NIST Special Publication 2100-01

Internet of Things Workshop Report

Alison Kahn
Marc Leh
Brianna Vendetti

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.2100-01

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 2100-01

Internet of Things Workshop Report

Alison Kahn
Public Safety Communications Research Division
Communications Technology Laboratory

Marc Leh
Brianna Vendetti
Corner Alliance
Washington, D.C.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.2100-01

July 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

National Institute of Standards and Technology Special Publication 2100-01
Natl. Inst. Stand. Technol. Spec. Publ. 2100-01, 48 pages (July 2019)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.2100-01

This page is intentionally left blank.

PSCR NIST

PUBLIC SAFETY INTERNET OF THINGS

Internet of Things
Workshop Report

July 3, 2019

Work performed in support of the:
Public Safety Communications Research Program

Submitted By:
Alison Kahn,
Marc Leh and
Brianna Vendetti

Project Manager: Jennifer O'Brate
Phone Number: 303-968-9006
Email: jo'brate@corneralliance.com

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.2100-01

Executive Summary

Purpose of Meeting

Purpose & Outcomes

The Public Safety Communications Research (PSCR) Program convened over 25 stakeholders at the Department of Commerce Boulder, CO campus to collect input on how public safety can best prepare for and leverage next generation Internet of Things (IoT) sensor and data collection capabilities. The Public Safety Sensors and Internet of Things project falls within the PSCR - Department of Homeland Security (DHS) research portfolio. DHS Science & Technology Directorate (S&T) sponsored and participated in the workshop and will continue to work with PSCR on the event outcomes. PSCR greatly appreciates their partnership and continued support of public safety IoT research.

This two-day event took place April 3-4, 2019 and provided stakeholders an opportunity to identify and prioritize technology, interoperability, and standards gaps inhibiting IoT commercialization and sensor integration in public safety environments. During the event, PSCR facilitated breakout and plenary discussions that invited attendees to consider the future trajectory of IoT research and development (R&D) activities and brainstorm opportunities for PSCR and the broader R&D community to help public safety realize the potential operational benefits presented by future IoT hardware, software, and data.

Attendees left the event with an improved understanding of public safety's highest priority goals and opportunities for leveraging IoT technologies. In addition, stakeholders identified a list of high-priority gaps that R&D organizations must address before public safety agencies can fully take advantage of commercial IoT capabilities. Attendees also brainstormed ways that R&D organizations can facilitate more consistent, efficient IoT data exchange between industry and first responders.

Background

PSCR chose to host this event because high priority projects in research lanes related to Data Analytics, Highly-Mobile Deployable Networks (HMDN), Location-Based Services (LBS), and User Interface / User Experience (UI) will require effective IoT sensor and data analysis approaches to integrate next generation technologies into public safety operational settings. This workshop asked attendees to consider how the wide range of next generation communications tools may need to be customized to meet unique public safety requirements such as ruggedized hardware components, the ability to process IoT sensor data in disconnected network environments, and the need to share intelligence across jurisdictions and responding agencies.

Definitions

For the purpose of this workshop, PSCR defined the *Internet of Things* as "the networking, sensor, and analytical capabilities that allow information to be sent to and received from objects and devices using the internet." As public safety agencies prepare for the arrival of a nationwide broadband LTE network, they need to consider how to design systems that yield maximum operational benefit from the significant increase in data available, processing power, speed, and reliability that broadband will likely provide. Several key environmental drivers illustrate public safety's need for enhanced IoT capabilities:

- **Proliferation of Small Cell, Deployable, and Multi-Platform Networks:** A greater number of networks will be needed to support customers' increased wireless demand in 5G and future environments. Communications networks will become more dynamic (networks brought in as needed) and platform-diverse (unmanned aerial systems, vehicle, cellular, fiber, satellite networks owned by various operators). These networks will need to interact seamlessly to ensure an optimal quality of experience for public safety users.
- **Proliferation of Edge Sensors, Computing, and Data Collection**: A greater number of connected devices will increase the amount of data available to users and will strain existing networks and analytical systems. Public safety will need new device components to collect this information and new data and computing processes to transform this edge data into useful intelligence for first responders.
- **Public Safety Needs Solutions in Connected and Disconnected Environments**: Emergency responders must have timely, accurate information regardless of whether they can connect to a broadband network. The ability to extract situational awareness in network-connected and device-local communications environments is a priority requirement for public safety.

Agenda

Attendees considered these environmental drivers, PSCR's IoT research to date and public safety's potential benefit from IoT adoption throughout the workshop. The agenda for the *PSCR Internet of Things Workshop* is detailed below:

Day 1 (Wednesday, April 3)

9:00am Welcome, Introductions, and Background
10:00am Review of Existing Public Safety IoT Resources
10:45am Identify Enabling IoT Technologies for Public Safety via a Smart City Use Case (Breakout)
1:30pm Review and Discuss List of Enabling IoT Technologies
2:00pm Gap Identification (Breakout)
3:15pm Prioritize Gaps List against PSCR Investment Criteria
4:30pm Adjourn

Day 2 (Thursday, April 4)

9:00am Review Day 1 Outputs and Discuss Gap Prioritization Results

9:30am Brainstorm Potential End-to-End Solutions that may Address Multiple Gaps
11:15am Demonstrate PSCR IoT Testbed Architecture
11:30am Provide Feedback on PSCR IoT Testbed Architecture
1:30pm Discuss Opportunities to Facilitate Improved IoT Data Access and Exchange between Industry and Public Safety
2:30pm Workshop Closeout, Hotwash, and Discussion of Next Steps
3:30pm Optional Tour of PSCR Research Laboratory

Attendees

This workshop was by invitation only and featured 28 stakeholders from industry, academia, and government:

	Name	**Organization**
1	Alison Kahn	PSCR
2	Andrew Jarrett	ResponderX
3	Anu Appaji	FirstNet
4	Barry Fraser	Bayrics
5	Bert Van Der Zaag	Motorola
6	Bill Schrier	FirstNet
7	Brianna Vendetti	Corner Alliance
8	Britta Voss	NIST
9	Cuong Luu	DHS
10	Don Chiang	DHS
11	Don Harriss	PSCR
12	Isabel Shaw	Corner Alliance
13	Jacob Meek	DHS
14	Jeremy DeMar	Springfield PD
15	Jon Cook	PSCR
16	Kevin McGinnis	National Association of State EMS Officials
17	Marc Leh	Corner Alliance
18	Max Maurice	PSCR
19	Michael Helfrich	Blueforce Development
20	Niki Papazoglakis	Mobility 4 Public Safety

21	Omar Elloumi	oneM2M and Nokia
22	Pete Hallenbeck	Efland FD
23	Sam Ray	PSCR
24	Stacey Trunnell	Corner Alliance
25	Steve Liang	SensorUp, Inc.

Key Themes and Outputs

Several capability and gap themes appeared after reviewing data across all workshop sessions. The following topics were mentioned multiple times across breakout and plenary discussions and are described in greater detail throughout this report.

Capability Themes

- **IoT Data Processing Architecture Brainstormed by Attendees Appears Very Similar to the Potential PSCR Testbed:** Attendees shared a common understanding of how raw IoT data (e.g., temperature reading) should move from the network edge to the public safety user. Public safety needs techniques to enrich information selectively and improve responder situational awareness as IoT data transfers from (1) Environmental Sensor Systems to (2) API Gateways, (3) Shared Databases and (4) Individual User Dashboards. PSCR did not share its proposed IoT testbed architecture with attendees until the conclusion of this workshop, so it is encouraging that attendee breakouts developed similar data processing models from the use cases and technology gaps discussed at this event.

- **Standardized Data Formats and Application Interfaces:** Attendees argued that there is no need to standardize vendor produced applications or visualization dashboards if they can ingest data in a common format. Standardized application programming interfaces would enable public safety to choose products optimized for response tasks while gleaning intelligence from common database sources. Key API capabilities discussed include:
    - Standard APIs that integrate with disparate building operating systems
    - Virtual Knox Box that temporarily allows public safety and non-public safety entities to tap into external databases to enrich IoT data analysis
    - Shared Communications Channel (e.g., Slack for an emergency event with authenticated responding parties)

- **Maintaining Consistent Situational Awareness Databases by Synchronizing Online vs. Offline Data Updates:** Attendees consistently expressed that public safety needs the best, vetted, real-time information from which to make decisions. Modern database structures are not predisposed to reconcile concurrent field updates from connected and disconnected environments. Capabilities such as universally timestamped data inputs into public safety analytical processes can reconcile disconnected data updates (e.g., a

responder moving through a building while off network) with live command center situational awareness dashboards to give responding teams the confidence required to trust emerging IoT technologies.

