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)

April 18 & 19, 2023

Virtual Meeting Platform: Webex

MEETING MINUTES

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

Speakers:

- **Andrea Amico**, Privacy4Cars
- **Jon Boulos**, Wisconsin IoT Council
- **Don Davidson**, Synopsys
- **Angela Fernandez**, GS1 US
- **Mobeen Kahn**, formerly AT&T
- **Steven Kelly**, National Security Council, The White House
- **Eric Simone**, Clearblade
- **Angela Smith,** NIST Supply Chain
- **Joe Weiss**, Applied Control Solutions, LLC

Action Items Over Both Days

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

General:

- All presentations can be found on the NIST website.
- Read the original DIGIT act to better understand the intent of Congress.
- IoTAB subgroups must indicate any proposed speakers for upcoming meetings to Co-Chairs, Mr. Chan, and Mr. Caprio

Report Discussion:

- **All IoTAB members** - The IoTAB must continue to draft content in agreement with the presented IoTAB outline (as agreed upon in the March meeting).
- **Mr. Chan –** Looking to determine how to address "cross-pollination" over multiple subgroups.
- **Mr. Chan** – Following up on a request by Ms. Mehra to examine updating the report template to reflect where federal agencies are in implementing IoTAB recommendations to-date (to illustrate existing activities vs. "net-new" recommendations).
- **All IoTAB Subgroups** - Complete recommendations at the earliest.
    - Recommendations are needed for the May meeting and need to be finalized by the July meeting.
    - As noted in the April meeting, if a subgroup can't complete the template for a particular recommendation, then it probably isn't worth pursuing.

IoTAB Sub-groups:

- **Mr. Chan / Infrastructure Subgroup** –
    - Split sustainable infrastructure into smart cities and sustainability.
    - Determine what the scope of sustainable infrastructure needs to be in the IoTAB report as called out in the legislation and in relation to critical infrastructure.

Schedule:

- Review the draft IoTAB timeline that was discussed during the meeting.
- As discussed in this March and April meeting – the IoTAB is looking at a one-year timeline:
    - 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.

Administrative:

- **Mr. Chan** - Confirm July meeting dates.
- **Mr. Chan** - Confirm board members' September meeting date availability by email.
- **Mr. Bergman** - Offered that CTA could host a hybrid meeting in Arlington, VA, however he needs to confirm their ability to accommodate public attendees.

The record also reflects requests made by IoTAB Members following speaker presentations:

- Following Mr. Weis' presentation, Mr. Katsioulas requested Mr. Weis provide a summary of the main barriers to adoption and an expanded discussion of his recommendations.
- Following Mr. Boulos' presentation, Ms. Reynolds requested more discussion on education / training for all ages.

IoTAB Meeting on Tuesday, April 18, 2023

Welcome and Agenda Review

Ms. Cuthill welcomed the attendees and opened the meeting. She indicated there would be on audience interaction and introduced the chair, Mr. Benson Chan.

Mr. Chan, Chair

Mr. Chan shared the agenda which can be found on the NIST website here: Agenda Discussion Slides

- 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 teams, insights from external speakers, plans for May meetings, and dates for future meetings.

Speaker - Jon Boulos, Wisconsin IoT Council – Manufacturers Perspectives on Barriers to IoT Adoption

Mr. Jon Boulos, Wisconsin IoT Council

Mr. Boulos shared slides which can be found on the NIST website here: Removing Barriers to IoT Adoption.

- Mr. Boulos leads technical strategy for digital products at Kimberly Clark, a major manufacturer.
- He serves on the board of directors of the Wisconsin IoT council which is a public/private partnership with deep roots in manufacturing.
- He identified that IoT is used to facilitate manufacturing and views IoT as both a core concept in manufacturing, as well as market opportunity.
- Wisconsin IoT Council members have identified key barriers and opportunities to IoT adoption:
  - the landscape, which is overly complex and expensive,
  - the need for clear and consistent standards that would accelerate the adoption of IoT,
  - cybersecurity,
  - infrastructure,
  - supply chain,
  - partnerships, and
  - education.
- The complexity of the landscape and the lack of standards are linked barriers that lead to indecision, difficulty in integrating solutions, lack of confidence in the survival of IoT equipment manufacturers to provide long-term support, and concerns about the total cost of ownership of implementation and maintenance of the equipment.
- Having clear and consistent standards was identified as an accelerator of adoption of IoT. This is linked to increasing interoperability and decreasing costs. Currently, there is a range of formal and informal standards as well as an increasing number of protocols. Streamlining these standards would reduce cost and complexity.
- The challenges with cybersecurity include the difficulty of evaluating and comparing vendors, the lack of minimum baselines which could drive users to “rogue connectivity models” that increase risk, the need for clear cybersecurity guidelines aligned with risk (i.e., light bulb vs. manufacturer tooling), the encouragement of the Secure-by-Design approach, the use of product labels that communicate

capabilities and help adopters evaluate and compare capabilities, and SBOMs which enable actionable vulnerability programs.

- Mr. Boulos discussed the need for data standards and ontologies that could enable vertical standards and indicated that data sharing with clear data ownership unlocks the "exponential" value of data which could go beyond IoT.
- Core infrastructure is a significant hurdle. Mr. Boulos presented digital public infrastructure as an essential solution which lowers participation cost for everyone.
- Supply chain was presented as requiring "repeat acts of heroism" to retain the ability to ship product, with many inefficiencies. An indication that manufacturers are encountering serious supply chain challenges is that they are abandoning Just-In-Time and lean principles.
- Partnerships provide the opportunities to collaborate, and share public data which could aid the economy, and invest in the workforce of tomorrow.

Group Discussion

- Ms. Reynolds requested more discussion on education / training for all ages and liked an example in the presentation.
  - Mr. Boulos followed up that we all learn what we're exposed to at a young age and it's more natural, but we can't wait for that. We will have to meet people where they are and equip them with the ability to prepare in the near term as well as next generation.
- Mr. Bergman pointed out the great feedback in the presentation and commented that the Board would hear tomorrow from the White House on the labeling program that uses baseline standards. He asked for examples of digital public infrastructure and asked about what the solution space might be for transitions of 5G networks to different cellular generations.
  - Mr. Boulos indicated that it goes back to lack of standards and that it's hard to select any one technology as vendors have used many different ones. Building and operating a private 5G network is expensive, both original investment and carrying cost, and there's a lack of trust the network will be supported over time. Broad agreement on a small number of standards and protocols and clear guidelines on the cybersecurity side can provide a reliable floor and a lower cost of entry.
- Mr. Katsioulas indicated there needs to be an orchestrated ecosystem approach, not just a simple public/private partnership, to the business of infrastructure. Because the cost of infrastructure is prohibitive today, supply chain to end markets are needed where different ecosystems "connect the dots". He indicated he would like more work done on infrastructure that enables monetization of individual applications and asked, "what does the ecosystem need?".
  - Mr. Boulos pointed out that these are hard questions and need to look for competition where value is added because that's where innovation is going to come from. Once you take away the "base plumbing" problems where there's no differentiation and getting data out to the cloud where it can be shared, exposing the data will allow smart people to make incredibly valuable insights. The products are going to be differentiated based on the use of data and thinks that is where we will foster competition at.
  - Mr. Katsioulas concluded this fit with his interest in the horizontal and vertical integration of data necessary to enable digitalization for monetization and create a marketplace with data producers and data consumers in a way that businesses can keep proprietary but license it on demand and that's an essential capability to fuel the future digital economy.
- Ms. Mehra agreed the presentation addressed many topics the IoTAB has been discussing and has a unique perspective from both industry and state government. The point regarding not recognizing IoT

devices as capital assets is interesting and asked - what is the annual KC spend on IoT and how justified is the depreciation over time?
    - Mr. Boulos commented that he can't speak to KC's specific numbers but that across Wisconsin, each company looks a bit differently. Are systems / assets retooled or built with IoT from beginning? Then you see variety in how the data is valued. It's not a balance sheet issue, but it may show up either as products and services that can be monetized or as efficiency. But it is hard to draw the direct ROI line. Sometimes value is delayed (e.g., needs lots of data) and sometimes there is a big up-front cost before you can monetize the data. The delays are a struggle.
- Mr. Tsoneris indicated that a list of barriers could be made, but is the government doing enough to direct the money to the right places? And commented that impact has to happen at the city level.
    - Mr. Boulos followed up that the problem is complex and having transparency around investments is how to take advantage of the challenge.
    - Mr. Tsoneris asked if the money is really out there but may be hard to get to (e.g., grants)?
    - Mr. Boulos pointed out that the Wisconsin IoT council did take advantage of a grant and the money was used for education - mostly for SMBs, work with the university, IoT and also tangential topics (e.g., cybersecurity). This seems to have benefitted those SMBs.

Speaker – Mr. Mobeen Kahn

- Mr. Kahn indicated his background is IoT for mobility working with carriers at different layers of the IoT infrastructure and pointed out some successes with connected cars and fleet management.
- He began by discussing the history of connectivity where the role of government has created the underlying infrastructure (e.g., DARPA and WWW, licenses for cellular communications and FirstNet) and how the creation of these infrastructures triggered significant innovation.
- In IoT, entrepreneurs aren't just creating stand-alone solutions, they must tap into all layers of the solution – e.g., business-to-business, business-to-government.
- He pointed out that what's needed is low-cost and easy integration for new applications that would spur innovation and could enable the commercial space (e.g., for example, the WWW spurred e-commerce applications that got build on top of the infrastructure).
- He gave the example of FirstNet which is a government-funded infrastructure for first responders. He indicated, however, that first responder IoT applications aren't being developed.
- He gave examples of applications that could be added to FirstNet such as connected fire trucks and ambulances and early warning systems. But to do so, he pointed out that there needs to be a lot of investment to create and make available infrastructure at low cost to developers and users.

Group Discussion

- Mr. Bergman wanted to confirm that this is a proposal to investigate funding a national infrastructure for connected devices (akin to public roads vs private streets).
    - Mr. Kahn confirmed, giving FirstNet as an example and cloud infrastructure as another, arguing that these paved the way for extensive e-commerce, collaboration, and social applications with a focus on ease of access and availability.
- Ms. Reynolds followed up on FirstNet – suggesting the extension beyond the first responder space.
    - Mr. Kahn indicated should start in first responder space by looking beyond disaster recovery and gave an example of a state-built system to monitor radiation around nuclear plants that may open up many opportunities.
- Ms. Mehra asked if the architecture for FirstNet could be found on blues.io.

  - Mr. Kahn indicated no, he was talking about a government-related effort and indicated that blues.io pushed IoT on FirstNet but didn't go too far, indicating that perhaps the next iteration could be expanded application for cars, vehicles, or equipment. He added that other examples of applications for FirstNet or a similar public safety network could be early warning systems, radiation detection, fire detection, or endangered species monitoring.
- Mr. Moss wanted to know how this would compare to the private sector like Amazon Sidewalk.
  - Mr. Kahn indicated it could be similar and indicated infrastructure is a place for "extremely large" business consortia or government involvement because of the scale required.
- Mr. Chan asked if the recommendation was for the government to get involved, clarifying that FirstNet was built by the network carriers (e.g., AT&T).
  - Mr. Kahn pointed out that large entities take on infrastructure and entrepreneurs take on innovation. And that in the US that's government, telecommunication companies, cable companies, and cloud infrastructure companies. FirstNet took six years of planning and is still being built out.
- Ms. Mehra referenced back to Mr. Boulos' talk where he identified the lack of considering IoT as a capital asset as a barrier and asked whether tethering to an infrastructure could get portfolio equipment to appear on a balance sheet.
  - Mr. Kahn pointed out that devices made for Sidewalk, LoRa, mobile, satellite all have different economics, technology stacks, and manufacturing processes, and that none of them take on critical volume or occupy an economic space akin to mobile phones
  - The latter have a lot of standardization and are well understood, whereas you have to custom-build for IoT where ROI needed is quite high and this is a reason many projects fail.
  - Many cities have gone into smart infrastructure and Mr. Kahn believes the successes have depended on the government's infrastructure investment.
- Mr. Bergman liked the "out of the box thinking" but indicated the model may need rethinking. With respect to competition to existing infrastructure players, asking the government to build a mobile network for IoT – there are already traditional challenges with rural infrastructure like what spectrum will be used, the duplication of mobile broadband at a high level, and if you're looking at LoRaWAN so "not just another 5G". He thinks it will be difficult to sell the funding without more justification on why it's "different from mobile broadband but paid for by the government".
  - Mr. Kahn reiterated that the FirstNet model was interesting where the government laid out requirements and then had competitive bidding to build to those requirements. He believes the orchestration would be such that providers are engaged in the process and government probably shouldn't build but could define the vision and let the commercial sectors determine the right solution.
  - Mr. Bergman indicated that the initial auction for FirstNet failed and that it has been more than a decade so there were lots of reasons why it was difficult then.

