet*	
International	*maps to*	International Engagement
		Other (Planned) Subgroups
		Consumer
		Regulations & Commerce (prune or move to Policies)
		Skills, Education, Workforce Development (assemble from subgroup contributions)
		Smart Homes
		Standards