Gap Themes

Several common gaps appeared across breakout and plenary discussions over the course of the workshop. They include:

- **Data Interoperability**
  - The need to integrate an increasing number of proprietary cloud databases that are vendor- or agency-specific, and store data in disparate formats.
- **Inability to Communicate with Building Sensors**
  - The lack of building data standards and classification rules
  - The cost of standardizing building data is too great to incentivize building operators to engage with public safety.
- **Indoor Location Tracking**
  - Public safety needs more precise victim-to-network LBS microcell triangulation with the ability to track assets in a building. More endpoints could lead to more precise LBS tracking.
- **Need to Secure and Authenticate Public Safety Users (and Third-Party Data Providers / Users) at a Greater Number of Sensor Endpoints**
  - Attendees noted that authentication credentials could be managed through mechanisms such as geofencing (e.g., responder arrives on scene and gains access to shared dashboard), temporary shared databases (e.g., virtual Knox Box), or predefined access roles and responsibilities.

The following table depicts a resulting list of prioritized capability gaps identified by attendees. The participants were asked to rate each gap for its feasibility, impact on public safety, and cost effectiveness, which we weighted for a total priority score as shown below. Reference the IoT Prioritization and Results section of this report for further details on the exercise and a full score breakdown.

	GAP LIST	Feasibility			Impact on Public Safety			Cost Effectiveness			TOTAL SCORE
	Criteria Weight	33%			50%			17%			
	Score Value	1	2	3	1	2	3	1	2	3	
1	The lack of interoperability of dashboards between vendors.	9	9	1	4	6	9	3	4	12	39.39
2	The lack of a fundamental definition of a level of information across “things.”	6	6	8	4	7	8	9	6	4	40.47
3	The lack of a wireless location accuracy standard (x, y, z).	3	5	11	3	6	10	6	6	7	44.31
4	The need for a mechanism to communicate between smart buildings and first responders.	6	7	6	5	8	6	3	5	11	39.86

	GAP LIST	Feasibility			Impact on Public Safety			Cost Effectiveness			TOTAL SCORE
	Criteria Weight	33%			50%			17%			
	Score Value	1	2	3	1	2	3	1	2	3	
5	The utilization of AI as a service rather than an application feature.	6	3	10	5	10	4	4	8	7	39.33
6	The ability for AI to be extended accurately into complex measurements such as hyperspectral algorithms, facial id, object id, and physiological status.	4	9	6	4	6	8	7	5	7	39.66
7	The lack of mitigation solutions for privacy policies.	14	1	3	12	4	3	6	11	2	28.53
8	The cost of integrating tech to buildings prevents most owners from doing so.	7	8	4	5	7	7	4	10	5	38.18
9	The need to promote interoperability between IoT devices that store their data in siloed cloud databases.	6	5	8	3	1	16	1	6	12	48.03
10	Mandate that all IoT sensor data sent into public safety systems have a timestamp.	3	1	15	5	10	4	8	5	6	41.12
11	Contextual information must be stored with IoT data to assign data to users, devices, other identifiers (sensors, cell locations) as it moves across systems.	5	10	4	1	8	10	1	9	9	43.53
12	Develop regional and/or federal IoT data exchanges (database with APIs for local agencies to tap into).	8	7	4	4	4	10	3	2	14	40.55
13	Develop regional and/or national data classification schema for: event type, role, rank, and data type to inform access levels.	4	7	8	7	5	7	5	7	5	38.64
14	Link building infrastructure (communications, data, security) to building maps.	5	11	3	2	9	8	1	7	11	42.04
15	Geofencing to individual room/ floor level is not possible using existing CAD systems.	10	5	4	11	4	4	12	5	2	30.82
16	Develop extensible, backwards compatible IoT data standards that can be added to by industry developers.	7	7	5	4	4	11	4	3	12	42.2

Session Data

The following chapters describe the key discussion points, outcomes, and themes for each workshop session. The document closely follows the workshop agenda. For each workshop session, this report details 1) the intended purpose and design for the conversation, and 2) the highlights and themes discussed by workshop participants. This report will present lightly themed and analyzed data collected during the workshop.

Welcome and Review of Existing Public Safety IoT Resources

Session Design

PSCR kicked off the workshop by providing an overview of the laboratory's positioning as an R&D organization and IoT research efforts either completed or currently underway at NIST. PSCR has internal and external research projects that aim to advance widely used and emerging products and standards poised to enable IoT adoption by public safety. In addition to measuring, testing, researching, and funding these projects, PSCR articulates the long-term research agenda for the R&D community supporting next generation public safety communications capabilities.

For example, PSCR conducted a thorough R&D road mapping process between 2013-2017 that detailed gaps and opportunities facing public safety use of LBS, Analytics, User Interface, and Deployable Network capabilities. The repeatable methodologies used in PSCR's road mapping approach informed the design of this workshop. PSCR also briefed attendees on its current IoT requirements gathering efforts, its partnership with the Department of Homeland Security (DHS) to develop an Airborne Deployable Research Platform (ADRP),[1] and extramural prize challenges focused on UAS Flight & Payload[2] and Smart City data analysis.[3]

After taking questions on current PSCR IoT projects, meeting facilitators described several frameworks that public safety agencies could reference as they begin to consider adopting IoT solutions. Resources such as the DHS Science and Technology Directorate (S&T) Next Generation First Responder (NGFR) Integration Handbook,[4] the National Fire Protection Association (NFPA) standards,[5] and the National Public Safety Telecommunications Council (NPSTC) IoT Working Group[6] intend to guide IoT system developers and vendors through unique public safety requirements when researching future products. These resources define architectures or standards that may be needed for integrated commercial products and analytical approaches with existing public safety systems.

Discussion Points, Highlights, and Outcomes

Attendees requested clarification on several definitions and assumptions outlined during this session. PSCR emphasized that public safety would need IoT capabilities to operate in "disconnected" environments, meaning that their devices may not always have connectivity to traditional networks (cellular, internet, etc.). PSCR is interested in examining how public safety can use devices and applications if a fixed network infrastructure is down. Traditionally, this loss of connectivity stops the flow of data, but first responders will need access to IoT data in

[1] https://www.nist.gov/sites/default/files/documents/2018/11/05/adrp_one-pager_v4.pdf
[2] nist.gov/ctl/pscr/funding-opportunities/prizes-challenges/2018-unmanned-aerial-systems-flight-and-payload
[3] https://www.techtoprotectchallenge.org/
[4] https://www.dhs.gov/science-and-technology/ngfr/handbook
[5] https://www.nfpa.org/Codes-and-Standards/All-Codes-and-Standards/List-of-Codes-and-Standards
[6] http://www.npstc.org/IoT.jsp

damaged network environments. Throughout this event, PSCR instructed attendees to think about how to make IoT benefits accessible when connected communications are not available.

Envisioning the Future State of IoT for Public Safety

Session Design

After baselining participants in the definitions, projects, and existing frameworks available to public safety entities interested in adopting IoT solutions, PSCR asked attendees to identify high-impact enabling technologies within a future-looking Smart City use case. The purpose of this session was for attendees to read through a 14-task scenario depicting a multi-agency response to an active shooter in a Smart City commercial high rise building and identify an IoT capability that most effectively supports or enhances the responder's completion of his or her operational tasks. A full description of the scenario and relevant environmental parameters to consider can be viewed in **Appendix 1: Smart City Use Case**.

PSCR provided attendees with example topics to guide them as they considered which IoT products and services are best suited to each of the 14 scenario tasks. The examples provided to attendees are listed in the table below:

Available IoT Technologies		
- Big Data - Analytics - Digital Twin - Software as a Service (SaaS) - Platform as a Service (PaaS) - Infrastructure as a Service (IaaS)	- Microelectromechanical Systems (MEMS) - Smart Clothing - Smart Fabric - Innovative Transmission Protocols (e.g., Weightless)[7] - Smart Dust Systems[8]	- Machine Learning Technologies - Unique Data Brokers / Services - Data Science Applications (e.g., EVRYTHNG)[9]

Note that the original design was to identify one enabling technology per one scenario task. Attendees were then instructed to consider the status of each technology (available today or a longer-term goal) and whether there were unique public safety requirements to implement before these technologies could be viable for first responder operations. One breakout group was instructed to begin with tasks 1-7 of the use case, while the other breakout group started with tasks 8-14. This approach ensured PSCR collected input on a wider range of response functions before reconvening as a full group to discuss the exercise results.

[7] http://www.weightless.org/
[8] newscientist.com/article/mg21829146-400-smart-dust-computers-are-no-bigger-than-a-snowflake/
[9] https://evrythng.com/

Discussion Points, Highlights, and Outcomes

Given that breakouts did not identify enabling technologies for all scenario tasks, the PSCR team believed it would yield better discussion to review and theme the capabilities discussed across breakout groups. Theming the data yielded a list of 12 discrete enabling technologies that fell into one of three categories. The results listed below align to multiple tasks detailed in the Smart City use case document.