Sustainable Infrastructure Topic review

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

Mr. Chan spoke for the subteam.

Mr. Chan shared slides which can be found on the NIST website here: Sustainable Infrastructure Draft Recommendations. There is a companion document: Sustainable Infrastructure Draft Outline.

- The slides presented cover the definition, common barriers / opportunities, use cases, and areas of recommendation.
- Mr. Chan stated that the subgroup started with the definition of Sustainable Infrastructure that they shared at the last meeting. The definition that they found that works is 'Infrastructure projects that are planned, designed, constructed, operated, and decommissioned in a manner to ensure economic and financial, social, environmental (including climate resilience), and institutional sustainability over the entire life cycle of the project.'
- Representative example opportunities are water, energy, transportation, buildings. Mr. Chan indicated that the subgroup already has identified some updates to this list.

Mr. Tseronis:

- Referenced the morning speaker on the opportunity to leverage advanced computational science or smart farming and precision medicine.
- A device introduces risk - cybersecurity and physical risk, cyber physical risk.
- There is no shortage of emphasis over the years on smart cities and IoT.
- Referenced the 'whole of government' approach is really a 'whole of country' approach and indicated there is no quick fix. He pointed out there has been a consistent theme around critical infrastructure. He pointed out that if government, academia, and industry are not working together then, [the United States] won't realize the benefits.
- Indicated that he thinks the government needs to make IoT/smart cities a programmatic function at the highest level. He pointed out IoT is not a CIO job, that there is no Smart City Officer, and that in addition to there being lots of chiefs there are also councils at the executive level.

Ms. Mehra:

- Raised a concern that the recommendations are smart city related rather than sustainable infrastructure related and asked if all sustainable infrastructure is synonymous with smart cities?
- Liked the idea of a "an agency Chief Smart City Officer" or something similar and added on 'Why not an IoT Officer instead of Smart City Officer?'
    - Mr. Chan clarified that smart cities can be seen as a subset of sustainable infrastructure and can be seen as 'low hanging fruit', indicating that the sustainability part is not complete. He also agreed that smart city is a broad term. The subgroup is looking at sustainability and green energy for recommendations too.
    - Mr. Tseronis commented on critical infrastructure in relation to sustainable. He pointed out that sustainable implies the implementation and deployment of IoT if done correctly and called out smart cities as a type of ecosystem and re-iterated his earlier points on a smart city role.

Ms. Megas:

- Pointed out that looking at the scope, there is a danger in saying that everything is smart cities, or everything is critical infrastructure. She then pointed at manufacturing and the term 'sustainable' in this context. The sponsors of the original bill wanted us to address issues around climate change and how we can deploy IoT around social justice. The term sustainability deserves its own focus.
- She agreed that putting sustainable and infrastructure together conflates it. As long as there is some focus being given to how we can use IoT to address some of these challenges, we want to give focus to the intent addressing issues of sustainability.
    - In response, Mr. Tseronis indicated that a sustainable smart cities office could address some of these things

Sustainable Infrastructure Recommendations

NOTE: the Sustainable Infrastructure team chose to present their recommendations in related clusters; the order of presentation in the following aligns with the presentation during the meeting.

Recommendation #1: The federal government should consider funding and establishing a nationwide network of "smart city/infrastructure" extension partnerships (SCEP) that will provide cities, counties, regional agencies, and states with expertise, resources, information and tools in planning, developing, and optimizing the use of "smart technologies".

- The subgroup identified a gap that cities and agencies face a lack of digital skills or resources. This would look like the Manufacturing Extension Partnerships.
- These would be initially funded by the government in partnership with universities or private industry. The goal is to make expertise available to the smaller cities.
- Smaller municipalities, especially have a huge challenge with knowing where to start with what resources.
- The goal is to provide a focal point for governance coordination and integration among CIO, CTO and everyone else needed. Currently there is not a role or an office to support the 'whole of government approach' which would benefit those at the state and local level.
- A barrier is limited expertise in the marketplace making it difficult to obtain.

Recommendation #8: The Federal Government should establish a Smart City Officer (SCO) within each of the twenty-four (24) CFO Act agencies.

- An official in each of the 24 Federal departments and agencies needs to lead the effort to move to smart cities. An identified point of contact and authority lends credibility to the effort.
- The job title is suggested, and the goal is to distinguish from a CIO or Chief Data Officer who have a different scope of responsibilities. Ideally there would also be a federal council of Smart City Officers.

Recommendation #11: 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.

- This recommendation was presented without additional comment.

Recommendation #2: 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.

- To get more IoT in use, the federal government should specify the use of IoT and smart technologies in infrastructure projects. This would be a recommendation to the agencies owning such project.
- This recommendation would require that project owners be knowledgeable about IoT.

Recommendation #3: The federal government should consider funding models for sustaining and support beyond the initial acquisition and building of new projects.

- Even when provided grants, it is a challenge for some small municipalities to sustain operations. Many small municipalities don't have the skills, training and resources and need long term arrangements possibly through public/private partnerships.

Recommendation #6: The federal government should consider offering grants to support smart city projects that target small and midsize cities and agencies.

- There are many more smaller municipalities than large ones. There needs to be a bigger focus on enabling IoT adoption in an equitable way. Regional models can be a successful approach.
- The recommendation for extensions partnership offices could help here.

Recommendation #5: The federal government should facilitate and support the development of smart city and sustainable infrastructure reference architectures.

- Each smart city does its own thing, and the available solutions are not integrated. There is no reference model for smart infrastructure opportunities. The recommendation is that the government use the existing structure that it has to facilitate and support development of smart city sustainable infrastructure. There is a big gap in the market.

Recommendation #7: The federal government should facilitate and support the adoption of smart city and sustainable infrastructure standards in projects.

- There are specific challenges for smart city standards such as integrating SCADA systems, and the convergence of OT and IT.

Recommendation #9: 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.

- There is a need for a (federal) document that speaks to an IoT data strategy (storage, analysis, integration, governance, sharing), and the related need for a governing entity for the recommendation that is going to deliver it.
- There have to be two deliverables – a strategy, and performance metrics to measure progress in meeting the strategy.
- A baseline for what the tools can and should measure is needed.

Recommendation #10: The Sector Risk Management Agencies (SRMAs) shall collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience.

- The government should develop a performance baseline for IoT performance metrics that includes a number of specific metrics that should be measured (quantity, reliability, security, scalability and energy efficiency).

Recommendation #4: 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.

- The goal is to attract talented students to smart city projects, which remains a struggle especially around technology.

The sustainable infrastructure team also provided a draft prioritization of its recommendations and indicated there may be additional recommendations in the future.

Group Discussion

- Multiple members found the template and prioritization approach helpful.
- Mr. Katsioulas suggested that a companion technical diagram of complexity vs. criticality would also be helpful, with the example that critical infrastructure elements, (e.g., nuclear power plants) are extremely critical, and complexity denotes the number of parties who have to collaborate to deliver a solution.
- Ms. Mehra:
  - With regard to recommendation #8 (Chief Smart City Officers) asked of those with government experience: how easy was it to create chief data officers? What impact / ROI could the board reference?
  - Suggested that the recommendation for a National Smart Cities Program Office is the #1 recommendation in current list and would set the stage for other recommendations to follow, and that she could envision other subgroups offering similar recommendations their areas.
  - Suggested it might be better to make the program office scope broader to address "IoT" vs. "Smart Cities".
- Mr. Bergman:
  - Suggested an action to break "sustainable" out into another subgroup, saying that the content that's been presented is for "smart cities" and the board should be honest about that.
  - Noted the board had heard from Mr. Boulos about the need for standards to achieve interoperable solutions, but believes more work needs to be done on interoperability and how to achieve it - perhaps through proof-of-concept / demonstration projects and cited the Matter protocol for Smart Home is an example of addressing interoperability across manufacturers.
- Mr. Chan:
  - Described the challenge in smart city space as the range of technologies, including legacy technologies. Indicated there are many stakeholders and technologies that need to co-exist.
  - Gave examples of intelligent traffic systems that don't talk to one another due to multiple proprietary standards and the similar situation with police radios across jurisdictions.
  - Described the standards concern as especially relevant if moving toward, e.g., traffic or air quality in smart regions as Ms. Raimundo discussed, where different cities are using different standards.
  - Concluded the discussion indicating that all of the recommendations are still draft and there might be adjustments as they are finalized with other IoTAB recommendations.

Augmented Logistics & Smart Supply Chains Topic Review

Sustainable Infrastructure team members: Robby Moss, Tom Katsioulas, Steve Griffith, Mike Bergman, Ann Mehra.

Mr. Katsioulas and Mr. Moss spoke for the subgroup

Mr. Katsioulas shared slides which can be found on the NIST website here: Supply Chain Sub-Working Group.

- There are two primary threads to this area:
  - *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 Background

- Augmented Supply Chain focuses on traditional supply chains and processes that are happening there. Mr. Moss described this as a "tactical approach", describing how integration of new technologies into the supply chain might be beneficial.
- Mr. Moss discussed ten categories of augmented supply chain opportunities. The real value lies in implementation and connecting across supply chains to reap the benefits of the data.
- Mr. Moss presented the opportunities presented by augmented supply chain concepts to the automotive supply chain, broken down by large process steps.
  - Pointed out that the "supplier performance monitoring" section represents an "art of the possible" item that would require a lot of change management and collaboration among suppliers but could be enabled by IoT and would support more resilient supply chains.
  - Suggested the potential for demand forecasting and pricing could be "huge".
  - Described the application of these techniques in a cost-effective way to smaller production lines as a notable opportunity.

Augmented Supply Chain Recommendations:

- The federal government should consider establishing a comprehensive national IoT strategy that outlines clear goals and objectives for IoT adoption in supply chain management. This strategy should encompass regulatory frameworks, infrastructure development, education, and incentives for implementation.
- Promote creation and adoption of IoT industry standards and protocols: Industry standards and protocols will help provide assurance of data privacy, security, and reliability, fostering trust among supply chain stakeholders and promoting the exchange of information across the entire ecosystem.
- Establish and provide financial incentives: Providing incentives aims to encourage businesses to adopt IoT technologies in their supply chain operations by reducing the initial investment costs and perceived risks associated with the implementation of IoT solutions.
- Establish and foster public-private partnerships (PPPs) focused on IoT adoption: PPPs focused on IoT adoption will aim to facilitate collaboration and knowledge sharing between government agencies, businesses, technology providers, and academia. By creating platforms to encourage the exchange of ideas, resources, and expertise, PPPs can help accelerate the development, deployment, and adoption of IoT technologies in supply chain management.
- Invest in and promote education and workforce development focused on IoT: By investing in educational programs, training initiatives, and professional development opportunities, the government

can help provide assurance that businesses have access to a workforce equipped with the necessary expertise to harness the potential of IoT technologies.

- Strengthen cybersecurity measures focused on IoT across supply chain networks: Strengthening cybersecurity measures involves promoting the development and adoption of security best practices, guidelines, and standards specifically tailored to IoT systems in supply chain management.
- Promote international collaboration in IoT adoption across global supply chains: Promoting international collaboration involves creating platforms and forums where policymakers, industry stakeholders, technology providers, and researchers from different countries can come together to exchange ideas, discuss common challenges, and explore opportunities for joint projects and initiatives. This can lead to the development of harmonized regulations, standards, and guidelines that enable seamless integration of IoT systems across borders, fostering efficient and resilient global supply chain networks.
- Support and strengthen sustainable and scalable growth in the domestic IoT manufacturing supply chain: This is achieved via an appropriate mix of policies, incentives, and grants that can gradually phase in domestic content requirements allowing manufacturers to effectively meet deployment goals and strive towards a future where this content is made in all of America by all of America's workers.

