July 2023 IoTAB: Outside Speaker Recommendations

Chris Moore

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

Mei Lin Fung

- Ms. Fung presented the IEEE Planet Positive list of guiding principles (slide 8), noting that principle #9 calls for responsible use of technology and technology labeling. She explained the point of that principle is to get and track feedback throughout lifecycle at clear checkpoints from design through end of life. She acknowledged that there can be different maturity levels but stated a desire to recognize the efforts of those (vendors/providers) who are more responsible.
- Recommendations (slide 9) Get and Track feedback throughout the lifecycle of a device at clear checkpoints
    - track and measure deployment of technology *at the innovation and experimentation stage*
    - implement a **standardized feedback process** for innovation with **checkpoints** *to catch dangerous or irreconcilable issues, unforeseen consequences*
    - '**responsible technology' labels** for robustly tested technology *so buyers are informed*
    - **certification** of responsible technology in use "by whom" and "for what purpose" *so users know*
    - **certification** of responsible disposal of technology *when End of Life is reached*
    - bring the marketplace in to by inviting insurance companies to participate in standards development, licensing, labeling design and operation. She said their involvement would enable more affordable insurance of IoT and allow the market to expand as more people will be "confident they will be taken care of".
- Ms. Fung summarized (slide 13) that PCI believes the four elements of license, label, identity, and interoperability can address the three barriers of security, identity, and lack of standards, supporting the concept of IoT of, by, and for the people. She added that the PCI community created the recommendations and has the ability to help achieve them.
    - Bonus Recommendation: Digital Common Law (link) has been proposed at G7 Germany and G7 Japan Think7.org, UN Global Digital Compact, to be proposed G7 Italy G7 to evolve laws and regulations always obeying national law, where local communities can make their own decisions while citing precedents from elsewhere
- See also the presentation appendix with 5 pages of input from PCI community (pages 16-20).

Chris Autrey

- Invest in integrating quantum-safe solutions directly into the network to future proof existing and future networks on existing infrastructure. This future proofing protects IoT.
- Invest in relatively autonomous, intelligent networking capabilities that require minimal human involvement once the technology is deployed. This reduces the potential for human error to enable security breaches. The goal is to make networks as automated as possible while maintaining transparency, which brings enormous cost savings potential (e.g., by eliminating the overhead of managing cryptographic keys, and reducing errors).
- Invest in decentralized, dynamic networks that can adapt in real time. He stated that IIoT / IoT are "designed precisely for this", and that it is nearly impossible to properly integrate dynamic IoT / IIoT devices into current static networks.

Paul Eisler

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

People Centered Internet Community Recommendations

Taken from "Strong Sustainability by Design: Prioritizing Ecosystem and Human Flourishing with Technology-based Solutions" (IEEE Standards Association Report)

https://sagroups.ieee.org/planetpositive2030/our-work/

Under The section on Guiding Principles #9, p. 71-73

Not developed specifically for the IoT Advisory Board.