Theme	Enabling Technologies
Asset Planning & Management	Bi-directional Situational Awareness Dashboard that updates in real time (verified map of building that includes location of responders, witnesses, etc. based on wearable sensor data, witness testimony)
	Integrated Dispatch and CAD system that recommends vehicle transit and affects traffic patterns to optimize route to scene
	Indoor drones or robots sent in to collect live environmental data and transmit back to incident command (shared dashboard or communications channel)
	Tagging assets (people, asset location, landmarks)
	Video and image analysis (facial recognition for sentiment analysis and perpetrator identification; asset routing)
	Standardized building data formats and interfaces that enable PS agencies to automatically to access and control building functions
Online / Offline Communications	Ability to maintain latest, cached data when a device falls off network or is reallocated to new user
	High density microcell and device-to-device networks enable more precise LBS triangulation (asset tracking), increased bandwidth (transmission of video and large data sets), micro-localized notifications to responders
	Display “last update” timestamp for data
	Feature rich IoT sub-network containing building information
Roles & Access Policies	Tiered levels of information / data access based on role (public facing dashboard that displays non-sensitive data to witnesses vs. SWAT team dashboard with all situational awareness information informing tactics)
	Tiered levels of information access based on physical location (geofencing)

In the next session, attendees were asked to identify specific gaps that need to be addressed before these 12 enabling technologies could be realized. Before breaking back out into groups for gap identification, participants were asked to provide feedback on what went well and what

did not during their brainstorm of enabling technologies. The group unanimously agreed that future use cases should be narrowed further to focus on one of three disciplines (choosing either Fire, Law Enforcement or EMS) and contain fewer independent tasks to solve. The large task list for several disciplines created difficulties in identifying technologies that spanned task responses or responding agencies. PSCR was advised also by attendees to limit the scope of solutions to no more than five years from development; without this limit, unknown factors such as future advances with self-driving vehicles and other pending future technologies led to questions on the feasibility of their solutions. Finally, attendees mentioned that their focus during their brainstorm revolved around sensors, although they acknowledged many other IoT technologies such as active controls of environments, including but not limited to, building doors, traffic lights, alarms, etc.

PSCR then explained the next session to attendees, prompting them to imagine their themed list of operationally-relevant technologies as reality and assess where the gaps lie prohibiting their current use for public safety IoT capabilities. The following two sections summarize the key discussion points and outputs from each breakout group during this session. Key enabling technologies are indicated in **bold**.

Breakout Group 2 - Enabling Technologies Identified per Task (Tasks 1-7)

Breakout Group 2 was charged with reviewing the use case scenario tasks 1-7. These tasks spanned from responders traveling through a Smart City environment to the active shooter inside a commercial high-rise to authenticating devices upon arriving on the scene to receiving continuous situational awareness updates while working to detain the perpetrator.

Task 1 of the use case reads as follows: “Police, SWAT, Fire, and EMS are deployed and **travel to the scene in emergency vehicles**, some of which host V2X communications technologies.”

- Task 1 Capabilities:
    - **Smart Buildings:** First responders would like to use an IOT application to allow them to connect to the “smart” building, which provides information about the building plan and current conditions within the building. The smart building would have indoor tracking.
    - **Automated Signaling, Integration of Traffic Patterns, Vehicle Telemetry:** First responders would like to be able to control traffic signals and affect traffic patterns via IOT applications to ensure safe and fast transportation to and from the scene of an incident. Useful capabilities of such an app include accident avoidance signaling, enabling vehicles that are approaching intersections to know that there are emergency vehicles coming, monitoring traffic conditions, and assessing the overall health of the vehicle.
    - **Smart Computer-Aided Dispatch (CAD) Systems Must Have Updated Data**: All public safety interactions with data terminals will be connected to CAD systems. By policy, it will not be freely accessible data. Engineers will need to determine how data can be collected, stored in a secure domain, and readily accessed when needed.
    - **Display in the Responding Vehicle / Interface:** The display or interface in the responding vehicle should show other ongoing incidents, so responders can tell

which areas are congested due to other circumstances.

- **Dispatch Center Abilities:** First responders would like for the dispatch center to provide the fastest routes, a capability they do not currently have. To serve first responders well, their dispatch centers need to integrate all the information received about an incident and current conditions, and dynamically change the response routes. “Suggested routes need to come from the dispatch center, not from Google Maps,” explained one attendee. “An ideal app would recommend routes, clear routes, and affect traffic lights to facilitate the route.”
- **Response Collision Avoidance:** Response collision avoidance features should be built into the vehicle itself rather than as a feature on the network. Two-way collision avoidance should be enabled in newer next generation vehicles that can interact with each other. Features would include signaling, collision avoidance, and awareness.
- **Reducing Cognitive Load on First Responders Through Analytics:** “Any time you can remove an unnecessary action from a user, it’s a win.”

- Other Thoughts Related to Task 1:
  - Industry has made efforts to address these problems for purposes unrelated to public safety. Since Google bought Waze, they have been integrating traffic signals into the app. OnStar is working on collision response solutions. Google maps provides information about routes and current conditions.
  - Currently, traffic monitoring is crowdsourced and needs a mechanism to change the routing information due to accidents and other circumstances. It takes several minutes for crowdsourced apps to change their current routes.

Task 2 of the use case reads as follows: “After interacting with various transportation infrastructures, departments **arrive on the scene and establish the area perimeter and incident command**.”

- Task 2 Technologies:
  - **Robust Incident Command Data Cloud and Area Networks:** The ability of the first persons on the scene to communicate is important. Their data will be best communicated through a display in a vehicle. The first responder would use the display technology to annotate data about the scene, create staging areas, and create polygons that are areas of interest. The challenge of this technology would be to make sure IoT data providers can create valuable situational awareness in a timely manner. Incident command would be charged with annotating the data, and there should be multiple commanders working to do this.
  - **Shared Communications Channel:** Responders should have a unified channel between states and other agencies. Other features and considerations for developers of the technology solution include:
    - Access to the data cloud should be tiered based on the roles of the first responders.
    - The cloud updates data from sensors.
    - Agencies need multiple staff to parse data**.** Multiple staff should be contributing to the incident command shared information.

- Public safety will probably need two channel platforms; one for an internal mapping system and another global situational awareness platform that houses more sensitive data - such as locations of responders - and which cannot be accessed as easily. All users need to understand the correct way to share data with the first responders. First responders also need clear instructions.
- When responders arrive on scene, they establish staging areas. That data would affect the routing information to make sure responders bring the vehicles into the proper place.

Task 3 of the use case reads as follows: “SWAT and police turn on and begin **authenticating communication devices and access Smart City cyber-physical systems** such as building sensors.”

- Task 3 Technologies:
  - **Authentication Platforms for IoT:** FEMA and ICAM do not yet have an authentication platform for IoT. This will be necessary for the technologies related to LBS, Analytics, and UI/UX. For example, their vehicles need to connect to the building network immediately at the scene of an accident.
    - Many different people and agencies will be trying to access the smart building information at the time of an emergency. While Police, Fire, and EMS are doing their own work at the scene of an incident, others—such as fusion centers and EOCs—will need data. They will want to know what is going on in a general sense.
  - Another challenge is the absence of standards for building management systems. Buildings are managed and outfitted with IoT by individuals and companies as they see fit. There are no guarantees that public and private sector entities are going to give first responders any information. They cannot be forced to provide information and data to first responders.
  - **Integrating Disparate Cloud Databases:** Public safety needs a common data exchange format identified to connect a data cloud with a local network interface. Ideally public safety could agree upon a universal standard for building systems that is compatible with the solutions deployed. Attendees noted that there is a financial incentive for building owners to enable firefighters to access their buildings and not have the fire department break their property in an emergency situation because they did not have the data available about the building. Other features and considerations for developers of the technology solution include:
    - Buildings will communicate directly to a cloud. Infrared motion sensors can do this independently of the building owner. An interface requirement should be imposed on building management systems.
    - The building needs to know who can get data from it. The building system should have the ability to take the sensors in the building and combine live status data with existing data.
    - Responders could have a heat map of users in the building if the commanding agency has access to the building’s Wi-Fi routers. People’s

phones access Wi-Fi to provide information. Many victims' phones will ping the Wi-Fi routers, and an application could use that information to create maps showing the locations and activities of persons inside the building.
    - Combine all building and sensor data and determine how to display it on the building plan. Wi-Fi, motion detection, and lighting control could paint a picture of the rooms that are occupied and others that are not.

Task 4 of the use case reads as follows: "Fire locates and **accesses their most recent in-building map** and shares it with the SWAT team."