Smart Supply Chain Background

- Mr. Katsioulas began with a chart showing the economics of the markets of concern, saying changes will be driven by electronics, regardless of market.
  - Pointed to the importance developing the "digital thread" for visibility of the monetization value of a "significant investment" and building the necessary associated trust.
  - Noted that consumer markets have a much faster life cycle; and the advent of cybersecurity labeling there can drive awareness that can later be extended to other markets.
  - Stated a need for US and EU regulations needed to drive supply chain provenance before considering traceability.

- Smart supply chains provide a "connected value chain" that enables leveraging technology to make smart decisions, supporting provenance, traceability and market preference. He explained this would create a "digital data thread" enabling data analytics and creating new applications that can be monetized.
- Discussed opportunities and drivers for traceable IoT value chains, saying he believes there is currently a "once in a lifetime" opportunity. He described the goal of becoming a "connected supplier" as part of digital transformation.
  - Pointed out the range of requirements for increased collaboration with allies to address supply chain risks, suggesting the US can establish leadership with domestic supply chains, then leverage that with global supply chains.
  - Stated that for provenance we need forward and backward traceability because tampering can happen anywhere in the supply chain and pointed to the use of HBOM/SBOM/DBOM in support of provenance, but also noting this creates a "huge cross-reference exercise".
  - Described international coordination in support of provenance as "absolutely essential".

- Discussed opportunities to create digitalized IoT value chains; he said while the slide content was written toward electronic supply chains it can be applied more broadly.
- Said digitalization of workflows was essential to creating a continuous digital thread of data to monetize, and this needs to extend to all workflows related to a device or product.

- Discussed the need for a new infrastructure where we digitalize the workflows. This infrastructure would support adding metadata indexing to support data marketplace, and a hierarchy of identifiers for physical items and process steps. He briefly mentioned the role of standards for this, saying "This is about recommendations for consistent methodologies and the [NIST] cybersecurity framework basically has shown that there is a way to do it in a recommendation fashion without being too prescriptive".

Smart Supply Chain Recommendations

- Encourage the use of Global Identifier Standards for supply chain traceability: The federal government should collaborate with international allies to create programs that incentivize suppliers to establish unique corporate IDs, product IDs, asset IDs and part IDs by using global standards such as GS1.
- Promote development and use of trusted architectures for supply chain provenance and traceability: The federal government should incentivize hardware suppliers to develop trusted architectures for supply chain provenance and traceability.
- Accelerate creation of a trusted digital thread (DBOM) in the value chain: The government should support the development of a digital thread or DBOM by incentivizing companies to digitalize their workflows and leverage the Cybersecurity labeling program to create a digital trail of IoT systems' holistic Bills of Materials (DBOM, HBOM, SBOM) that vary by vertical market.
- Encourage global cooperation on supply chain traceability standards: NIST and the wider USG should work with international partners to integrate the Cyber Security Framework (CSF) with IoT Security and Cyber-Supply Chain Risk Management (C-SCRM) to enable digitalization methodologies and consistent traceability metrics across borders. This will help reduce compliance costs, track goods across the globe, improve customs controls, reduce administrative burdens, improve global trade and ensure that supply chains are transparent, efficient, and resilient.
- Incentivize the OT Supply Chain to accelerate adoption of trusted traceability: To incentivize the adoption of trusted traceability methods for the OT supply chain, the government could offer tax credits, grants, or other financial incentives to companies that offer traceable OT products. The government could also require contractors and suppliers to adhere to specific security and traceability standards when bidding on government contracts especially for critical infrastructure.
- Promote the Creation of Trusted IoT Network Ecosystems: Drive awareness and interoperability programs on how trust is established among devices, networks, and personas operating in connected IoT environments, in ways that enable secure and reliable data exchanges and protect against malicious attacks, data breaches, and other security threats.
- Incentivize formation of trusted data marketplace: The government can incentivize marketplaces where data producers and consumers can connect and share data, enabling better supply chain visibility and traceability.
- Subsidize digitalization of enterprises in the IoT value chain: The digitalization of all business functions (design, production, marketing, procurement, distribution, etc.) enables more efficient management, greater visibility and traceability over supply chains to track products, monitor quality, and fix issues or defects. By using cryptographic methods, digitalization can have a major impart in the security, reliability, and integrity of the data for the digital economy.
- Promote creation of trusted value chains: Promote orchestration of networks of entities, such as manufacturers, service providers, and regulatory bodies, that interact to establish and maintain Trust through collaboration and accountability to ensure that the IoT value chains and infrastructure are secure, transparent, trustworthy.

- Subsidize orchestrated value chain partnerships: The federal government can accelerate the creation of traceable supply chains by subsidizing orchestration of connected Private-Public Partnerships across complex value chains that digitalize portions of supply chains piecemeal using consistent methods of "receivables-process-deliverables".
- Establish Data policies that drive economic growth: Monetization of data will require infrastructure for Security & Privacy, Data Sharing, Ownership and Control Frameworks, Identity and Access management (IAM), Data Protection, Sharing and Exchange, plus Data Analytics with AI to minimize supply chain risk and maximize economic value.
- Facilitate the Creation of Data-driven business ecosystems: The federal government should raise awareness about the New Gold, Data Monetization Strategies, Data Analytics for Insights, Trusted Data Marketplaces, Platform-based Business Ecosystems, Network effects, Digital Thread of Data in connected value chains, Data Regulations, and tools for Monitoring and Managing Data Marketplaces.

Group Discussion

- Prof. Kornegay asked about how to build this system in a scalable way on top of existing infrastructure with "lots of holes in it" and manage the risks, raising concerns about billions of non-compliant, legacy devices that are still going to be out there. He stated there are "lots of risks" and identified challenges that include a need for extensive HW/SW vendor collaboration, the problem of "competing against economic factors", noting that we aren't going to add a Trusted Program Module (TPM) to a 60-cent chip, which he aligned with the automobile use case of having 300-400 ECUs in a car, and growing.
    - Mr. Katsioulas noted that the subgroup hasn't addressed barriers, saying they will bring that to the next meeting and are focusing here on possibilities. He stated that digitalization of an enterprise can be done today as an add-on, as the validation of the process. He said the application of identifiers enables starting to build the digital thread, which needs to be connected to assets.
    - Regarding security versus cost, Mr. Katsioulas acknowledged there are different cost-performance curves, but said that there is a "vector that everyone has to comply to". He said the subgroup is recommending that government ensure enterprises providing the infrastructure for IoT should be digitalizing guided by requirements similar to the CSF. To do this suppliers will have to make decision to move to newer generation devices that offer useful security.
- Ms. Rerecich highlighted the item about the Federal government raising awareness in data monetization. Specifically, she wanted to ensure there is consideration of consumer privacy and that consumers retain ownership and control over the use of their data.

Smart Traffic and Transit Technologies Topic Review

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

Mr. Griffith spoke for the subgroup

Mr. Chan shared slides which can be found on the NIST website here: Smart Traffic and Transit Technologies.

Smart Traffic and Transit Technologies Background

- Mr. Griffith described the range of technologies being considered and noted there was a strong linkage to the "smart and critical infrastructure" topic.

- The presentation further enumerated a range of potential benefits, particularly with regard to improved safety.
- The identified barriers included interoperability and cybersecurity which present unique challenges for transportation.

Smart Traffic and Transit Technologies Recommendations

Recommendation #1: The federal government should support a National Privacy/Data 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.

- Potential Benefits Examples:
  - Traffic cameras could help determine accident responsibility for more efficient insurance claims processing;
  - Vehicles could receive basic safety information from roadway infrastructure.
- Mr. Griffith pointed that there is personal data embedded in these communications that needs to be stripped out and noted that while some states have privacy legislation the subgroup believes a national framework is needed for consistency.
- Mr. Bergman stated that CTA uses framework terminology for issues like this because of the complexity of the problem, and that something more flexible than prescriptive regulation is needed.

Recommendation #2: The federal government should support 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.

- Mr. Griffith stated that these are currently lacking, leading to interoperability and safety concerns. Potential topics he identified for such standards include communicating with other vehicles, and with infrastructure, and he noted there are many stakeholders. Mr. Griffith said that such standards should be industry-led, but the subgroup sees a role for National Highway Traffic Safety Administration (NHTSA), and many different stakeholders can contribute including autonomous vehicle manufacturers, and providers of infrastructure and communications services.
- Prof. Kornegay described sensors as a perfect example of where standards are needed, noting the broad range of sensors, and the risks of data exposure or spoofing. He asked who should be held responsible for data security. He also raised the challenge of dealing with older, analog devices.
- Mr. Chan observed that this problem was broader than just autonomous vehicles, as many vehicles have a lot of sensors that are used by different parties for different things.
  - Mr. Griffith agreed and suggested the recommendation can be generalized to "sensors in connected vehicles".
- Mr. Chan pointed out that today insurance companies use the data from car sensors and also from smart phones in vehicles and complain that due to little consistency among the readings they aren't getting the same results when looking at driver behavior.

Recommendation #3: 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.

- As an example, he cited challenges today with support for Electric Vehicles (EVs) outside of urban and suburban areas. He suggested that EV-supportive language could be added into building codes and noted that this might be a broader recommendation connected to other subgroups.

Recommendation #4: The federal government should support industry lead standards for minimum baseline interoperability and cybersecurity requirements for smart transportation technologies.

- There are unique components for transportation (e.g., unique keys to unlock traffic cabinets), and the subgroup believes baseline requirements can support innovation without fragmentation.
- Mr. Bergman asked whether government could fulfill baseline interoperability requirements without picking winners and losers and asked for an example.
  - Mr. Griffith responded that an approach being used in surface transportation is to specify the problem you want to solve and let the vendor community design a solution, focusing on an outcome-based approach. He said there are some examples of that being put in place in some locations, such as a vehicle in a school zone displaying a localized warning message.
- Mr. Katsioulas applaud the approach of being use case-driven and asked if the standards would be for device-to-device interactions, device-to-infrastructure, or supply chains.
  - Mr. Griffith described the goal as a technology-agnostic standard for how vehicles communicate to infrastructure, citing the example of emergency vehicle pre-emption of traffic lights to speed emergency responses as an example use case.
- Prof. Kornegay described a use case of totally autonomous vehicles including inter-vehicle communications where an accident, such as a pile-up, occurs. He asked how the data would be shared and disseminated in that situation sorted out and disseminated.
  - Mr. Griffith said they haven't considered such a situation, noting that he doesn't expect to see full AVs on highways in the near-term.

Recommendation #5: The federal government should invest and promote education and workforce development in smart transportation technologies.

- He stated that the traditional "concrete and asphalt" of road construction isn't just that anymore, with the integration of communications technology and signaling, as well as the need for cybersecurity. He suggested that such education programs could start at the high school level.
  - Mr. Chan noted that high school vocational programs have become much less common, at least in the US. He also pointed out that the mechanics of fixing cars are changing quickly, noting this is a challenge for vehicle owners in underserved areas. He suggested a workforce that could reach out to such areas could benefit and noted the similarities to the agriculture "right to repair" movement, and the concerns regarding the availability of skills and tools.
  - Mr. Griffith described the challenges of having the EV charging infrastructure working reliably provided another candidate area for growing an operations and maintenance workforce.
- Mr. Chan asked if the board was defining transportation as cars and excluding other forms.
  - Mr. Griffith said he feels all forms of transportation are in scope.

Public Safety Topic Area

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

Ms. Mehra spoke for the subgroup

Ms. Mehra shared a document which can be found on the NIST website here: Public Safety Summary.