Name and Email	Comment
Vint Cerf vgcerf@gmail.com	Desirable Properties of an IoT Ecosystem https://drive.google.com/file/d/1b_gu1evm5ZHGGmuezOrKSsghoZZ-_9kQ/view?usp=sharing
Albert Boulanger aboulanger@worldteamnow.org	The IOT needs the intelligent enablement for devices to self-tag. Tags in traditional SCADA are manually assigned. Devices need to be aware by a discovery mechanism or imprinted with their role/position in the system they are embedded in, like I am the outside air temp sensor of the 10th floor NW corner air handler to generate its smart tag. There is a lot of related work and good architecture, like IEEE 1451 smart transducer standards https://en.wikipedia.org/wiki/IEEE_1451, including Transducer electronic data sheets (TEDS), SensorML (OGC) https://en.wikipedia.org/wiki/SensorML, Semantic Sensor WEB (OGC) https://en.wikipedia.org/wiki/Semantic_Sensor_Web and Sensor Grid https://en.wikipedia.org/wiki/Sensor_grid and more. Here is a 2005(!) as-is/to-be diagram from How Martingale stochastic control navigates computer-aided lean energy management Oil & Gas Journal Volume: 103 Issue: 35 September 19, 2005, Roger Anderson Albert Boulanger. I believe full realization of what could be done with this as still lacking. http://tiger.aboulanger.com/web/lean/ogj/ogj-9-19-05_files/cap_z050919ogjxan03.gif
Deborah Kobza dkobza@certifiedisao.org	The security of connected products and systems (IoT) continues to be of critical concern for consumers, and public-private organizations on a national, and global scale, with exploited vulnerabilities, malware, denial-of-service, and other attack vectors taking control and subverting the operations of IoT connected systems - impacting public health and safety, and national, global security. 'Security-by-Design' and "Security-by-Default' including implementation of "Zero-Trust' protocols and technology, and continued information sharing of 'actionable' security intelligence and coordinated response within and across public-private critical infrastructure sectors are paramount to ensure and sustain IoT security resilience.
Alexa Raad araad@alexaraad.com	adding to the challenges is the fact that IoT devices introduce new security and privacy challenges because of limited processing capability, lack of high interconnectivity and high interactivity with the physical world and interaction with cloud services. In addition because of lack of data privacy regulation there is little privacy and transparency. In other words IoT devices are passively collecting personal information and the average consumer has little transparency and limited means to understand the data that is being collected and then shared. Another issue is the skills gap. Although cybersecurity industry has been plagued with this for a while now, it is worse when considering IoT and cybersecurity and the problem will only get worse as these devices proliferate,
Dan Esbensen misterdan@gmail.com	Given that at some point, either Quantum computers or advanced Artificial Intelligence will be able to break all of the public key encryption that IOT devices use, how serious of a problem is this?

Name and Email	Comment
Linton Wells linwells@gmail.com	NIST has a major project underway on: "Cyber-Physical Systems/Internet of Things for Smart Cities" <https://www.nist.gov/programs-projects/cyber-physical-systemsinternet-things-smart-cities> Two key concepts shape this program. The first is the need to consolidate the vast amount of insights developed and collected from the previous smart city program and formalize them into a portfolio of publications and guidelines. The second concept is the need to identify opportunities to support standards development processes for smart cities and communities technologies. It has 3 sub-programs related to this: The CPS/IoT Program: develops and demonstrates new measurement science and promotes the emergence of consensus standards and protocols for advanced cyber-physical systems and IoT that are scalable, effective, measurable, interoperable, trustworthy, and assured. Testbed: The IoT/CPS Program is addressing this need through the development of a cross-sector CPS/IoT testbed based on co-simulation and consensus-based design principles for modular, composable testbeds that are interoperable with facilities across the nation and around the world for varying scale and readily reconfigurable for work across the nation and around the world for varying scale and readily reconfigurable for work across domains and applications. Foundations: This project addresses these limitations through the development and application of a CPS Framework (applicable to CPS and IoT) to serve as a foundation for shared development, information exchange, and new formal methods applicable across domains. In addition, NIST has a Special Publication on "Cyber-Physical Systems and the IOT." SP 1900-202 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf> So they've done, and are doing, a lot of work on this. My biggest concern would be: how is NIST's excellent work being adopted in the field, especially abroad? My perception is that the economic incentives related to IOT are (1) functionality, and (2) speed to market. Security doesn't place very high in what's being bought. I'd be glad to be corrected on this, but it seems as though we are building smart cities around the world on a foundation of sand based on IoT insecurity. So my question to them is: (1) How is this changing? and (2) What can we do to see the standards adopted more thoroughly and quickly? Comments welcome. I also agree with Mister Dan's point about the pending threat from quantum computing and advanced AI, but I just think we have an even more dangerous current threat.