- Task 4 Technologies:
    - **Real-Time Mapping:** From the moment first responders arrive on the scene of an incident, they need real-time mapping apps as well as the building map.
    - **Power:** When firefighters enter buildings that are on fire, they turn of the power. Many buildings have solar panels, which are difficult to turn off. How will they turn the power off in this situation?

Task 5 of the use case reads as follows: "Police begin victim and witness interviews to **collect orienting information about the identification and location of the perpetrator(s)**."

- Task 5 Technologies:
    - **Deployable Sensors:** A deployable sensor goes through the building and returns with a map. Emergency response teams need to know where walls are located regardless of whether or not the wall was reported in the building map data.
    - **Cell Phone Data:** Public safety could leverage victims' text-to-911 data, social media posts, and location information to learn more about an event while it is occurring. Analytics could potentially compare photo or video data captured by victim cell phones to gain actionable intelligence on the perpetrators' whereabouts and/or identity.
- Other thoughts related to Task 5:
    - Video analytics could provide accurate location information and determine if the shooter has a gun.
    - More precise victim-to-network LBS triangulation would be helpful.
    - **"Semantic interoperability"** - taking the raw information and providing additional information about what is relevant, who sees the information, and so forth.

Task 6 of the use case reads as follows: "While referencing building and personnel records, and security systems, they **transmit updates to the SWAT unit** (that has since taken post at building exits) **and to central command."**

- Task 6 Technologies:
    - Public safety needs more precise victim-to-network LBS microcell triangulation with the ability to track assets in a building.

Task 7 of the use case reads as follows: "Responders continuously **receive situational**

awareness information from others on scene and incident command."

- Task 7 Technologies:
    - **Methods of communication to first responders:** Attendees noted that, in reality, the responders on the ground may not look at any of this IoT data. The commander may look at it to inform decisions, assuming there is location tracking within the building. Incident commanders may be able to radio information to the boots on the ground. This relates to the importance of multiple people having access to IoT data, including someone to annotate and parse the data and forward relevant data to appropriate parties.
    - **Autonomous Vehicles, Drones, and Robots:** More often and when possible, first responders should utilize robots to get data from inside buildings. A robot with a video feed is the best option for capturing footage. UAS often find better angles, can snap pictures from video feeds, and send higher quality data to teams.

Breakout Group 1 - Enabling Technologies Identified per Task (Tasks 8-14)

This breakout group concluded its discussion at task 11 (out of 14), noting that starting in the middle of the use cases was challenging since many tasks had to be covered before #8. The group also noted that many of the tasks blended together, rather than being discrete. Therefore, even though three tasks were covered, the discussion covered a range of the use case scenario tasks.

This breakout group was charged with reviewing the latter half of use case scenario tasks, beginning with task 8. Tasks 8 and 9 of the use case reads as follows: "All responders receive an alert to the location of offenders and possible victims, (8), confirm receipt of this message, and coordinate a response to the location point of interest." (9)."

- Tasks 8-9 Technologies:
    - This group discussed XYZ coordinates as an output of the technology identified for the task. For example, there is an existing FCC mandate regarding commercial phones, which must make XYZ coordinates available to carriers once the XYZ coordinate is known. This technology should/could also be made available to public safety, which would make it possible to locate offenders as well as victims. Another technology discussed was **chip-enabled phones which can receive beacons**. Similarly, the idea here is that public safety would be provided with this beacon information in order to understand positioning of persons of interest.
    - This group also talked about using location information to tag victims electronically. **Tagging with associated XYZ coordinates**, for example, could help public safety personnel account for victims and offenders, and track them individually. The Las Vegas shooting was identified as a real-life use case for this technology capability. In that circumstance, many victims were lying down, but some were deceased while some were not. Tagging buildings also came up during this part of the conversation. Specifically, the group discussed the possibility of tagging buildings and even individuals through a mapping app that could lay out the scene and allow users to simply "drop a pin."

- One area of concern regarding communication had to do with two-way call and response. When a person (potential victim) calls, the question remains: is it possible to tag his/her identity and status in one step? Currently, this is a two-step process for public safety, and there is a desire to streamline this technology capability.
- The group discussed having a readout of this information on a **situational dashboard**, which could be displayed through a phone. However, some in the group raised concern about the impediment or distraction of having to handle a phone. For example, members of a SWAT team cannot afford to take their hands off their weapons. Therefore, this group began discussing other technologies such as **voice, virtual reality, and augmented reality** as ways to communicate the needed information to first responders without distracting or impeding their mission.

- Other Thoughts Related to Tasks 8-9:
  - The group discussed the fact that **some of the tagging technology already existed** in other places, or at least it had the potential to exist with few developments on current products. Connectivity via **Artificial Intelligence** (AI) and how it could coordinate to building tags was discussed. Buildings may also contain **sensors** which are connected for room occupant analysis that describes the location, count, and movement of persons throughout a building to optimize energy conservation. This capability could be applied to public safety's need to route civilians and first responders through a building during an active shooter scenario. With AI, there is the potential to update and stitch together continuously what a user sees in real time. It was noted that this is currently being done with self-driving cars, which are able to update maps as they drive. Benefits to public safety would include knowing when a building model has changed - even during an incident (e.g., a window is broken, or a wall has fallen down). **Existing building sensors** could collect the information, and AI could be used for continuously updating the information in real time. Via this connectivity, participants said, incident personnel could stay informed via incident command or at the edge.
  - Other capabilities on the radar for industry included video surveillance cameras. This led to questions about a capability that would allow victims themselves to have a way to share video from their phones. Some participants offered that in a smart building, heat sensors or similar devices could be used to provide situational awareness as it relates to a perpetrator or victim. Group participants continued down this line of thought, leading to discussion about the idea of designing a sensor that might indicate whether a person was carrying a piece of heavy metal, such as a gun. The group also noted image analysis as **one of the most important technologies available** for a scenario such as this use case. Specifically, **sentiment analysis was mentioned as an existing way** to zero in on certain circumstances, such as whether a person is panicking or how many people are panicking. The group noted that **given the ubiquitous deployment of surveillance cameras**, it would be plausible for industry to provide this

technology. The group also talked about using traffic cameras to track not only cars but buildings, and using image analysis to view object trajectories.

- Commercial wearables were also discussed as a way of communicating vital situational information to public safety. This includes smartphone connected health monitors, and may soon encompass pulse, heart rate, blood pressure, etc. as ways of understanding who may be about to enter a state of shock. It was mentioned that **the FCC currently has this in the pipeline.**
- Finally, a significant portion of the conversation dove into the use of beacons. **Exit signs are currently being fitted with beacons and sensors to provide certain building information.** Additional sensors could be added in the same way to determine the concentration of people in a certain location related to the sign. The group discussed using beacons "out of the box" to determine not only concentrations of people but the distance between them. Eddystone (a Google product) and iBeacon (Apple)—which may provide global unique IDs for tracking purposes—were both identified during this conversation. For **more intelligent routing of information**, ArcAngel was identified as an app which could help provide two-way communications so **first responders could send messages through the building management sensors.** This app could allow individuals registered with the app to receive emergency alerts while located in a geofenced region and indicate whether they are "safe" or "unsafe" during the event. Despite these promising capabilities, attendees consistently expressed skepticism that first responders could reliably access and use information produced by building management sensors.
- As specific public safety requirements for implementation, the group listed the following:
  - Seamless aggregation of data from different cell carriers.
  - A catalogue of categorized information which could be secured from vulnerabilities
  - Reliability, accessibility, and accuracy
  - A map to inform occupancy status (outfitted for discovery of silicon and human assets)

The group then addressed task 10 of the use case, which reads as follows: "**All disciplines can control the Smart Building alerts** to communicate with victims on which exits are safe to use and where to stay hidden."