- Ms. Mehra summarized the activities of the Public Safety subgroup, noting the overlap of work between subgroups. She stated Public Safety has focused thus far on barriers to adoption and achieving overall value in IoT. She said the subgroup had no recommendations to present at this time but expects things will "cross-breed" with the work of other subgroups. She explained the subgroup has tried to view things through a lens of overall priority and thinks matters such as delivery of healthcare should receive highest priority.
- The subgroup found that education is both the biggest barrier to adoption and an opportunity.
- Ms. Mehra said the subgroup had worked on an in-scope / out-of-scope list of devices and subjects for this topic (see the list in the shared document) and noted that particular items highlight the potential for overlap with the Smart Cities and Transportation subgroups. She pointed out that what's in-scope for this group would include communications among departments involved in public safety, and many such departments are still utilizing radio technology and haven't adopted IoT. She explained that the subgroup was working in term of categories of public safety regions, started at local governments and then considering implications of moving up the levels of government, and noted that receiving conflicting information from different areas can have significant public safety consequences.
- Described a concept of concentric circles around a crisis: individual impacted by a crisis, individuals deployed in response to a crisis, and resources (other than people) deployed in response to a crisis. She also observed that scale is important to consider regarding barriers to adoption: how do smaller scale solutions scale up to large events (citing the example of large fire), which are another circumstance that may involve dealing with conflicting information. She emphasized the importance of time ("every millisecond matters") and noted the potential for robotics to play a bigger role in public safety, which introduces additional elements of mobility. She also noted the group had identified a very short out-of-scope list, primarily personal safety and deployment of US public safety or crisis teams internationally.
- Stated that the subgroup wants to leverage NIST knowledge in public safety and invited Ms. Kahn to provide some context.
    - Ms. Kahn explained that she was familiar with two relevant groups at NIST, one focused on firefighters, and a public safety communications research group; Ms. Kahn is part of the latter group, which grew from providing the research arm of FirstNet. She said the group was looking into how to evolve first responder communications; how can first responders use sensors in personal area networks and extended to their apparatus; also, the potential use of sensors in constrained and remote areas. Ms. Kahn said her group has found technical obstacles similar to what IoTAB is seeing, such as incompatible protocols, and lack of interoperability between departments, noting that the US has no consistent requirements for first responder communications equipment, and it is often difficult or impossible to communicate in multi-agency response. She also said the community is resistant to change when they have something that works. She mentioned successes with funding prize challenge programs and commercializing solutions. She noted that this is a small market, so it is difficult to get solutions to specific use cases.
    - Ms. Kahn said she has requested more information from the fire research lab. She noted that group has been involved in a global cities challenge that has a public safety component.

- Said it is important to consider whether this is about IoT devices vs. "internet of people" concept and invited Mr. Caprio to provide more information.
  - Mr. Caprio said he has heard the "Internet of people" concept discussed in Europe for some time. He said the IoT Council there have been discussing first principles for about 15 years. He summarized that a focus on protecting people was being recognized in the US but has been under discussion in Europe for many years.

Group Discussion

- Mr. Griffith recommended that the subgroup consider fire safety equipment within a structure (fire alarms, smoke detectors). He noted these provide life safety functions within buildings and are increasingly becoming IoT-enabled. He said there is a group at NEMA focused on "fire & life safety within structures".
- Mr. Chan took an action item to determine how to address "cross-pollination" over multiple subgroups.

Healthcare

Healthcare team members: Maria Rerecich, Dan Caprio, Mike Bergman, Ann Mehra.

Ms. Mehra and Ms. Rerecich presented for the subgroup

Ms. Mehra shared a document which can be found on the NIST website here: Healthcare Summary.

- Ms. Mehra began by stating she believes health care is the most important category of IoT devices, especially those directly delivering therapy to patients. She said the subgroup had tackled barriers to adoption and worked on scope of Internet of Medical Things (IoMTs), considering criticality, and where devices reside on the network. She said their scope included OT devices that are related to healthcare delivery (e.g., sterilization, air handlers) but excludes general IT. She stated that cybersecurity and privacy play a key role.
- A key challenge is asset inventory. A device becomes a "true liability" if it fails to deliver correct care (e.g., medication doses), and stated the position that IoMTs are one of the first asset categories the IoTAB should make recommendations for. She said the healthcare industry needs to consider IoMTs as an asset, similar to, e.g., a ventilator. She also stressed the importance of lifecycle management, and that it is very important to remove EOL devices from service.
- Ms. Rerecich defined the item discussing validation from manufacturers as having some indication that an IoMT device is doing the right thing and hasn't been tampered with. She said this topic was primarily regarding medication delivery.
- Ms. Mehra said the "resounding theme" for the healthcare subgroup is higher levels of scrutiny, and the associated topic of standards for IoMTs. She identified several concerns including a lack of consistent UI among similar devices, and a lack of transparency about algorithms used within individual devices; both of these things can vary both between manufacturers, and between single manufacturer product lines.
- As with supply chain and public safety, there's resistance within the medical community to changing something that's working. This, combined with the treatment of IoMT devices as cost line items, is a barrier because it becomes difficult to shift to new devices with different UI and generally to evolve as the technology changes.
- Health care IoT includes both devices that are in medical facilities (e.g., at bedside, at nursing stations) as well as telehealth devices in homes or vehicles that are monitoring patients.

- Regarding mobile apps and trackers, Ms. Rerecich explained that there has been a proliferation of apps tracking various health aspects (e.g., mental, reproductive), and that the data collected in most cases is not HIPAA protected even though users typically think it is. She described this as partly an education thing but also there is a need to specifically address protecting this data.
    - Ms. Mehra described this item as a barrier to adoption, saying the subgroup will have recommendations.

- Ms. Mehra stated that provider portals are also in-scope to consider, as are both business-to-government and business-to-business interactions. She described data feeds and data-in-transit within a facility or beyond as in-scope and needing recommendations for protection, and the subgroup has a catalog of data potentially at risk (see document).
- The subgroup's education recommendations will address a range from consumers, through healthcare workers, family members, and support providers. Finally, she noted the document lists a collection of background information they've identified and a speaker they hope to have at the next meeting.

Group Discussion

- Mr. Katsioulas described his takeaways as the need consider the assets and their life cycle and where they require transforming existing end users. He described this as an important cost factor that needs to offset the ROI factor. He also identified that testing should be part of traceability in the supply chain, recording testing done and results, and suggested that can that appear in the cybersecurity label.
- Mr. Bergman addressed IoMT asset tracking, noting that identifying capital assets vs. expense line item is a tax law matter and there's a price breakpoint where something becomes a capital asset, which are subject to depreciation. He said the lack of tracking expense line items is an important insight, but he doesn't think making all IoT devices a capital asset is the straight-line solution.
    - Ms. Mehra explained that how these medical devices are procured and budgeted is very different from non-IoMT purchases: biomedical engineers and teams are responsible from a budget line and product selection perspective, then the responsibility to implement and manage the devices is placed back on IT organization. She stated only very large, very expensive items (e.g., MRI scanners) are treated as capital assets.
    - Mr. Bergman described this as a topic to explore starting with whether there's traceability at time of purchase. He noted that there are efforts to include unique device identifiers through cybersecurity requirements, suggesting that could give IT departments visibility into devices on the network, and that the missing piece is associated requirements regarding management console and UI to support asset tracking. He describes this as business process improvement, rather than technology concerns, and suggested that identifying tracking of IoT after acquisition as a "best practices guideline" would be a useful recommendation.

- Mr. Bergman noted that the recommendation for "transparency" for AI use and algorithms in IoMT would need some development, and perhaps should be scoped to the medically significant aspects. He identified a concern of creating a requirement for large volumes of documentation that yield very little insight.
    - Ms. Rerecich noted that another aspect of algorithm transparency is the ability to review for algorithmic bias, something that can be particular important in a healthcare context. She suggested transparency would mean the opportunity for external review and/or peer review to look for bias.
    - Mr. Bergman responded that that was heavily dependent on training data.
    - Ms. Reynolds noted that, with regard to regulations, AI is a "super-hot" topic in EU and that in the US there are already some laws, including an AI audit requirement in New York State.

  - Mr. Caprio concurred, suggesting that the IoTAB needs to "tread lightly and carefully", and thread issues around transparency, accountability, and regulation while still allowing AI in health care and other areas to flourish.

- Mr. Chan suggested that AI was its own separate topic that cuts across a lot of sector areas and should be acknowledged but in a limited way.
  - Ms. Cuthill stressed that AI is not the scope of the IoTAB, other than as it relates to IoT.
  - Ms. Megas suggested that the group had struck the right chord and can't completely ignore AI implications of IoT. She pointed out this is not a new discussion, noting that CPSC had a series of workshops trying to understand all the elements of risk of connected products. She also pointed out the existence of an AI FACA[1] and suggested the IoTAB could recommend that the AI FACA examine AI as related to IoT and provide some considerations. She also noted existing NIST work with the EU, leveraging the AI RMF, and suggested they could arrange a presentation.

Closing

Mr. Chan received two action items:
- Split smart city / sustainability into two sub-teams.
- Determine how to address cross-pollination topics.

Ms. Cuthill adjourned the meeting.

[11] Information on the National AI Advisory Committee can be found at https://www.ai.gov/naiac/

IoTAB Meeting on Wednesday, April 19, 2023

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

Mr. Chan reviewed the agenda and introduced Eric Simone

Speaker – Eric Simone (Clearblade)

Mr. Eric Simone shared slides, which can be found on the NIST website here: State of IoT.

- Mr. Eric Simone is CEO, founder of Clearblade, based in Austin, Texas. Clearblade is an edge software company and has software deployed in multiple verticals.
- He discussed some of the customers:
  - Rheem, a water heater company, over 500,000 units today connected for energy savings and energy efficiency.
  - Canadian National uses Clearblade Software to monitor critical rail equipment (i.e., crossing switches) and modernize existing infrastructure.
  - Baker Hughes uses Clearblade technology to optimize drilling, in remote locations.
- He identified the following barriers to IoT adoption:
  - Industry churn: It's a nascent industry with too many players entering and leaving the industry
  - Cost: IoT technology is expensive
  - Custom-built solutions can take years to develop and most typically fail to meet expectations (80% was suggested)
  - Scalability: What works for 50,000 devices may not work for 100,000+ devices
  - Cloud Infrastructure: Services provided by the cloud may be too disparate to build an IoT solution that scales effectively
- He compared to the early days of competing operating systems. He predicted that the IoT industry is going to boil down to a handful of true, proven operating systems that can run in any cloud or at the Edge.
- Emerging Areas of Success (and Lack of Success):
  - Several big players are getting out of IoT (e.g., Bosch, IBM, Ericsson, Cisco), and this is happening because of a lack of success.
  - There are successes emerging. Examples include:
    - Rail industry vendors have proven software at scale. This is software that spans their critical infrastructure, not custom built or tethered to a hardware vendor.
    - Electric grid needing to modernize substations and charging stations because of demand for electric vehicles.
  - It will take a few more years to effectively scale these IoT deployments.
- Advancement is about providing foundational software to sit above the operating system.
  - Linux, usually, or Windows runs on a gateway at a railroad crossing or in the cloud.
  - Behind a secure firewall, different companies can customize and build vertical solutions for sectors (i.e., energy, transportation, manufacturing, agriculture, etc.).
  - Clearblade customers listed from transportation/logistics (lots of Class 1 rail, electric vehicles), energy/sustainability (oil and gas), connected products (monitor, control).
  - We need to think of how this software is built and make sure that there is a de facto 'standard' that evolves.

Group Discussion

- Mr. Caprio noted that part of the opportunity the IoTAB has is to issue recommendations on how to grow IoT. He asked if Mr. Simone had any specific recommendations or could name any barriers.
  - Mr. Simone responded that lots of people talk about Smart Cities, and he believes that the funding should come from federal level. Instead of different solutions for rail, light grid etc., there should be a standard.
  - Rail succeeded because it had government funding to modernize existing equipment rather than buying new infrastructure. It greatly reduced truck rolls for maintenance of equipment and providing accountability and logging on full function on that equipment.
- Mr. Chan asked Mr. Simone to elaborate on the difficulties for smaller companies of breaking through in this space, especially with the federal railway administration.
  - Mr. Simone: Things typically go to the big players: IBM; Microsoft; Amazon. They have great stuff. He pointed out the real proof is in deployment. Look at massive industries like rail, oil, gas. It's hard to compete with the advertising these organizations can buy. It is hard for companies that are truly innovating. Then there is lots of fake news about technology. There are a lot of promises of AI. It's hard for anyone trying to make a decision. What is marketing noise from reality? Small businesses need help from the government to remain competitive.
- Mr. Bergman cited Open Radio Access Networks (RAN) and the Matter initiative. Open RAN has competition to decide how to have a common software running on radio network platforms for mobile and broadband base stations. Matter initiative is a secure protocol and supports interoperability. Small businesses can certify products as supporting Matter. Mr. Bergman asked if similar cloud standards would have to be portable between cloud providers and not just the IoT device itself?
  - Mr. Simone: Yes, it would be portable between cloud and gateway. I've done work with Silicon Labs on this in the past. You've got hardware vendors and sensor vendors. There's what I consider remote execution at the gateway level, which is the same as what runs in the cloud.
  - Mr. Simone pointed out that they were the first company to put edge in there. People laughed at us then but now it is everywhere. It lacks definition. It's a foundational layer that can run at a gateway level. It runs on Linux, allows a software vendor to customize software. He pointed out there are lots of companies that like to wall off their technology. We believe in Open API, an open standard and that it would sit alongside Matter and allow for full execution. He pointed out that Matter is a good analog to what Clearblade is doing.