Name and Email	Comment
Vandana Upadhyay vandana_upadhyay@yahoo.com	I would bring up security.... Currently, the focus is on protecting data ...the IT derivative approach. However, IoT devices are functional and autonomous devices performing tasks per embedded logic and/or real-time control signals... There is not much appreciation for this as IT teams are tasked with addressing IoT security and they hold the view that with device OS/App security and data security (encryption mainly), it's done. Forgive me for using a morbid illustration in that nobody dies if bank accounts are hacked. Businesses/service providers call cleanup crews, pay off hackers, compensate affected users and its business as usual i.e. that's just cost of doing business. But with IoT as ample examples have demonstrated, potentialities for people to die or the everyday functioning of the world which we take for granted since everything runs on the net, can be stopped (grid, self driving trains, cars and trucks, implanted medical devices, hospital equipment....and of course one's toaster and coffee maker. It's another matter that the IT security stack is also fundamentally broken.... and much of it owes to the design choices made at the time the early protocols of internet were being conceived. The early thought was that internet protocols did not need security elements because communication was essentially inside the building from one floor to another and buildings have physical security and computers required passwords. No one at that time thought it would become a worldwide net. (as documented in anecdotes of Internet History by those who were there and not my opinion.). I co-founded a startup to address this with an approach derived from a market where it's in billions of endpoints using proven technology pieces and using standard protocols (thus minimizing technology risk) but could not get customers to pay for it... .. One could say we wrote the book on this but nobody was buying the book..because as yet a catastrophic incident that moves adoption (e.g. pandemic and Zoom) had not happenned. Tiem and gaian this was the response from CTOs, CIOs and oterh top execuitievs at some very major names in many different sectors... Since we were a starup saying this may it did not carry weight, perhaps NIST can put some guidelines in place. Caveat, there is already oen apper out there from NIST but I believe idoes not provide sufficient coverage of all aspects and does not go deep into implementation and interoperability aspects. And more importantly, it appears advisory in nature with no mechanisms for enforcement either via standards or regulation. There are two strata to this 1. What are the fundamental security principles that should be universally applied to ensure secuirty e.g. over device lifecycle, change of ownership, cross business entity/ecosystem interactions 2. What technologoes enable us to achieve those design principles e.g. encryption algorithms, their interoperability, unbreakability etc... If the first one is not addressed, every advance in 2, will be rendered ineffective at some point. There is always a lot of excitement and investment around 2, but little discussion around one and NIST is the organization to perhaps accomplish 1, the way ITU did for telecom.

Name and Email	Comment
Chris Swan chris@swanz.net	Hopefully you're already aware of the manufacturer usage description (MUD) draft RFC, but just making sure (as it's a good fit for your labels interest). https://datatracker.ietf.org/doc/html/rfc8520 Eliot Lear at Cisco has a couple of posts explaining the background and how it can help with some of the issues that have cropped up with IoT: https://ofcourseimright.com/?p=1859 https://ofcourseimright.com/?tag=mud
Jennifer Hegelson NIST	there is a nascent piece of work - to automate the labeling - under community resilience - NLP - being user tested at U of MD - ask for a demo. Researchers spending a long time on labeling - so learn from the human, scan frequency of terms - makes a suggestion an highlights a short paragraph the "theme" then human collects - an approach to taxonomy and label to do intensive content analysis to understand pieces - qualitative content analysis - under AI umbrella - idea of article on Digital Observatory - analysis of text, understand frequency, bridge what human gets out of it, updates logic
Robert Tse rtse2@mac.com	The rapid development of agriculture technology aka precision agriculture devices and its critical role for 21st century farm suffers from the lack of interoperability as one of two major constraints. The other is broadband. NIST could contribute to resolution of this challenge by helping develop interoperable standards that will enhance the use of the thousands of new agriculture technology devices on farm, encourage continued innovation by new entrants, help farmers obtain the maximum benefit of IoT devices that are integrated seamlessly into farm operations. This will also help farmers integrate and normalize climate adoption technology into farm operations. https://youtu.be/m8oTtS8duDc Here is the use case for interoperability between farm machines. I would expand this further to include all on farm IoT devices."
Marc Goldburg marc.goldburg@stanfordalumni.org	Security principles for the devices themselves, for the protocols they use to communicate with other devices/services including cloud platforms (Google Home/Nest, Apple Homekit, Amazon Alexa), and for the cloud platforms themselves. Safety of life considerations, e.g., hacks of alarm, energy (e.g., residential solar power systems), medical, HVAC and even EV Things Privacy considerations, e.g., unauthorized/undesired access to in-workplace or in-home video, audio and motion sensor Things and their cloud platforms. Also, whether there are safeguards to prevent correlation of an individual's IoT data across multiple platforms/vendors to create a more comprehensive record of their activities than is available from any single platform. The last two might be considered subcategories of "security."