- Task 10 Technologies:
  - Group participants identified **indoor location** as the most important alert to receive in this use case scenario. They discussed receiving confirmation of the location then being provided arrows to tell them which direction to go. These arrows could be overlays in **online and offline maps**; the data would have to be **integrated so that it would be available in online and offline operational modes**. The group noted that when there is enough bandwidth, **they would want the map to update and upload automatically for seamless synchronization.** It was discussed that this capability of a real-time update

would help with identifying where the perpetrator was, as it is unlikely the offender would be in a static position.
    - **Personal area networks** (PANs) were also a focus of this group's conversation. The group spoke about a situation in which an incident commander designates a limited group of team members based on dashboard locations and data updates. People could then be added to the network as they arrive or be removed if their shift ends. **Geofencing or Wi-Fi connected to the SWAT team** was discussed as a beneficial technology which would push the data to FirstNet's wide area network. For this approach to work, the group discussed the necessity of a **mesh network** for each person to carry, yielding coordinated networks that would move data from sPAN to wide area networks. It was discussed that this capability could be in the form of **something deployable, something secure, and something sustainable**.
- Other Thoughts Related to Task 10:
    - In terms of whether or not these technologies were already on industry radar, the group discussed **Building Information Modeling (BIM), Haptics, and AI**. BIM is a process for rendering (design package) specific to buildings as a way of collecting building information - walls, windows, HVAC, sensors, etc. - to communicate with first responders. The issue is that BIM is still information overload for first responders. To address this obstacle, the group talked about leveraging AI to filter only the most relevant information to first responders which would aid in creating context for the incident. Specific cues were discussed, similar to **what is currently used in GPS** (e.g., "turn left here"). Besides vocal cues, haptic feedback was also discussed. However, the group agreed that all this future technology would be rendered useless if the network went down; first responders would always defer to their radios. Given this reality check, the group discussed whether AI capabilities could replace radios. The consensus was 'yes,' but if the output were inaccurate one time, first responders would never adopt it. The group noted that AI's false positives/negatives were a concern and, although AI might provide a confidence level with its outputs, that first responders would not have the time to assess calculations in the moment of response.
    - As for specific public safety requirements for implementation, the group discussed:
        - Indoor and 3-dimensional mapping
        - Recent and potentially hazardous materials identified

The group moved on to assess Task 11 of the use case which asked responders to "**assess and treat injured victims, then prioritize treatment of victims based on the available data**."

- Task 11 Technologies:
    - At this point in the use case, when public safety would be communicating (via 911 call) with the victim, if the victim were able to respond, the process would begin by identifying a warm body, identifying (via public safety answering point [PSAP]) that the person is in fact a victim, then starting the conversation of talking the victim through next steps. Ideally, this would be achieved by putting a

mobile instant-application monitor on the patient even before responders arrived on scene, whether via sensors, cellular devices, etc.

- Other Thoughts Related to Task 11:
  - In terms of technology currently on industry's radar, the group largely discussed **connecting standard APIs to different building operating systems,** including but not limited to lighting, a PA system, and Wi-Fi access points. The concern here was that the perpetrator would be receiving this information as well.
  - BACnet (a data communication protocol for Building Automation and Control networks) building data was also discussed briefly in this group, although it was noted that the technology does not cover elevators. If there were an app with an open API, there could be better coverage capabilities available; this could be an avenue for crowdsourcing safety. AED (automated external defibrillator) and standoff technologies were also briefly mentioned, but it was noted that a responder would have to be very physically close (within two feet) to know a person's status.
  - Finally, it was noted that **as sensors get cheaper and smaller, they could they be available to more people**, thus transmitting valuable information to public safety which would help in prioritizing evacuation and treatment.
  - Specific requirements discussed for public safety implementation included:
    - Abilities to marry sensor data with cellular data and even image/video data
    - An ability for changing the status, association, or relationship of sensor tracking. The group emphasized that first responders need to track resources rather than sensors and that as sensor assignment to resources changes, the identification of sensors also needs to change, accordingly.
    - Camera input. Together, object tracking in image, sensor, and mobile device data would be a benefit to public safety—for tracking victims as well as first responders.
    - Ease of Use
  - One point of concern for this group was who would have control of the data, and where that controlled data would live. Developing data ownership and control processes would be critical to enable public safety adoption of IoT technology in a Smart City environment. The group discussed use of **AirDrop** for public safety as well as a **virtual Knox Box**. For context, a Knox Box currently in use is a physical location that utilizes a box with a master key that can give first responders access to a building. The virtual Knox Box would allow first responders to connect to and communicate among systems within a building.

IoT Gap Identification—Comparing Current vs. Future State

Session Design

After collecting a list of operationally relevant technologies that would enable public safety IoT capabilities in a future Smart City scenario, attendees were asked to brainstorm what gaps need to be addressed to realize this future state. PSCR assigned both breakout groups several IoT enabling technologies identified in the previous session to begin identifying gaps.

In addition to identifying technology gaps in need of attention, participants were asked to describe specific action items or roles that both industry and public safety could assume to help address each gap. Breakout groups were instructed to aim for a total of about 10 total gaps. Before starting the session, PSCR provided attendees with guidance on what makes a good gap (an underlying technology in need of attention that is relevant, measurable, and specific) and examples of IoT-relevant gaps identified in the 2016 *PSCR Data Analytics for Public Safety Roadmap.*[10]

Discussion Points, Highlights, and Outcomes

The two breakout groups identified a total of 16 technology gaps that aligned with the enabling IoT technologies supporting the Smart City use case. The final, **non-prioritized** list of gaps that attendees felt warrant additional attention from R&D organizations supporting public safety IoT adoption include:

1	The lack of interoperability of dashboards between vendors
2	The lack of a fundamental definition of a level of information across “things”
3	The lack of a wireless location accuracy standard (x, y, z)
4	A need for a mechanism to communicate between smart buildings and first responders
5	The utilization of Artificial Intelligence as a service rather than an application feature
6	The ability for Artificial Intelligence to be extended accurately into complex measurements such as hyperspectral algorithms, facial id, object id, and physiological status
7	Lack of mitigation solutions for privacy policies
8	The cost of integrating tech into buildings prevents most owners from doing so
9	Need to promote interoperability between IoT devices that store data in siloed cloud databases
10	Mandate all IoT sensor data sent into public safety systems must have a timestamp (minimum vs. maximum granularity TBD)
11	Contextual information must be stored with IoT data to assign data to users, devices, other identifiers (sensors, cell locations) as it moves across systems
12	Develop regional and/or federal IoT data exchanges (database with APIs for local agencies to tap into)
13	Develop regional and/or national data classification schema for: type of event, role rank, data type to inform access levels

[10] https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1917.pdf

14	Link building infrastructure (communications, data, security) to building maps / diagrams
15	Geofencing to individual room or floor level not possible using existing CAD systems
16	Develop extensible, backwards compatible IoT data standards that can be added to by industry software developers

After briefly reviewing the gaps list, attendees were asked to prioritize gaps against one another using PSCR's investment criteria in the final session on day 1 of the workshop. A more detailed summary of both breakout group discussions, and the specific gaps they identified, is provided below:

Gaps Identified by Breakout Group 1

In breakout group 1, the group was instructed to identify gaps that aligned with the *Asset Planning & Management* technologies discussed earlier in the workshop. The first technology discussed in this group was a Bi-Directional Situational Awareness Dashboard.

This group first identified a gap in **interoperability**. They noted that a lot of work has been done for IoT in different silos, but public safety has not been the focus. An existing need would be a standards body or consortium (similar to the 3GPP). The group remarked that Google and others are not forcing the integration of sensors using standards (communications layer and data layer). Therefore, they would want the body to develop a standard that serves public safety, acknowledging that public safety practitioners would need to agree on what they want, and acknowledge that fire, police, and EMS have different priorities. Group participants specifically mentioned wanting a customizable dashboard.

Moreover, the participants in this group noted that public safety needs to do a better job of working with Smart City initiatives; currently these entities are not talking to each other. While for public safety, there are cost barriers to addressing IoT interoperability and standards, an opportunity exists to offset these costs by collaborating with Smart Cities. The group also noted that they should be talking about Smart Cities standards, since public safety standards are just a subset of that. Ideally, first responders would like to be able to **communicate with smart buildings**.

Another gap identified by this group surrounded both a **lack of standards**, and too many standards. An opportunity exists to **define further what "things" are** (e.g., a device, the device's condition) in IoT, and an IoT Alliance—similar to the existing Wi-Fi Alliance—was proposed.

Additionally, this group acknowledged that public safety has struggled with creating a value proposition for industry adoption. The reality of the first responder market is that it is fragmented. With industry, vendors push their own agendas to market. If there were a stronger market voice for public safety, that might make a difference in terms of feasibility. For public safety to succeed, the opportunity exists to find something that would also be a marketable

solution for industry. This group talked about using purchasing decisions as guidance for developing standards which could ultimately inform device requirements. There has to be a spending justification when it comes to standardizing CAD systems, and a requirement for certification against a standard would provide the best justification.

Another topic that came up in this group was a conversation around **AI services versus features**. One comment in the group was about how at some point adoption will be less about the individual technologies and more about the services a person is subscribed to. The group identified systems that currently use routing as a service versus proprietary routing (e.g., Waze); it was said that the gap with current CAD systems is the lack of integrated AI (i.e., routing decisions do not incorporate current traffic patterns as they would under Waze). The group agreed that implementing AI services on the local level will require moving away from current closed-loop CAD system designs.