Speaker – Steven M. Kelly, CISSP –National Security Council

Mr. Steven M. Kelly, Special Assistant to the President and Senior Director for Cybersecurity and Emerging Technology, National Security Council, The White House.

- Mr. Kelly called out that in the October White House event, Deputy National Security Advisor, Anne Neuberger expressed her intent to announce next steps in establishing a National IoT Security Labeling Program in the spring.
- He described this as Energy Star for cyber that is needed to raise the bar for security across the vast product ecosystem thereby reducing the nation's vulnerability to cyber-attacks and helping individual consumers choose products that are safe and secure by design.
- The NSC has been working to identify an agency to serve as the program owner. We are on track to make an announcement in late May in line with a section of the National Cybersecurity strategy[2].
- Mr. Kelly pointed out some key elements of the anticipated announcement:

[2] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

  - This is intended to be a voluntary program.
  - The program will use NISTIR 8425 as the program's foundation
  - The program will start with consumer products, but there is intent to extend into the industrial space.
  - The program owner is expected to unveil the national mark at the end of May.
  - The new program will likely leverage ongoing industry efforts through a licensing agreement.
    - The government does not intent to testing all IoT products.
    - We will be licensing use of the mark to programs that align with our intent.
- Harmonization and mutual recognition with analogous labeling programs in other countries is a goal.
  - Have had a lot of interest from EU, Japan, Singapore. Products labeled under a US program could be marketable across the world with mutual recognition agreements.
  - Planting a flag and having a voice as eventual international standards develop.
- Mr. Kelly expressed appreciation for all the work that NIST has done over the last 5 years to get us to where we are now.

Group Discussion

- Mr. Caprio asked - How do you envision the Labeling Program working with all the different elements: private sector, Executive Branch, Congress, agencies, etc.?
  - Mr. Kelly addressed several areas
    - Interest in Congress:
      - Have had conversations with Senator King and his staff since a similar recommendation came out of the Solarium Commission Report.
      - This has bipartisan interest. Serves a public policy need as well as being good for business.
      - Legislation may be needed.
    - On the Government side:
      - This is not a very expensive program in the context of federal budgets.
      - This is a fairly high cost/benefit analysis.
      - Some appropriations will be needed for the program owner.
    - Third-party organizations:
      - The government will create the mark and license its use.
      - There will be some compliance mechanisms (such as audit and market surveillance and policing within their own programs).
      - In circumstances where something goes off the rails, those issues can be handled inside the National Licensing Program and with referrals to a regulatory organization.
      - The Department of Justice could address major issues with their cyber civil fraud initiative.
- Mr. Bergman pointed out that this is not just for consumers. At launch it will just be consumers. And added – do you envision this being something that can be expanded to industrial and enterprise? Can you expand on that?
  - Mr. Kelly: We have discussed this internally - whether this should just be for consumer products.
    - The conclusion was that there is a lot of need based on the threat picture with products like smart energy inverters or smart meters.
    - The attack surface – critical infrastructure functions is significant. The bar is higher than for a doorbell camera in the home. There is some debate about whether we need tailored requirements for different product classes.
    - Expect the Department of Energy and the National Labs to get involved in that technical and standards work.

    - NISTIR 8425 is built for a consumer product use case. We could probably easily move into industrial products. We don't want to miss an opportunity when the need is there.
- Ms. Mehra: I'm assuming you're familiar with the IoT Federal Working Group (IoTFWG) to whom we are providing this report and our recommendations for adoption. Are you working with them? I'm reminded of the program that pushed out many years ago with the proliferation and implementation of Health Information Technology (HIT) solutions and recommendations, which also led to a mark and a certification program that they manage for HITs.
    - Mr. Kelly: We have inter agency policy committees where departments and agencies are involved to discuss policy issues. All the agencies that are in the IoTFWG are involved in that. We discuss how to align and support the program owner.
    - In terms of health devices, we need to get up to speed on that. We want alignment. Thanks for flagging that.

Cybersecurity Topic Review

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

Mr. Bergman spoke for the subgroup

Mr. Chan shared slides which can be found on the NIST website here: Cybersecurity Subgroup.

Cybersecurity Background

- Update on the consumer IoT cybersecurity label program from an operational perspective:
    - The Cybersecurity subgroup is looking at eight elements and the labeling program is one of those eight elements with the focus here on recommendations.
    - The private sector has been meeting to operationalize what the White House is planning.
    - Worldwide, several countries have some labeling in place: Finland, Singapore, Japan, Malaysia, Canada, Australia. Looking at a global ecosystem. The US is a bit different.
    - The US National Label Effort plan is a little different than elsewhere.
    - The CTA working group is working on a framework for a labeling program including:
        - A common US mark, to be unveiled in May. Will be set criteria to use the mark.
        - Will be a way to license existing voluntary industry label programs to use the mark
        - Will be a self-attestation path for qualified manufacturers.
        - Will also be a third-party certification path for manufacturers.
        - Will promote and advertise it domestically to obtain buy in and promote it domestically also.
    - The label is conceived as a QR code that links to a page with some consumer-friendly information; this minimizes the footprint on the package. From the front page, link to a second page, which is more detailed, for those that need more information.
    - Criteria for the use of the mark. The criteria for the use of the mark are already known. We are using NIST IR 8425. The government expression is a “consumer baseline” for an average homeowner, however, the baseline isn’t “perfect” or “high-end” security (e.g., no secure root of trust) but solid improvement on the current situation.
    - The scheme for the label program – could be manufacturer specific, segment-oriented, etc. The first one could be UL, CSA, Matter, ioXt.
    - License existing voluntary industry label programs to issue the mark and establish self-attestation for qualified manufacturers. Improvement of what we have now. You'll see no default passwords, encryption of data at rest, things like that.

  - That is a quick run through – happy to take the odd question at the end.
  - The label program is one item on list of eight for this subgroup. Because this meeting is more about our recommendations, if you want a detailed walkthrough of the labeling program reach out to me offline.
- This is a summary report out from the cybersecurity subgroup:
- Proposed Cybersecurity Section Content – General:
  - There are linkages to many of the subgroups.
  - This group is not going to deal with privacy end to end. Generally, we are going to address how device storage of data should be considered in the context of privacy. More emphasis is needed on the linkage between security of devices and user privacy. So, when devices are in the proximity of users, they tend to collect data about those users and as soon as that data goes off the device, there's a privacy concern.
- This subgroup will distinguish between major IoT sectors and their different needs:
  - There are accepted standards in industrial (62443) IoT and certification programs (isa-secure.org)
  - We think there are special considerations like the needs of the medical community versus the needs of the industrial world in terms of cyber security
  - Medical devices are different, they come under FDA review.
- Another major topic is that security should be designed from the inside:
  - Especially at the high end, considering security from the development of the chip inside provides opportunities to improve technical security (e.g., secure root of trust) and apply secure development lifecycles.
  - Considering how supply chain traceability applies to the security of the device, we need to identify opportunities for improvement (e.g., secure component, tamper coating, supply chain consideration, counterfeit devices, most devices originate overseas "out of sight").
  - Baseline security only gives you so far. Next level up you could have secure design with secure components.
- Counterfeit devices are a concern.
- Legacy IoT must be addressed.
  - There isn't a good solution for legacy IoT beyond encouraging swap-out for more secure devices, and this should be "part of the plan".
- Secure computing platforms:
  - Trusted Program Module (TPM) is the industry standard. Commonly these are found in laptops (for example, a computer can't boot Windows 11 without a TPM). Getting that level of security in to be standard in IoT is something we want to be thinking about.
  - We need to be planning now about how to put secure elements into cost-sensitive developments.
  - When most components are made overseas, out of sight from the original designer, it's a challenge. How do you deal with full security to avoid malicious tampering? This is where traceability comes in.
  - Noted NIST work on this since 2017.
  - Also, we need to also look at emerging attack vectors: for example, battery draining attacks.
- Barriers:
  - Lack of trust in connected devices:
    - For example, people have concerns about smart speakers – which includes privacy issues.
    - Biggest issue in the consumer space is probably botnets running on their devices (e.g., printers) - probably more common than Alexa listening in.

        - In 2021, 80% of botnet attacks (and there are a lot, stats at Cloudflare) were Mirai-based, which relies heavily on failures to meet minimum requirements (for example, using default passwords).
        - These minimum requirements are addressed by baseline security
    - Large installed base of older, non-updated (or updatable) devices:
        - There is a large install base that is not going away soon. People have devices that haven't been updated, or possibly can't be updated.
        - There is still exists heavy reliance on default admin passwords
        - There is a need to build more trust with addressing these low-end issues.
    - Fragmentation over different countries (e.g., Singapore, UK). It would be better for manufacturers to focus on getting cybersecurity right with a single set of requirements.
    - There are evolving capabilities of malicious apps:
        - As an example, people were hacking smart cards by doing statistical analysis on power supply usage when a pin number was sent incorrectly.
        - Hacking techniques continually evolve
- Potential Opportunities – "Largely turning barriers into opportunities":
    - Local collection / storage of data: the NIST concept of a product makes use of cryptographic techniques to protect an entire system important
    - Legacy devices: We are stuck with billions of older devices that are not easily patched, maybe not even supported anymore.
    - Fragmentation: about what's required in different countries. Singapore now has a national legal requirement.
    - Requirements: Manufacturers needing to comply with all these different requirements, it's better for them to focus on getting it right with a single set of requirements.
    - Government coordination: Steve Kelly talked about conversations among governments
    - Transparency: how to improve transparency of security, manufacturer processes, data storage, traceability of devices? Cryptographic traceability is "on the horizon, needs to be considered"
    - Attacks: what more can be done?
    - Privacy: We support the privacy subgroup by looking at how devices should be more secure with the use of data. We will rely on the privacy subgroup to deal with increasing privacy and trust in devices overall.
- He presented a slide with potential solutions and activities
    - Consumer IoT: e-Labeling is an overlapping concept; USA Trade doing work on this
    - Security by Design: CISA just came out with Secure-by-design / default guidance which applies to IoT
    - Built in security in products and systems: Built-in security relates to #2, but also other aspects
    - Harmonization
    - Market incentives for implementing cybersecurity: Market incentives: part of the group consensus; "earned safe harbor for liability issues if complying with best practices"
    - Other technologies: Steve Kelly: There are now cybersecurity requirements in building codes, in 2023 codes; part of the solution here
    - Training and workforce (horizontal topic)
- He indicated that rather than trying to "drink the ocean" a lot of people are trying to hit the low end, such as starting with default passwords and working up.

Cybersecurity Recommendations

Recommendation #1 - Engage with Industry: Prioritize broad and active industry engagement when developing and maintaining the government-sponsored portion of this program.

- The White House continues working with industry on how the program should work.
- This is much more complicated to assess conformity for cybersecurity and expertise for this is mostly in industry.
- There are differences from Energy Star largely in the measurement / conformity aspects.

Recommendation #2 - Keep Voluntary: Conformance to any specific set of requirements should be voluntary.

Recommendation #3: Support Current Roles: Continue to support NIST as the developer of outcome-based requirements that inform industry consensus standards, and industry as the developer of those standards.

- Also, a need to continue to model what works in other areas.

Recommendation #4: Create Further Incentives: The Administration should encourage Congressional support to deploy this program, including establishing incentives for manufacturers to participate.