Name and Email	Comment
Paul Werbos pwerbos@gmail.com	In the UN conference this morning, they emphasized civilian markets. As I recall, the official US speaker urged us to pay attention to these NIST actions, but for the civilian side. On the CIVILIAN side... I would still emphasize the need to develop and deploy more powerful, advanced technologies to harden cybersecurity for MANY areas (like what the earlier IEEE EPC motion called for). For the hardware side... we need to develop "quantum bromium", the massive improvement which can be enabled by true Quantum Annealing (true Quantum AGI, as we have discussed before. Most of the knowledgeable speakers this morning (like the main speaker from IA/CAS) gave strong emphasis to the cybersecurity urgencies both in civilian and military sectors. They all called for better open source detection of objects in the sky, which is dual use civilian (especially NASA) and military. Work plans for use of QAGI in seeing the sky, for shared open transparent use, would be our very best hope, in my view. Science France says they want new partnerships with US in many areas, such as quantum, but we will see how far they REALLY go this evening at their open house. I plan to be very quiet and listen a lot. Science France says they want new partnerships with US in many areas, such as quantum, but we will see how far they REALLY go this evening at their open house. I plan to be very quiet and listen a lot.

Name and Email	Comment
Doug Hohulin doug.hohulin@gmail.com	I agree the focus needs to be on security and privacy My one statement would be We need to create a People Centered IoT that focuses the technology to be helpful, honest, and harmless. It is likely in the next 20 years we will have trillions of Intelligent IoT achieving complex goals. We need to ensure these goals are aligned with humanities goals (UN SDG). I fed the this email chain and my statement into Claude and ask for a statement and 10 actions points, here is the response Claude We need to create a People Centered IoT that focuses the technology to be helpful, honest, and harmless. As we approach a future with trillions of Intelligent IoT devices collaborating autonomously to achieve complex goals, we must proactively align these technological capabilities with ethical priorities that serve humanity's wellbeing. Through establishing frameworks for accountable AI, prioritizing security/privacy by design, incentivizing openness and interoperability, and strengthening public-private partnerships, we can steer IoT innovation toward supporting human dignity, sustainability, justice and empowerment for all. With intention and vigilance, the promise of this technological revolution can be harnessed to uplift humanity and accelerate progress on the UN Sustainable Development Goals. Here are 10 action points I would suggest for NIST regarding People Centered IoT: Prioritize security and privacy from the ground up in IoT device and system design. Build trust through transparency. Develop standards and best practices for data minimization - only collect what is needed. Give users control over their data. Create frameworks for accountable AI in IoT - ensure fairness, explainability, and human oversight. Incentivize interoperability and open standards. Break down data and technology silos. Establish methodologies to assess societal impacts early and often. Consult diverse voices. Champion user-centric design, accessibility, and inclusion. Enable technology self-determination. Promote sustainability - ensure IoT lifespan, repair, recycling, and environmental impacts are considered. Build capacity for cybersecurity workforce, digital literacy, and community participation. Partner with other agencies, industry, and civil society to realize shared goals. Lead by example. Create roadmaps for positive technological futures - guide innovation toward serving social good. I gave presentations on the IoT and 6G/WiFi. Here is additional material that may be of use 6G White Paper on Edge Intelligence - 6G Flagship we are constantly assisting at an evolution from the “Internet of Things” to the “Internet of Intelligent Things”. There is a need for an “Intelligent Internet of Intelligent Things” to make such internet more reliable, more efficient, more resilient, and more secure. This is exactly the area where 6G communication with edge-driven artificial intelligence can play a fundamental role.”

Name and Email	Comment
David Bray, PhD david.a.bray@gmail.com	Building on Paul's comments - in 2019 I was invited to give a keynote to the United Nations on UN Charter Day re: what the future might have in store re: AI, IoT, and other advances in technologies. https://www.un.org/en/academic-impact/unai-charter-day-lecture-technology-data-and-future-un From that 2019 talk the same thing I would suggest to NIST is the crucial question: Can open societies, to include democratic nations, benefit from IOT to inform more effective local and national decision-making while simultaneously reinforcing and preserving personal privacy? ... because if we don't answer that question, autocracies will race ahead in using IOT for their social ends and/or open societies will erode privacy protections in order to benefit from IOT. We have to demonstrate better ways forward with IOT to provide benefits to communities will reinforcing individual freedoms include the right to be forgotten and choose when and where information about us is shared.
Brian Donohue briandonohuelaw@gmail.com	NIST needs to develop national standards for the healthcare industry for the most effective clinical use of the Social Determinants of Health.