In terms of tagging technology (devices used to identify places, people, or things with information relevant to first responders such as a victim's medical status, a cleared room, etc.), the conversation in this group highlighted a policy gap. The question was, "Who is the right entity to maintain the data, and who will take responsibility for it?" It was noted that geospatial companies are trying to be the authorities in this area. It was suggested that many ordinances grandfather in existing buildings, so that they do not have to comply with new communications standards. The group emphasized skepticism that businesses would feel incentivized about putting all this publicly-beneficial IoT technology in their buildings; the **cost to building owners** would simply be too great. This topic naturally highlighted concerns about **privacy** and risks that would need to be mitigated to an acceptable level. It was noted that many leading cities now are trying to minimize the PII they keep and only keeping what they need. It was also noted that 70-80% of departments are operating in small communities, so the capabilities of maintaining and protecting this data at that level may not be realistic.

With regard to video and image analysis, AI's gaps were the subject of discussion. For example, **AI cannot currently detect objects within thermal images**, whereas detection in millimeter wave images (e.g., airport scanners) is as good as in hyperspectral imaging. AI would need to be extended to data sets and measurements in order to obtain reliable vital signs. It was discussed that a lot of large cities do not implement facial recognition because of privacy concerns; although this technology has the potential to keep people safe, some vendors are saying they do not want to be associated with facial recognition because of the possibility of social backlash. In addition, the group discussed that some agencies would prefer taped video they could go back and review rather than receiving real-time video footage. This discussion again brought up the point about a policy gap.

The conversation in this group wrapped by discussing gaps in **standardizing building data**. One existing technology that reemerged was the idea of a virtual or electronic Knox Box. This is a capability used by realtors which could have public safety applications as well, if fire departments encouraged residents to purchase them. Ring video camera doorbells were also brought up during this conversation, eliciting natural concerns about privacy. The building owner

in each scenario would have to be confident that the technology was so secure that perpetrators could never get the information. Annunciator panels and VPN tunnels were also mentioned in this conversation.

Participants emphasized that for all of the technologies covered, the gap in standards was most glaring. At this point, the lack of standards translates to a lack of integration. This problem is especially evident in circumstances where interagency response occurs; typically, such scenarios involve each entity bringing their own gear. The group mentioned again that an autonomous body could make sense of all the differences. In addition, cost was another overarching theme; the group agreed that a large enough target market would have to exist to make the per-unit cost affordable for public safety.

Relevant IoT Gaps Identified by Breakout 2

Breakout Group 2 was instructed to identify gaps that aligned with *Online / Offline Communications* and *Roles & Access Policies* enablers discussed earlier in the workshop. The group identified Gaps #9-16 listed in the table at the top of this section. The following content describes the key Breakout 2 discussion topics for this session and may include 1) industry action items and 2) public safety action items that can begin to address this gap.

Interoperability and Proprietary Data Silos

The first responders in the group emphasized the importance of having the ability to monitor the status of firefighters and police simultaneously. Interoperability within and between company databases and government agencies would enable the public and private sectors to address public safety challenges together. Their communications systems should seamlessly facilitate exchanges between agencies and departments. “It is an easier problem to solve than the others - it is the most needed,” noted one of the group members.

Another group member noted that using middleware to facilitate exchanges is acceptable, but “bloated” middleware is not helpful.

Centralized IoT hubs for Data Exchange

The group members all agreed on the merits of a regional and federal “hubs” for IoT and sensor data. Ideally, government agencies would be able to decide which data they want to share, and with whom, within their departments. Users of regional and federal data hubs would follow data classifications for different types of events. All users within first responder organizations would be required to abide by hierarchical data access standards for different types of first responder roles.

IoT Data Standards and Timestamps

Language standards tend to be very skeletal. Public safety and industry need to develop extensible IoT data standards that are backward-compatible and able to accept add-ons or extensions from vendors. Vendors should be able to add special functionalities but still adhere to the same core standards expected in the field. A data language standards mandate should

be established by a trusted, capable, and respected agency such as FirstNet, which has the ability to codify and maintain such data language standards.

The agency also needs to develop a mandate specifically for timestamps. “All IoT sensor data sent to public safety systems must have a timestamp, and context information must be stored with IoT data,” explained a group member. Ideally, the sensor data will also provide context information such as the name of the first responder associated with the report, devices used to collect data, cell locations, and other identifiers.

As the group discussed, every mandate requires a funding source. Future discussions about IoT data standards and timestamps should include the topic of funding for mandates and its potential sources.

IoT Building Data
There is a lot of information stored in schools, hospitals, etc., but if public safety is not a regular user it will not be useful to the responder. Responders need dedicated systems and people within emergency response teams to build and follow protocols. The person who is responsible for building data is a key person in the response effort and should train in collaboration with other building employees and local first responders. Such persons should always be included in routine exercises. Sometimes public safety agencies do not bring in every player, and advances in data utilization are impeded.

IoT Gap Prioritization and Results

Session Design

PSCR has used a common set of investment criteria to evaluate and prioritize potential R&D investment areas since the commencement of its technology road mapping process in November 2013. Given that PSCR has emphasized using a consistent, repeatable planning methodology in past R&D summits, the IoT research team asked attendees to prioritize the 16 gaps identified during this workshop against three criteria: 1) Impact to public safety, 2) Feasibility, and 3) Cost effectiveness. PSCR designed a session in which each attendee received poker chips that corresponded to the three criteria. Three chip colors corresponded to the three criteria, and each chip was labeled with a score value of 1, 2, or 3 (with 3 being the highest positive rating). PSCR reviewed the gaps list with all attendees who assigned each gap a 1–3 rating for each criterion. PSCR also allocated a priority weighting to each criterion that signified that impact to public safety was the highest priority criterion, followed by feasibility, and cost effectiveness as the lowest priority criterion, but still important. The definitions for all three criteria are provided below:

1. **Impact to Public Safety (50% Relative Importance):** *the transformational and wide-ranging positive effects a new technology would have on public safety operations. Impacts can be measured in improvements in common good, response effectiveness, and overall public safety.*

a. Example: If addressed, which gaps would most positively impact the day-to-day operations of public safety?

2. **Feasibility (33% Importance):** *the probability of a successful return on investment in light of current or anticipated trends, drivers, or technical enablers.*
   a. Example: Which gaps have the highest likelihood of being addressed within public safety operational settings?

3. **Cost Effectiveness (17% Importance):** *the overall cost of investment to address gap and cost of ownership required to operate supporting technologies.*
   a. Example: Which gaps can be addressed with the least cost burden to public safety agencies and the surrounding R&D community?

Discussion Points, Highlights, and Outcomes

Attendee ratings of each gap per criterion were aggregated and then multiplied by the criteria priority weights to produce an overall weighted score for each gap. The results and reactions to this prioritization exercise are listed below in descending order of total score (highest to lowest priority):

	GAP LIST	TOTAL SCORE	Feasibility	Impact Score	Cost Score
1	The need to promote interoperability between IoT devices that stores data in siloed cloud databases.	48.03	40	53	49
2	The lack of a wireless location accuracy standard (x, y, z).	44.31	46	45	39
3	Contextual information must be stored with IoT data to assign data to users, devices, other identifiers (sensors, cell locations) as it moves across systems.	43.53	37	47	46
4	Develop extensible, backward compatible IoT data standards that can be added to by industry software developers.	42.2	36	45	46
5	Link building infrastructure (communications, data, security) to building maps / diagrams.	42.04	36	44	48
6	Mandate that all IoT sensor data sent into public safety systems have a timestamp.	41.12	50	37	36

	GAP LIST	TOTAL SCORE	Feasibility	Impact Score	Cost Score
7	Develop regional and/or federal IoT data exchanges (database with APIs for local agencies to tap into)	40.55	34	42	49
8	The lack of a fundamental definition of a level of information across “things.”	40.47	42	42	33
9	A need for a mechanism to communicate between smart buildings and first responders.	39.86	38	39	46
10	The ability for AI to be extended accurately into complex measurements such as hyperspectral algorithms, facial ID, object ID, and physiological status.	39.66	40	40	38
11	The lack of interoperability of dashboards between vendors.	39.39	30	43	47
12	The utilization of AI as a service rather than an application feature.	39.33	42	37	41
13	Develop regional and/or national data classification schema for event type, role rank, data type to inform access levels.	38.64	42	38	34
14	The cost of integrating tech into buildings prevents most owners from doing so.	38.18	35	40	39
15	Geofencing to individual room or floor level is not possible using existing CAD systems	30.82	32	31	28
16	Lack of mitigation solutions for privacy policies.	28.53	25	29	34

PSCR presented the prioritization results to attendees as a group and asked for their reactions on the outcome. Clarifying questions and answers filled the conversation at first. Then, one participant voiced surprise at seeing Gap #2—the lack of a wireless location accuracy standard (x,y,z)—ranked so highly. In response, however, several attendees explained that they valued this gap due to the urgency in addressing false-positive locations from wireless 9-1-1 calls. Others chimed in that standardizing x and y measurements alone would alleviate many of the great pains in locating victims and that pressurized building systems can assist in determining the z measurement to identify locations of victims and responders in multi-story structures. After closing discussion around Gap #2, another participant shared concern with Gap #14— the cost

of integrating technologies into buildings prevents most owners from doing so—being so low on the list. Attendees acknowledged in response that developing more affordable solutions is also urgently needed; one participant recommended that PSCR contribute to combating high cost by publishing more research, noting that competition around patents often causes expensive solutions.

