Q: IoT technology is clearly critical, but expensive. How do you see funding for these critical technologies given limitations of local government funding opportunities?

Peter Hallenbeck: While the actual production cost of these devices is low, there is the usual problem of "As soon as you stamp 'Emergency Responders' on anything the price goes up." Imagine injury or death that could have been prevented if an IoT device had not failed. Using an example from the talk, was the failure of the wiring to the firefighter's speaker-mike something that could result in litigation against the radio manufacturer? As for sources of money, certainly there would be the normal grant opportunities. Note also that accepted best practices are good because they reduce the potential for obsolescence allowing departments to slowly accumulate IoT technology over time. At the end of the day, your concern is very valid. At a time when there is great pressure to reduce funding for all government agencies, emergency services will need increase budgets to cover health and safety equipment, which includes for IoT sensors for responders. Additionally, at a time when staffing is under siege, adding technology for many departments will mean yet another person on scene to monitor and manage the flow of digital information so that Command can be appraised of the current situation. This is similar to when SCBAs (Airpacks/breathing equipment) and better turnout gear were introduced. In our department, we have moved from $50 hoods to the $100 hoods that substantially remove fine particulate matter. This is an age-old problem of how to fund equipment that better protects responders. I don't have a good answer for you, other than to point out that good data exchange standards should help to reduce the cost of IoT equipment and allow for spreading out the purchases over time due to a reduced risk of obsolescence

Q: Any thoughts on aggregation of IoT such as AWS or Azure IoT hub, and standards such as MQTT?

Peter Hallenbeck: I think all those systems for moving IoT data around and managing it will be in use. It seems unlikely that there will be one "winner". These systems are a level above the actual sensor information itself. Note also that these standards are not particularly well suited for a sensor using Bluetooth LE because they require full duplex communications sessions, typically using a TCP connection. It is also not clear that you would want to use these systems all the way out to a PAN device on a person, or the system on an apparatus. Once the IoT data is in a server, be that one the agency runs or one a cloud-based provider runs, then these systems make sense. A superset of the IoT data "Best Practices" are protocols for exchanging sensor data with full contextual information. For incident information that might be APCO 2.105.1-2017 / NG911 Emergency Incident Data Document (EIDD). For final incident information, it might be the NFIRS data definition.

From my perspective, the IoT data solutions are comprised of everything from the sensor to a server that is has a hardwired or very high-speed connection to the Internet. That server will be the one to then use Amazon, Google or Microsoft based cloud systems with their respective interface requirements. MQTT also falls in this class. Running MQTT all the way to the PAN hub will add a lot of data traffic to the scene, which may have limits bandwidth due to local LTE data rate/coverage constraints. But MQTT from a could sever makes a lot of sense because it is so well defined and supported. If that system provides what a software systems developer needs, then that's great. It is important to keep in mind that the size of the IoT data packet must be kept small enough that it can be sent using a number of different communication protocols. For a lot of this data, the packets would need to be under 100 bytes. This is another reason that the larger and more complex storage systems mentions are best handled at a server level where there are no such packet size and bandwidth constraints. A huge part of the IoT problem that we were not really able to touch on due to time constraints is the limitations and considerations for the "Sensor to Server" environment.

Q: Is there an organization that bridges the cellular IoT and WAN/PAN/LAN-based IoT that is specified by IEEE (802.15 1/3/4/7) and proprietary systems such as Sigfox, LoRa and Thread?

Peter Hallenbeck: It's important to keep the distinction between the IoT data definitions and the network/communications channels clear. Cellular data, WAN/LAN, SigFox, Mess Network, LoRa, Zigbee, Thread and others are communications systems designed to deliver packets of data. It is very important that IoT data consist of printable ASCII characters that use the UTF-8 character set. This typically means encoding the software data object in XML or JSON. This then means that IoT data can be communicated using any of the above networks. It is also important that the IoT data standards and encoding selections produce character strings for the packets that will not be so large that they cannot be transported using many of the above systems. For many systems, this could be a limit of 100 to 400 bytes of data.

Q: Is PSCR working with oneM2M to define specifications for an IoT services platform? Is there an overlap between the work that PSCR and oneM2M are conducting?

Alison Kahn: PSCR is not currently working with any SDO towards direct specification of standards. PSCR's current goal is to evaluate existing standards and determine elements that will or will not serve public safety. In our current situation, we are working towards definition, not standards development, and we hope to minimize any overlap that could occur. oneM2M was an active

participant in our roundtable, and we hope to continue gaining insights from them and other organizations looking to promote a more connected communications environment.

Q: Can you direct me to a page on the NIST website that details your Public Safety IoT efforts, reports, etc.?

Alison Kahn: A great place to start would be pscr.gov, which outlines our research portfolios, funding, and publications. If you would like additional information, please reach out to me at Alison.kahn@nist.gov, and I'd be happy to help further.

Q: Is there an organized "donation program" for modern devices / smart phones that could be used for PSCR as an "end of life" strategy (it's okay if they get broken) ?

Alison Kahn: We currently have different hardware loan opportunities, but no direct donation program that I'm aware of. If you'd like to discuss the details further, please reach out to Alison.kahn@nist.gov.

Q: Is there ongoing disuccsion on the "hub" that was referenced in this presentation?

Peter Hallenbeck: There really isn't a discussion of that. My goal has been to make some hardware that has various wireless formats so that there is a platform than can be used to evaluate and discover hub performance. The Raspberry Pi based device will have Bluetooth LE and 4GLTE via USB. Since ti runs Linux, the pool of people who can work on the software should be very large. With some basic software "shell" done, it could even be a good Hackathon project since all the networking is done by Linux and people can just play with algorithms in C, Java, PHP or Python. The overkill on the processor side makes it an ideal tool for discover. The TI chips and module-based hub is classic low level embedded system. As such, it should be low powered and is most likely a better candidate for field testing due to smaller size and weight. The pool of programmers for it is smaller. I see the "Pi Brick" as a good learning tool, and the "Embedded Device" as a good device for field trials. A lot of this is in NISTs court w/r/t/ exactly what the plan is for IoT research and field tests.

Q: What solicitations are coming out for the industry to interact with?
Alison Kahn: All current opportunities with PSCR are listed at https://www.nist.gov/ctl/pscr/funding-opportunities including grants and cooperative agreements as well as open innovation prizes and challenges. We will be updating this as new opportunities are announced.

Q: LTE was mentioned as a network transportation method, is any research being done utilizing 5G?

Alison Kahn: Yes, 5G is a network transport that is currently being explored in several avenues by PSCR. We are also researching technologies that will be enabled by the features of the 5G network.

Q: Since RapidSOS aggregates data from many sources and sends it to 3500 PSAPS, they could be involved in data message standards.

Alison Kahn: I would be happy to discuss this further, please reach out to me at Alison.kahn@nist.gov .