- Consumers will look for the label
- The label opens the door to litigation if hacked (increased liability)
- Manufacturers would like balancing "safe harbor" and harmonization
- Consumer education - big consumer education effort is "beyond what industry can do" and needs government action
- How to obtain funding from Congress
- Coordinated communications among agencies to consumers

Group Discussion

- Mr. Caprio: There are a lot of specifics to consider. International cooperation – harmonization or mutual recognition – it's hard and there is no low hanging fruit. Where should we be looking for cooperation/recognition?
    - Mr. Bergman: Outcomes is where I would start. Harmonization worldwide usually means one standard, one mark. And that harmonization ship has sailed. So now we are looking for mutual recognition (e.g., accept EU mark that sufficient work has been done).
    - What that means is we need a gap analysis on requirement sets and look at the structures for cooperation. Global ecosystem players operating in different countries that can bridge gaps. Desired outcomes may come from those players.
- Mr. Chan: Driving cost down has been a driver in IoT (e.g., manufacturers with 1,000s of devices). Are we giving up security for low cost, how to address that?
    - Mr. Bergman: Drew an analogy with the cultural change required for manufacturers to adopt rigorous quality programs as Japan's quality success demonstrated. At first, this change was viewed as too expensive to do, but the long-term benefits were significant. We need cultural shifts as much as technology improvement. Scale works in our favor – the cost of the hardware element becomes less important. The cultural effort takes on much more importance. We need to get product out there that doesn't have default passwords and unencrypted credentials.

- Mr. Griffith: I'm working on an effort within building management systems. Maybe there's an insurance premium offer to a building manager that implements a set of cybersecurity provisions in the building. Also, a lot of organizations have safety training where they go through safety training, starting from the C suite. Need to make it a mandate from the top down. It is a market shift that is happening.
- Mr. Katsioulas: This is a very tough problem, bridges between cybersecurity and flexibility. There is the secure element, low end devices and there are two answers at the chip level and at the device level. At chip level, you never going to be able to protect the security at every chip. Certain cheap chips that cannot add adequate security.

Privacy Topic Area

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

- **Ms. Reynolds presented for the subgroup**

Ms. Reynolds shared slides which can be found on the NIST website here: Privacy Subteam Recommendations. There is an accompanying document which can be found on the NIST website here: Privacy Recommendations Outline.

Privacy Background

- Ms. Reynolds started by indicating that privacy issues have been touched on by many groups.
- At a high level, the presentation covers opportunities, barriers, and recommendations:
  - Opportunities: privacy throughout life cycle, not just at the end
  - Barriers: lack of trust is a common theme (smart speaker example)
  - Recommendations are not in any priority order

Privacy Recommendations

Recommendation #1: Simplifying Privacy Policies for Reading Accessibility

- There is a "gem" of a 3-page federal law "Plain Writing Act" which applies to every agency. This might be a good model.
- The European Union currently has required this; it's in EU law.
- Privacy policies need to be written in plain language; some companied "dinged" by regulators in EU – this is mostly seeing compliance and should be acceptable in the US.
- There was group discussion around the Plain Writing Act and its potential use as a model of "good behavior."

Recommendation #2. Establish "data use" basics for privacy policies

- This is a recommendation to come up with a high-level "point list" of things that should be included in a privacy policy for IoT products. This could be some sort of baseline regarding data use and make it easier to compare policies.

Recommendation #3 Learning from CCPA, GDPR, and other Privacy Regulations.

- GDPR and CCPA have a history (3-5 years), and we can learn from their successes (e.g., CCPA has a good way to help companies categorize data they collect).

Recommendation #4. Create a National Privacy Framework for Innovation and Data Protection

Recommendation #5: Implementing US Federal Privacy Regulation

Group Discussion

- Mr. Chan: There seems like a heavy consumer focus, but there are also business privacy concerns (e.g., protection of proprietary information). An agriculture business would have devices collecting data that could be viewed as a "secret family recipe", and companies collecting data could look to monetize that data.
  - Ms. Reynolds: The team is also looking at the Business-to-Business side, but many of gaps they're seeing are on the consumer side. We have been listening to other groups' privacy examples. Different parties may have differing views. What's needed is transparency and that's not there yet. Could give customer (e.g., a farmer) control over what can be shared; and currently there is no standard for that level of transparency.
- Mr. Caprio: Is this separate from the American Data Privacy and Protection Act (ADPPA) that passed out of committee in the House?
  - Ms. Reynolds: have looked closely at that bill and am familiar with the federal v. state / local level issue. Many both inside and outside of government think a framework is needed. There is an opportunity to recommend something that can be foundational and acceptable on a federal level. The problem with ADPPA is it's hard to get agreement. The two issues stifling progress are "private right of action" and "pre-emption" so maybe side-step those two - need something that's not a huge omnibus bill.
  - The subgroup didn't have consensus on the ADPPA approach. At the very least need to mention this as agencies have been working to fit privacy within their existing remit. There are strands in ADPPA that relate directly to our goals.
  - Mr. Bergman: If we are going to be supporting regulation, what are we supporting? Felt that discussion was unfinished. We need to be clear on what we're recommending. ADPPA could be on the table with other recommendations noted under learning from what's out there.
  - Ms. Reynolds: Agrees - still in the talking phase. Could be a missed opportunity if didn't address this topic. Can discuss more in subgroup discussions and would like to connect to work of what agencies have been doing.
- Mr. Bergman: Proposed using language around a framework approach rather than a regulatory approach.

Recommendation #6: Privacy Label Creation for IoT

- The cybersecurity label was discussed earlier today. People often co-mingle cybersecurity and privacy, but they are not the same.
- We must find a way to imbue privacy into the transparency part of what we're doing about IoT. Still working on the best recommendation.
- Can think of cybersecurity as the 'table stakes' and the privacy part is more fine-grained.
  - User control over data is commonly addressed in privacy regulation (i.e., state, federal). Users (whether business or consumer) need visibility and control of data about themselves.
  - An example is automobile insurance agencies using data collected from cars to influence insurance rates.
  - Driver's weight information being used to calibrate airbag could also be collected and sold. These are illustrative of concerns consumers have about their data.

- Ms. Rerecich: How could we envision a way that a purchaser can know what the privacy landscape looks like? This could influence choice of products that could move the market. A privacy label at point of sale?
  - Ms. Reynolds: Something akin to EnergyStar that provides transparency.
  - Ms. Bergman: Would like to understand how this thinking relates to different levels of anonymization (i.e., none, reversible, complete). Where do these things drop in relation to those lines? Corporations may not want to revisit these issues for anonymized data.
  - Ms. Reynolds: The least amount of personally identifiable information reduces privacy risk considerably. Still figuring out the anonymization solution.
- Ms. Reynolds: Still in the beginning talking stage now. Want to explore training for the consumer, for the workforce and tie-in to international agreements. These are topics for future meetings.

Katerina Megas and Angela Smith, NIST – Transparency Framework for IoT Cybersecurity

Ms. Katerina Megas / Ms. Angela Smith, NIST

Mr. Chan shared the presenters' slides which can be found on the NIST website here: Labels, SBOMs, Vulnerability Reports, Transparency Reports Oh My….

- Ms. Megas, Program Manager of the Cybersecurity for IoT Program at NIST gave a brief description of NIST's work on IoT cybersecurity.
- Ms. Smith, Technical Lead for NIST's Cybersecurity Supply Chain Risk Management Program (CSCRMP) mentioned that "IoT is a closet passion".
- Ms. Megas indicated that she is seeing more request for forms of transparency and that both parts of NIST and ITL's mission includes 'advancing trust in technology'. There has been discussion about what organizations should do for cybersecurity and now it's time to talk about transparency.
- Ms. Smith pointed out that transparency is the latest buzzword, but there needs to be an understanding where there are transparency gaps. She can envision multiple benefits, but we want to understand the risks, the people involved (aka supply chain) and a recognition that we need to better share information. This would extend beyond transparency requirements into looking towards positive outcomes such as better relationships, improving reputation, etc.
- Ms. Smith pointed out that the supply chain world is often very opaque, and information has to be discovered which is suboptimal. Want to move it towards more dialogue and include measurement as an important aspect.
- Mr. Bergman and Mr. Katsioulas: What about Hardware Bill of Materials (HBOM)?
  - Ms. Smith indicated that as a framework, it can address any prospective need.
  - Ms. Megas pointed out that that the initial scope is to connected products / IoT to see if the principles apply broadly.
  - Mr. Bergman pointed out that an HBOM would apply to a connected product and indicated there is a group effort to build a framework in industry that is close to publication.
  - Ms. Megas said that this would apply to all transparency requests as a consistent way to look for potential to profile for specific cases. And indicated tend to pick on a SBOM.
  - Mr. Katsioulas pointed out that there is an HBOM and a Digital Bill of Materials (DBOM) for the enterprise representation BOM and would love to have a discussion (citing another individual).
- Mr. Caprio asked if this is intended to be more at the tactical / compliance level or seeking to up-level to strategic level? How you think about risk is an essential concern. And indicated he is not clear how this relates to risk.

  - Ms. Smith thinks it's beneficial to take the strategic picture view as compliance would take us down a narrow path. We want to enable better informed decisions and start asking those questions starts to 'tease out' what should be included in the framework.
  - Ms. Megas indicated that from an IoT perspective, the baseline started with technical requirements and then started to articulate non-technical requirements. This opened the discussion around transparency. We've had a lot of conversations about documentation. The framework is a next step responding to the feedback we received.
- Ms. Megas identified next steps and indicated this is all proposed. Hopes for lots of conversation at RSA Conference and is looking for both positive / negative feedback. Plan to put out a blog and a plan for a discussion essay reflecting the inputs we've heard. The overall target is a year from now.
- Mr. Bergman called attention to the difficulty in reporting the right information. He said to create a framework to increase reporting is one thing, managing the "don't report this if you don't have to" is important too.
  - Ms. Megas concurred. It may help recipients scope what they should be asking about and help providers examine what's actionable by recipient to examine the useful information.
  - Mr. Katsioulas pointed out this connects to supply chain, cybersecurity, and privacy. He added that if pushed as a NIST strategy could have a huge impact.

Environmental Monitoring Topic Area

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

Dr. Shehabi spoke for the subgroup

Mr. Shehabi shared a document, which can be found on the NIST website here: Environmental Monitoring Sub-Working Group.

- Indicated the subgroup is a little behind.
- Environmental Monitoring is an approach to achieve something and will be integrated with the other subgroups to help achieve their goals.
- Environmental monitoring impacts the public safety, supply chain, precision agriculture, and sustainable infrastructure sectors.
- Environmental Monitoring has been around for the last century in some form. IoT is how this will evolve in the future.
- Three ideas:
- Opportunities where collected data is centralized, and sensors are remote. (For example, how EPA has measured air quality in the past).
- Monitoring cheap, ubiquitous sensors in consumer products (e.g., Waze using motion sensors in phones for traffic information).
- Moving monitoring to a place we haven't been able to monitor in the past (e.g., close connection here with supply chain and a potential for looking at "Scope 3" CO2 emissions).
- Barriers are similar to other areas and are not well developed yet.
- There is an explosion in data collection - Who is going to own that data? This could hinder growth if not fully understood. With environmental monitoring there's also a concern when tracking through supply chains and that information about companies and their suppliers will be collected.
- Ms. Mehra: Would caution to remain aware of privacy concerns about this data.

  - Dr. Chandra indicated that Microsoft doesn't own any of the data in its agriculture projects. So, providing the privacy hooks – Microsoft doesn't have visibility into the data. Agrees that data ownership should be key and should belong to the stakeholders that are making decisions.
  - Mr. Katsioulas: This is the purpose of the digital thread and examining monetization at each step.
- Consumer privacy is a concern.
- Opportunities:
  - Environmental Sustainability Governance (ESG) investing and ESG's relationship to environmental monitoring. This is something that manufacturers and retailers struggle with (e.g., 'how do I know my carbon footprint?' measure "Scope 3" emissions). Right now, we have environmental product declarations that are an attempt but limited by information provided by the company. There is no consistency; a tracking system within each step of production could help.
  - Environmental Statements for permits: For example, commercial construction in California where companies have to file environmental statements with anticipated emissions, and mitigation plans. This could be an opportunity, for example, with air quality sensors on construction sites or influencing activities like controlling dust on site.
  - Fits with remote sensing and aggregation of data. It's impractical to ask the contractor to deploy monitors and address in real time but opens new opportunities for "what can be measured".
  - Noted overlap with sustainable infrastructure.
  - Enables complex combinations of monitoring air, water and energy recognizing nexus among different areas and provide greater transparency
  - Measuring biodiversity could help quantify impacts on biodiversity.