Before moving on to the next session, participants finally began organically suggesting logical groups of gaps within the priority list. Attendees suggested that Gap #2 (lack of a wireless location accuracy standard), Gap #5 (link building infrastructure to building maps and diagrams), and Gap #15 (geofencing to individual room or floor level is not possible using existing CAD systems) all revolved around location. The group developed consensus that when identifying solutions during the next session, they could link these gaps together in their architecture. The other cluster of gaps included Gap #1 and Gaps #3–8. These gaps were identified as similar in that they all pivot on defining standards and architecture, even if only from a different perspective. Armed with a new natural organization to the gaps list, attendees were released from this plenary session and invited to rejoin their breakout groups one final time to begin designing solutions.

End-to-End Solution Brainstorming for Priority Gaps

Session Design

After prioritizing the key challenges that responders face as they begin to take advantage of commercial advances in IoT hardware and data science, PSCR asked attendees to brainstorm *system-level* approaches to address **multiple gaps**. PSCR defined “end-to-end” solution as *how a user interacts with IoT hardware and data from the edge to central processing and user interface.* The opening breakout discussion on Day 2 demonstrated significant attendee expertise, as they were asked to incorporate the following considerations into their solutions:

- Hardware / software capabilities that need to be developed to process IoT data (new or existing prototypes)
- Network management and operations (how to manage different applications/users on the network?)
- Network architecture (how to design network topology?)
- Edge computing, sensors and data processing capabilities (how to store and process data locally vs. core?)
- Protocols and Standards (how to ensure interoperability between different systems, jurisdictions, and users?)
- Security / ICAM capabilities (how to secure the network or authenticate users?)

After brainstorming standalone approaches for addressing multiple high-priority gaps, attendees

were asked to consider any differences between commercial and public safety implementations of the solution identified. The resulting data added to PSCR's running list of next generation, public safety-specific communications requirements. A breakdown of stakeholder-identified approaches to address multiple gaps is provided below.

Discussion Points, Highlights, and Outcomes

Breakout 1 End-to-End Solutions:

Solution 1: To address Gaps #2–8, Breakout Group 1 proposed a **Network of Sensors, with an Open API Model, Regulated and Standardized by an IoT Alliance.** This solution would replicate the current Wi-Fi Alliance for IoT, as an organization which would enforce compliance and certification for public safety IoT products while IEEE writes the standards. They noted that this solution could not be isolated for public safety; 99% of the solution could apply to IoT for other sectors, and just 1% of the solution could address public safety needs to encourage buy-in and development by commercial vendors. For this solution, standard authentication such as ICAM would be required as well as an Open API for mandatory data requirements. The group discussed an API with the following capabilities: 1) transport protocol; 2) data encoding, and 3) interfaces for querying the data. To create a framework that would be valuable, the group agreed that the data standard would be required for both input to and output from the dashboard; there has to be a standard for the box in order for people to invest in it.

As this group developed their solution model, participants began to draw on existing infrastructure that could be used as a reference for their solution. One participant mentioned DARPA's Ocean of Things as a model, explaining that the Department of Defense gets automatic updates to online and offline maps on its iPads, which is the benefit of incident-level IoT distribution. After discussing how the group could apply DARPA's model to their IoT solution, such as first creating an API before creating the hardware (in this case, sensors), geospatial standards were introduced as an example of the concept. With geospatial standards, a majority group often must agree how they share their data. This type of approach would not be an end-to-end solution, but rather an open API model that others could discover and connect with via domain standards that the proposed IoT Alliance created (as related to connecting the core).

As a segment of this discussion, the group also noted which critical sensors for public safety operations must integrate with their open API. The sensors mentioned included body-worn cameras, smart clothing and bandages, patient monitors, and firearm holster sensors. They acknowledged that companies should not stretch to build an end-to-end solution, because it requires a focus on developing the elements they cannot develop, like dashboards. They should instead focus on their core competencies which should interact with a dashboard to make up an end-to-end solution with parts that communicate. The group cited BACnet as an example. They also discussed the technology being used in smart homes, mentioning, however, that much of it was proprietary. That said, there could be the option of adding new solutions to proprietary

technologies. The U.S. Army's Communications-Electronic Research, Development and Engineering Center (CERDEC) has added new solutions to proprietary technology. One of their programs is Multi-Access Cellular Extension (MACE), which bridges communications between Wi-Fi, 4G LTE, and tactical systems to provide connectivity to field teams. One attendee familiar with the center stated that CERDEC offers 49 sensors to which cleared vendors can add their proprietary, web-based offerings. CERDEC has built an IoT controller and developed a process to regularly update the controllers. Today, the 49 sensors are limited to military purposes, but there could be an option for the public safety R&D community to leverage these military capabilities for enhanced IoT sensor integration.

Solution 2: After exhausting ideas on the initial solution, the participants shifted their focus to a second solution targeted at addressing Gaps #2, 5, and 15 in which **public safety organizations would conduct indoor mapping during the pre-planning process,** such as that which is being explored through PSCR's investment in a LiDAR backpack and Point Cloud City research grants/cooperative agreements. They ventured that data from pre-planning could be brought into GIS to conduct regular updates. First responders could then communicate changes in interior building structures via wearables worn during the incident. The group discussed the possibility of first responders bringing in their own mesh network for this hypothetical scenario. The group also discussed how this data could be used; Pix4D was noted as a tool already in use for displaying mapping data, but its drawback is that it cannot be manipulated (e.g., rotated) to provide comprehensive views when warranted, such as to identify a riser room, hazardous material, an alarm panel, etc.

It was noted by the group that 3D indoor mapping would be difficult to implement in the US because, in some municipalities, it is apolitically hot button issue; adoption will likely be slow. That said, the group felt that this was the better alternative to expensive geospatial data. The group noted that indoor map data could be crowdsourced by citizens, but that this option might run into privacy and security issues. Accordingly, the group entertained a second option of asking citizens to allow firefighters to map for them. The advantage to mapping conducted by fire marshals would be a rendering that is trusted by public safety. However, fire marshals would have to be committed to this concept and new responsibility. PSCR staff let the group know that their newly launched Tech to Protect Challenge was serving to address some of these obstacles as well by asking coders to develop an application that would make it easy for citizens to map and annotate their own residences for future emergency scenarios. The group concluded this discussion with an agreement that there would have to be some consumer benefit in order to get people to opt in; the benefit should not be solely for public safety, since that is not as scalable. Private 3D mapping companies were considered, but group members expressed concerns around relying on the private sector to make their data publicly available.

To ease this notion of marketability, the group brainstormed ways that indoor mapping might appeal to a buyer audience. Realtors and commercial real estate companies were introduced for their use of sensors to understand the flow of people and room occupancy. The group considered the possibility of piggybacking on these capabilities and standardizing them, noting that any type of smart building would have some sort of sophisticated sensors, although they

would vary due to the lack of standards. It was noted that commercial solutions are already in use for connecting with building systems in order to optimize energy savings. The group agreed this concept could one day apply to the public safety market.

After working their way through the concept of an indoor mapping solution, this group began to identify the individual components that would comprise it. Ultimately, the group decided that a sort of **virtual Knox Box**, to which first responders could connect, would allow first responder applications to communicate with buildings and internal systems. The Knox Box would require backup batteries and ruggedizing to accommodate high temperatures, fire, and water damage that could occur during an emergency event. The group considered that one centralized location for data processing might not be accessible during disaster recovery, and that data centers should be replicated for backup storage elsewhere.

Sensors that interact with the virtual Knox Box should include biometric and physiological sensors, occupancy and motion sensors, localization of persons, and thermometers. The group emphasized that most critically, responders need to know how many people are in a certain area, how many people need to be rescued, and how viable a rescue is. They added that historical data from motion sensors could help detect the scale of an incident as well. The group realized that occupancy intelligence is the solution they want from sensors, but that mapping data would need to precede this sensor input. One approach to achieving this capability would be to accept data from any sources already available (e.g., open source, digitized plans) before seeking an active mapping solution somewhere down the line (via public officials, cameras, etc.). They agreed that the occupancy data should cover time periods before, during and after the incident, expecting to combine this information for maximum awareness. The group then discussed the idea that this approach could be attractive for industry and gave the example of Coca-Cola wanting to know where to put their vending machines in a given building. Similarly, the group suggested shopping malls might track movements to lease their spaces accordingly. Monetizing this capability could be a win-win with investors. It was noted that Knox Boxes could allow for this type of data to be extracted and that the software could perform an inventory of people before or after an event. The Kennedy Space Center was noted as an example of where this is currently being done (pre- and post-launch). RFID technology was also offered as an example of commercial technology that could help first responders in this area.