Precision Agriculture Topic Area

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

Dr. Chandra spoke for the subgroup

Dr. Chandra shared slides which can be found on the NIST website here: Precision Agriculture presentation. There is also a document which can be found on the NIST website here: Precision Agriculture Recommendations.

Precision Agriculture Background

Dr. Chandra:

- Opportunities for IoT in precision agriculture:
  - reduced use of chemicals in aquaculture (e.g., better manage feeding),
  - better decision-making regarding crop selection,
  - post-harvest management,
  - improved farmer income and food security.
- Barriers
  - Complexity: finding how to reduce complexity and enable IoT system to work with other data streams and applications on the farm.
  - Resistance to change, particular in an aging farmer population
  - The lack of a common standard for agricultural data, which inhibits sharing
  - Energy, in particular the challenge of powering devices deployed across a farm
  - Connectivity, citing a USDA study that 60% of US farmland doesn't have good internet connectivity

  - Data privacy and security concerns, where farmers don't want to share their data
- Mr. Bergman ask whether lack of standards and lack of interoperability really the same point?
  - Dr. Chandra said they intersect but cover different points: interoperability is mostly about data and devices talking (e.g., weather, moisture, camera) and will be a bigger problem over time. Standards goes beyond data, things like how you define a farm boundary. He said it is necessary to write custom scripts to ingest data from different providers, and this burden falls on the farmer, who is typically using many digital apps.
  - Mr. Bergman suggested the challenge often isn't lack of standards, but lack of standards being applied or diverse implementation of standards, and that there is a need for manufacturer buy-in to go to something common, citing the CSA Matter standard as an example of the latter.
  - Dr. Chandra replied that there has been work on gateway standards for many years, but it hasn't converged on something manufacturers are willing to use;
  - Mr. Bergman suggested that "lack of incentives for interoperability" or "lack of incentives to use or agree upon standards" as possible rewording of the barrier.

Recommendation #1: "The federal government should consider subsidizing the use of IoT in farms."

- The goal is approaches that are equitable.
- Mr. Bergman noted this is currently framed as a technological play (IoT for sake of IoT), and suggested themes like "The use of IoT in mitigating environmental impact of farming" or "the use of connected devices for reducing water consumption", and generally having a list of specific agricultural priorities tied to the use of connected technologies."
- Dr. Chandra and Ms. Mehra agreed this is a good idea. Dr. Chandra stated the USDA has list of incentive areas for famers that could be linked to IoT use: "climate-smart agriculture", "water use", "carbon capture".

Recommendation #2: "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 broad acre, horticulture, livestock, and aquaculture."

- Dr. Chandra stated that most land-grant universities have AG extension centers, and this recommendation would require substantial funding and financial incentives, but that the subgroup believes this would showcase the benefits of IoT. He said this should be done nation-wide to incorporate region-specific considerations. He explained that land-grant universities have R&D programs going on, and these model farms can helps research for digital agriculture. He acknowledged the varying preparedness of universities, so there is a need for training, an interdisciplinary approach with other university departments, or pairing universities to share knowledge. He also said there would be a need to define at least a minimum level of associated cybersecurity requirements.
- Mr. Bergman asked the subgroup's thoughts on scale of grant per university, noting there are about 100 land grant universities, and the potential range of expenditures (e.g., sensor vs. a connected combine).
  - Dr. Chandra noted other factors, including the size of the model farms, and the need to consider both initial and recurring costs.
- Mr. Chan and Mr. Emmanuel noted the potential for this idea to help address the lengthy adoption cycles that are typical in agriculture can be 7-15 years; the model farms can help generate data on IoT's ability to influence the results.

Recommendation #3: "The federal government should consider increasing funding and accelerating implementation of broadband deployment across rural America."

- Mr. Emanuel stated that this is the #1 barrier to adoption of many agriculture technologies. He noted that the challenges for this are variable by region and acknowledged there are a lot of existing initiatives, and this recommendation is trying to push those further.
- Mr. Chan subdivided agricultural broadband into three connectivity challenges: broadband to the farm (house); the "last acre" issue, as farms can span thousands of acres; and that data rates currently considered "broadband" aren't sufficient.
- Dr. Chandra points out that a lot of the IoT data for agriculture is uplink whereas most broadband technologies focus more on download speeds. He suggested that a 20 megabit down / 100 megabit up capability in the middle of the farm might be sufficient for current IoT applications, and noted that downlink speeds will become more important in the future with growth of robotics
- Mr. Bergman, Mr. Chan, and Dr. Chandra agreed that there needs to be more investigation of the most suitable broadband technologies for the agricultural environment, and Dr. Chandra suggested that support for this could be added to the farm bill.

Personas

Personas team members: Debbie Reynolds, Debra. Lam, Nicole Coughlin, Benson Chan.

Ms. Reynolds spoke for the subgroup.

Ms. Reynolds shared a slide which can be found on the NIST website here: Personas Chart.

Ms. Reynolds:
- Presented a slide identifying six persona categories and 16 categories of barriers to IoT adoption.
- Described this information as intended to facilitate other subgroup's thinking while considering barriers, opportunities and recommendations.

Mr. Chan:
- Asked for a brief (~1 page) personas write-up for the report.
  - Ms. Reynolds said she will work on that.
- Suggested subgroups can use the personas to ensure they are considering all groups relevant to their focus and use them as a framework to capture who is impacted by particular recommendations.

Action Items

Mr. Chan, Chair

Mr. Chan:
- Stated that he wanted to review two action items in particular: the updated scope discussion, and the collaboration between cybersecurity & infrastructure

Mr. Bergman:
- Described the scope description has shifted to a "You'll know what IoT is when you see it" approach to give the subgroups flexibility, and said he will update draft content to reflect those changes
- Explained that in US policy circles "critical infrastructure" is well-defined and IoTAB should use that definition

- Suggested the IoTAB use the term "systemically-important infrastructure" to avoid colliding with federal definition, and only use the term "critical infrastructure" when applying the federal meaning.
  - Mr. Tseronis concurred with Mr. Bergman and pointed to "dhs.gov/criticalinfrastructure" for the definitions[3] and noted that there are cyber-physical systems that support critical infrastructure.
  - Ms. Megas clarified that critical infrastructure is mentioned once in the legislation, in the context of security, with requirements to look at policies that "... enhance the security of the Internet of Things, including the security of critical infrastructure." She also discussed what was meant by "sustainable infrastructure" (impact of climate change, etc.), describing it as "infrastructure that supports a sustainable future".
- Mr. Bergman emphasized the point was to not use "critical" with regard to infrastructure. He also noted that Smart Cities has become a subgroup of its own because they have so much content, and sustainable infrastructure now needs its own subgroup.
  - Ms. Megas stated that sustainable infrastructure is part of the mandated scope; smart cities is going beyond;
  - Mr. Tseronis stated that having "sustainable climate-resilient infrastructure" requires using IoT, and that our current infrastructure isn't sustainable after 100 years. He expressed goal of want our infrastructure to sustain for the next 100 years, describing that as motivation for money being spent today and citing a figure of $2 trillion being invested over the next decade.
  - Ms. Megas added that adapting buildings to be more energy efficient is part of it. She said there are findings in the bill that drove the IoTAB motivation for "sustainable" and it's specifically related to environmental considerations.
- Mr. Chan said he sees overlap with smart cities and transportation and proposed the alternative term "essential infrastructure".
  - Mr. Tseronis warned that the meaning of "essential", when used with regard to personnel, varies from agency to agency.

July / August / September Meeting Schedule

Mr. Chan, Chair

Mr. Chan led a discussion of the meeting schedule for the July through September timeframe

- He stated that July 18-19 seemed to be generally acceptable.
  - Ms. Cuthill requested Mr. Chan confirm acceptability with members not present.
- He stated that there seems to be a consensus is to skip August and hold a meeting in September.
- Ms. Megas stressed the importance of having recommendations by the July meeting if the board was not going to meeting in August. She also noted that the board might receive questions about draft recommendations from the public.
- Ms. Mehra asked for clarification about what happens to the IoTAB recommendations once provided to the IoT FWG? May have 30-50 total recommendations?
  - Ms. Megas stated that the FWG is required to consider the IoTAB's recommendations, and the FWG report to Congress will address what FWG opts to do with what the IoTAB recommends and why. She noted that the secretariat is concurrently also working on FWG report which has particular Federal government requirements and reminded members that the IoTAB report will be public on delivery. She stated she anticipates some interaction between FWG and IoTAB regarding specific

[3] The URL Mr. Tseronis provided redirects to https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

recommendations, where the IoTAB may be asked to expand on recommendation(s), or provide support for expanding authorities (e.g., things that require Congressional action or appropriations). She concluded that what happens from there is up to Congress.

- Ms. Mehra suggested adding to the report template information about where federal agencies are with regarding implementation of IoTAB recommendations to-date, to support the ability to identify existing activities the board wants to support versus "net-new" recommendations.
  - Mr. Chan took an action item to update the template.
- Ms. Megas suggested, as an example, that if board members are aware of existing federal activities, such as specific grant programs, their recommendations could address aspects of those programs (e.g., require use of IoT technology in applications for the grant). She said that such opportunities would be very actionable if not requiring new funding or new authorities.
- Ms. Mehra asked if the IoTAB get to review FWG responses before going to Congress.
  - Ms. Megas stated that she didn't believe that is the intent, and that the FWG report will go to Congress and be made public once all of the participating agencies have cleared it.
  - Ms. Cuthill added that there are some timing issues, and that since all of the agencies have to clear the FWG report, the review process could be "lengthier than we would like".

Invited Speaker: Angela Fernandez, GS1 US – Global Identifiers for IoT

Angela Fernandez, GS1 US

Ms. Fernandez shared slides which can be found on the NIST website here: About GS1 Standards.

Mr. Katsioulas:

- Explained he had invited Ms. Fernandez because he believes identifiers are low-hanging fruit for the traceability challenge, and pertinent for supply chain logistics, labeling, anything related to workflows that deliver assets. He concluded that he believes GS1 has the most advanced standard in this area.

Ms. Fernandez:

- Described GS1 as a global standards organization, ISO-recognized, and in operation for over 50 years. She said the organization was best known generally for its creation of the UPC bar code, their very first standard.
- Explained GS1 operations as industry-driven, global processes whose participants are active supply chain stakeholders (raw material manufacturers, distributors, grocery, retail, hospitals, anywhere items are being utilized or consumed).
- That GS1 develops voluntary standards using a federated model with a global office based in Brussels, Belgium and local offices in 117 countries that support implementation across 150 countries.
- Is from GS1 US office, focused on assisting in the adoption and use of GS1 standards; the local offices respond to the needs of local constituents and with local business and regulatory practices
- Stated that a lot of the work is in "non-competitive spaces".
- Describe the types of standards GS1 develops, organizing them into three groups:
  - Identify: Five distinct types of identification numbers
  - Capture: data carriers, in the form of seven bar code formats
  - Share: On-line data exchange services, which store over 4,000 attributes to identify products across 25 industries, including support for transactional processes and physical event data for chain of custody;

- Provided metrics to illustrate current use of GS1 standards. She explained that only customers on supply side need to license an identification number from GS1. Customers who are only on the receiving side don't need to license a number, so those aren't counted in some of the metrics.
- Stated that the global data network has been in operation since approximately 2000 for exchanging data. Customers can enter data once and share it with trading partners, including real-time updates.
- Described the primary functions of GS1 US
- Provided a number of illustrative examples of the application of GS1 standards spanning a number of industries and types of products.
- Noted that GS1 is working with emerging opportunities in electronics and semiconductors based on opportunities Mr. Katsioulas had highlighted. These include pilot projects for "verified credentials and decentralized identifiers".

General Discussion

- Mr. Katsioulas asked if GS1 has a use case to adopt their standards for physical identifiers?
  - Ms. Fernandez replied this varied among industries, depending partly on whether they are more price-driven or more regulatory-driven, noting that unique identifiers can help with counterfeit identification. She also said that unique identifiers can help with circularity and sustainability use cases.

Invited Speaker: Joe Weis, Applied Control Solutions

Joe Weiss, Applied Control Solutions, LLC

Mr. Weiss shared his slides which can be found on the NIST website here: IoT, IIoT, and supply chain implications in OT and process sensor cyber security.

Mr. Katsioulas:

- Introduced the speaker, noting that he had been invited by Mr. Katsioulas and Mr. Griffith to speak regarding "industrial infrastructure".

Mr. Weis:

- Stated that the community (including the IoTAB) had been focusing on networks and has not address concerns related to process sensors, a type of component used in all infrastructures and relevant to all sectors of interest to the IoTAB. He stated that process sensors are not secure and noted that counterfeit parts are a problem.
- Provided a brief illustration of the industrial environment for context.
- Explained his definitions for IoT, IIoT, and industrial process sensors:
  - IoT devices are inexpensive, and perform non-critical functions, possibly including cameras supporting for physical security (typical cost range: $5-20).
  - IIoT devices support data gathering to feed "big data analytics" but have no responsibility for real-time control or safety (typical cost $50).
  - Process sensors are purpose designed to direct all real-time control and safety, and most have direct connections to the Internet (typical cost range: $500-$1000).
- Characterized the insecurity of process sensors, describing them as "technologically incapable of being secured" but treated as 100% trusted.

- Cited examples of numerous incidents, including airplane crashes, power grid issues, and industrial accidents associated with process sensor cyber failures, and emphasized that these incidents happened despite the fact that process sensors are "designed for purpose", whereas IoT and IIoT are not.
- Stated that the insecurity of process sensors has not been addressed in multiple government reports. He shared relevant quotes illustrating the consistent message that process sensors aren't being examined and are assumed to be uncompromised and correct.
- Described a case study of a productivity analysis at an industrial facility, saying it illustrated both the problem and a solution.
  - The investigators monitored the "raw physics" of the sensors using out-of-band monitoring to gather data, and machine learning for analysis.
  - The investigation uncovered the inability of MS Windows to adequately serve as a monitoring and control mechanism for process sensor monitoring, noting that the Windows system missed numerous issues (e.g., inoperable sensors).
  - This investigation was described in an article in the November 2022 issue of IEEE *Computer* (Mr. Weis is a co-author).
- Listed the key project findings, noting that this was not a cybersecurity investigation, and directly involved the plant's engineering staff. Finding included:
  - Process sensors are not as accurate as had been believed.
  - Windows is inadequate for monitoring processes of sensors and is "misleading by design".
  - The cybersecurity of process sensors would better be assigned to engineering than networking, and there is "real ROI" when they are carefully monitored.
- Presented several conclusions and recommendations:
  - Cyber-related incidents have caused billions of dollars in losses and thousands of deaths;
  - Need to bring process sensors "in scope" for cybersecurity requirements;
  - Need appropriate cybersecurity training for responsible personnel.

General Discussion

- Mr. Katsioulas requested Mr. Weis provide a summary of the main barriers to adoption and an expanded discussion of his recommendations.

Public Speaker Period -- Don Davidson – Synopsys

Don Davidson, Synopsis

Mr. Davidson shared his slides which can be found on the NIST website here: Cyber-SCRM perspectives.

Mr. Davidson:

- Described his Cyber-SCRM perspective noting he authored the C-SCRM chapter in recent book from Institute for Critical Infrastructure Technologies book on Securing The Nation's Critical Infrastructures.
- Explained that C-SCRM started under the Comprehensive National Cybersecurity Initiative (CNCI);
- Discussed challenges regarding confidence in for IoT / IIoT, nothing that those systems are network- and software-intensive, with expanded attach surfaces.
- Reviewed lessons learned from DoD and recommended learning from DoD approach to criticality analysis
- Provided a history of SCRM efforts, noting that most mentioned here are continuing and recognizing many are public/private efforts.

- Provided information on numerous relevant references.
- Explained that many supply chain discussions and documents focus on resiliency (mostly availability), but that he believes product integrity and information system confidentiality should be primary concerns. He related this view to NIST SPs 800-161 and 800-171, as well as the DoD Cybersecurity Maturity Model Certification (CMMC). He also noted that the latest National Cybersecurity Strategy "leans in" on product integrity.
- Pointed out that the latest NDAA has a clause requires "establish[ing} a microelectronics traceability and diversification initiative" applicable to both IT and OT.
- Provided references and definitions associated with C-SCRM
  - SP 800-161 is a requirement for federal agencies; foundation for the models of SCRM
- Described a concept of assurance levels
- Noted that SP 800-161 is foundational, with CNSSD 505 providing additional guidance related to national security systems and DoD 5200.44 applying to the secure systems.
- Suggested that the levels of assurance concept should be considered for IoT.
- Stated that individual enterprises must develop overlays or controls, specifications, or standards to measure and manage the risk to their respective area. This could be done based on sectors, use cases, or other approach.
- Emphasized the need to develop traceability and provenance metrics than allow system implementers to make informed design trades.
- Identified the need to have a bar code identifying products, linked to a website with broader information.
- Identified the need to have access limited through role-based access control to provide trust and confidence in the data that defines the digital thread.

General Discussion

- Mr. Katsioulas stated that Mr. Davidson has volunteered to be a resource for the IoTAB on this subject, and that his perspective complements Mr. Katsioulas' "business guy" viewpoint.

Public Speaker Period – Andrea Amico – Privacy 4 Cars

Mr. Andrea Amico

Mr. Chan shared slides which can be found on the NIST website here: Solving at scale PI breaches and transparency of data practices in automotive.

Ms. Reynolds:

- Provided an introduction, saying she has been collaborating with Mr. Amico on data and telematics.

Mr. Amico:

- Identified himself as the founder of Privacy4Cars a company focused on creating privacy solutions for vehicles and related their work to opportunities that have been discussed by the IoTAB.
- Provided a problem statement saying a vehicle is "unencrypted hard drive of personal info". He noted that the connection of phones to cars enabled vehicles to download data in unencrypted form, losing all the phone's protection in the process. He also said even cars without navigation systems probably still have GPS and can track location.
- Explained how used cars are loaded with previous owner data that is routinely not being deleted before resale.

  - Less than 5% of dealers have a process for purging this data.
  - 80% of use cars sold still contain unencrypted data about previous owners.
  - The volume of annual used car sales implies the exposure of huge amounts of leaked data.
- Pointed out that the NIST standard for purging data (SP 800-88, Rev 1) is over 10 years old, and define accepted practice in retail for other consumer electronics but is not applied to cars.
- Stated that manufacturer's privacy policies put responsibility on the owner for deleting data.
  - Manufacturers are not telling franchise dealerships they need to take action on this data.
  - The FTC has issued guidance multiple times but there's no enforcement.
  - Noted that a similar problem exists with rental cars.
- Pointed out that auto manufacturer privacy policies are lengthy, when compared to those of typical technology companies
  - These polices are not written at understandable language levels
  - Sales personnel routinely misrepresent privacy policies.
  - Studies in Europe found that there is not transparency regarding personal data, and this represents an unfair market practice, with the customer implicitly entering into an undisclosed data sharing agreement.
- Presented an accessible, free vehicle privacy report that Privacy4Cars will announce in 10 days, intended to produce "instant transparency".
  - Entering a VIN returns information about any actions taking to protect you, good and bad actors
  - The presentation summarizes privacy policies with 10 items, 5 each highlighting what information is collected and how it may be shared or sold.
  - The site provides links to document quotes and original sources for full disclosure.
  - Future enhancements are planned.
- Discussed things that can be done to improve the situation.
  - Noted a hearing in Congress today on data brokers, saying that cars need to become part of that conversation, similar to other ICT
  - Pointed out that better practices are totally invisible, so consumers are uninformed
  - Drew a parallel to the history of customer interest in vehicle safety increasing after IIHS began publishing crash test results.

General Discussion

- Mr. Bergman asked whether the situation was the same with rental cars.
  - Mr. Amico replied absolutely yes, plus he noted that most rental vehicles have an independent secondary tracking system installed.
- Mr. Davidson reported this topic was brought up at RSAC and discussed the potential for autonomous vehicles to record cabin conversations. He said the question discussed was "how to make the inside of the car secure?"
- Prof. Kornegay said the presentation resonates with an NSF grant he participates on regarding security and privacy in the lifecycle of consumer electronics. He drew a parallel to a smart apartment rental scenario where previous tenant data may still reside in the system and described this as a life-cycle problem from design through decommissioning that involves both security & privacy. He concluded that there is work on framework to address this lifecycle problem.
- Mr. Amico noted particular challenges regarding vehicles:
  - The typical vehicle is 12 years old, so backward compatible solutions addressing the current installed base are needed, as replacement isn't viable.

  - Procedures designed to purge data from vehicles are either ineffective or improperly implemented by dealerships; he said that Privacy4Cars has spent a lot of time trying to figure out the best possible solution for each car, within the bounds of its technology limitations.
  - There are substantial differences among vehicles.
- Prof. Kornegay suggested the need for guidelines to clarify what a "factory reset" means, noting that it may not scrub user-specific information.
- Ms. Reynold described an example where a car will often download the address book from a connected phone, that contact data can still exist after a factory reset, can be transmitted, and is often resold without the consumer's knowledge.
  - Prof. Kornegay noted this can extend to connections between cars and "smart speakers" inside homes, allowing the potential for the car to access data from the devices in the home. He summarized that the intimacy of IoT devices make us more vulnerable.
- Ms. Rerecich pointed out that cars "talk all the time", potentially transmitting data to many destinations. She also noted the use of remote apps that interact with the car, saying it's a known issue that the previous owner can often still access the car (similar to smart home / smart apartment problem). She also suggested that it may be possible to mine some features of the vehicle privacy report for an IoT privacy label.

Action Items and Wrap-up

Mr. Chan, Chair

- Mr. Chan listed four action items from this meeting
  - Split sustainable infrastructure into smart cities and sustainability
  - Capture and address overlaps between teams
  - Confirm July meeting dates
    - This was completed during the meeting. Mr. Bergman offered that CTA could host a hybrid meeting in Arlington, VA, however he needs to confirm their ability to accommodate public attendees.
  - Confirm board members' September meeting date availability by email

The board conducted a lengthy discussion of the path forward for developing recommendations and the final report, with the following results:

- Schedule:
  - There needs to be agreement on the schedule so that the board members and the NIST secretariat are all working to a common schedule
  - A responsive schedule is important because Congress is "watching and waiting" for the board's results, and Congressional interest in the results can wane if the report is delayed
  - Long intervals between full board meetings will appear to be unproductive periods if there isn't other activity evident
- Recommendations
  - The board's primary job is to provide their best possible independent recommendations
  - Using the template to develop and present recommendations will aid in completeness, consistency, integration; if a subgroup can't complete the template for a particular recommendation, then it probably isn't worth pursuing
  - The subgroups should submit draft recommendations sooner, as there will be time to refine them

  - The board members need to understand when the board will vote to approve recommendations. Earlier approval of recommendations permits FWG review and potential question and answer interactions or recommendation fine-tuning between the FWG and the IoTAB
  - The FWG will consider all recommendations received from the IoTAB
- Organization
  - Subgroups that begin their operations later can benefit from the work already done, especially with regard to recommendations that are cross-cutting or over-arching recommendations
  - Concerns were raised about possible over-reach given that the board has identified 16 subgroups compared to the 7 mandated topics in the legislation. Mr. Bergman developed a table to help visualize the situation (included below).
- Assistance
  - Subgroups can ask the Secretariat for research support regarding specific, on-going IoT initiatives in the Federal government, however there isn't capacity to provide general, government-wide answers
- Background
  - NIST encourages all of the IoTAB members to read the original DIGIT act to better understand the intent of Congress.

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)

Charter Element		Current Subgroups (as of April 2023 meeting)
		Skills, Education, Workforce Development (assemble from subgroup contributions)
		Smart Homes
		Standards

Closing

Ms. Cuthill adjourned the meeting.