In summary, this group discussion began with an abstract idea of a virtual Knox Box solution with a common API that could provide responders with access to mapping data on scene, integrated with applications which would provide real-time updates from building sensors, responders and citizens. The group agreed that the foundational aspect of the solution surrounds discovery and identification of resources available for first responders in a given scenario. The second piece is managing the data and defining the interface (API) with the virtual Knox Box. Much of the conversation from this breakout supported the current PSCR IoT Testbed Architecture. During the closing session, participants noted several components aligned well with the architecture that was presented for feedback.

Breakout 2 End-to-End Solutions:

Given the focus attendees afforded interoperability and standards development during the gaps prioritization exercise, this breakout group discussed the possibility to develop **common public safety data classification standards.** After emphasizing the importance of standardizing the units of measurement, indexing processes, and using object-oriented software models for public safety, the breakout took a step back to brainstorm an **IoT data processing model for public safety** as described below:

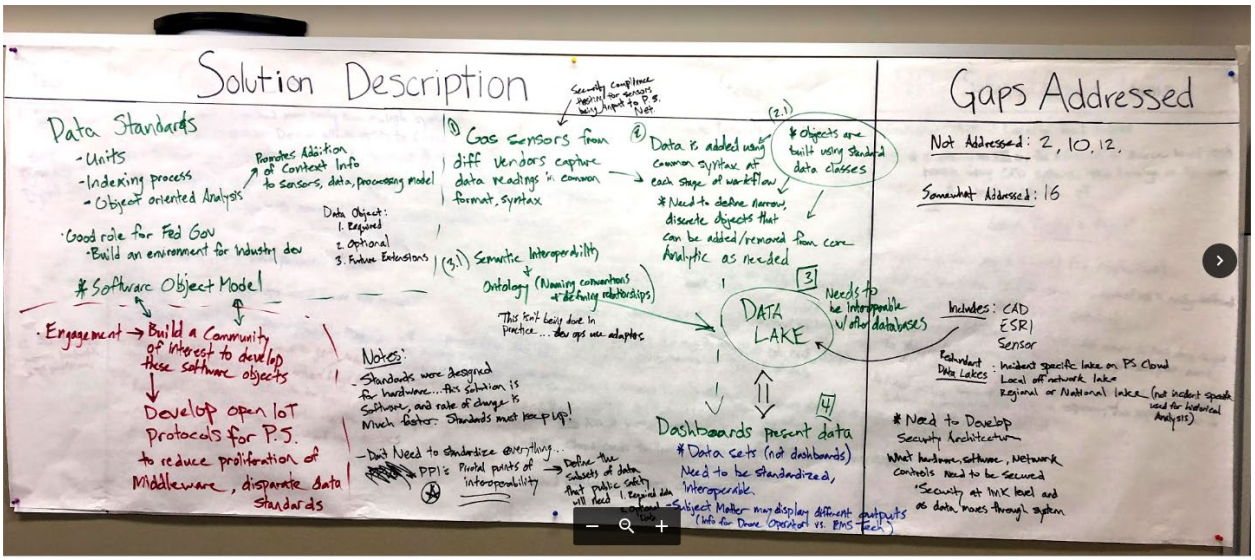
1. Environmental sensors (e.g., in-building barometric or noxious gas sensors) from a variety of vendors ingest into public safety analytical models in a common readable format and syntax.
2. Interfaces continuously add disparately formatted data from a wide variety of sensors to the analytical model as the information moves from edge sensor to user. As data moves through this public safety workflow, it remains imperative that a common classification is used to facilitate efficient object-oriented programming. This classification enables analytical models used at one public safety agency to scale models more easily for ingesting new information and to redeploy effective models in other agencies at negligible cost.
3. Intelligence is transferred to a 'data lake' (centralized database for agency-wide analytical processing that can be selectively tapped into by third parties such as building owners, network operators, and citizen witnesses) that is fully interoperable with third-party databases or APIs (owned by entities such as commercial building tenants, a transportation authority operating around event scene, and social media carriers offering nearby sentiment analysis).
4. Fully-enriched IoT analytic data moves from data lake and to the first responder through a display interface that is optimized for usability supporting his or her response task.

Attendees emphasized that datasets—not dashboards—need to be standardized. Given the immense scope of response tasks, dashboards should be customized to meet the unique usability needs of responders such as wildfire rescue, drone operators, urban SWAT, and Emergency Medical Technicians (EMT). Rather than specifying individual applications, R&D organizations should investigate how to facilitate the aggregation and formatting of disparate IoT datasets into shared repositories for public safety agencies to leverage as needed. Furthermore, R&D organizations should train agencies on how to do this effectively and securely with limited resources.

Attendees supported the idea of developing a catalogue of sensors to help public safety workers determine which type of sensors to deploy in which contexts. Such a guide would tell first responders about data standards for sensors and provide the names and agreed-upon indexes for temperature, pressure, and other measurements.

To standardize data interoperability, the group recommended standards writers establish "pivotal points of interoperability" (PPIs) as required features of all interfaces. Data standards

would categorize features as required, optional, or able to be added in, allowing for more flexibility for end users to define their own dashboards. “If initial software objects are well-defined and clustered correctly,” explained one attendee, “a PPI system could be very useful to public safety.” To establish PPIs for data interoperability, data standards writers will need to identify subsets of information that will be considered critical. A best practices document would provide valuable guidance for what public safety data operators need to add at each stage of processing workflow while considering security at every step. Below is a graphic that depicts the IoT data processing workflow brainstormed by Breakout 2.

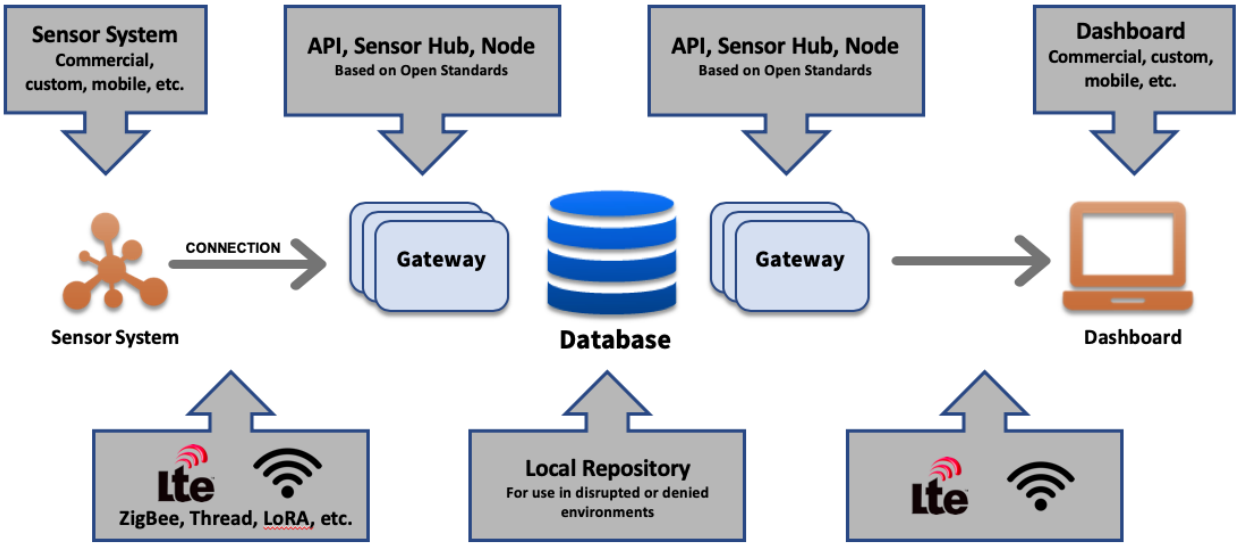


Demonstrate and Collect Feedback on PSCR IoT Testbed Architecture

Session Design

Measurement science, standards and technology are key elements of NIST’s mission. Within NIST, PSCR works to drive innovation and advance public safety communications technologies through cutting-edge research and development. With support from the Department of Homeland Security (DHS), Science and Technology Directorate (S&T), PSCR intends to create a framework where PSCR and its stakeholder community can experiment with concepts, demonstrate advancements and document the benefits of using the Internet of Things in the most demanding public safety use cases.

PSCR’s initial testbed architecture (illustrated below) attempts to address public safety-specific issues (such as limited network connection availability during an emergency event) by housing the testbed on a deployed network with only local connectivity. Future modifications to this testbed will enable PSCR, industry, and public safety stakeholders to collaborate more effectively on future IoT product and service development. Experiments will be designed using data collected during this workshop.



Discussion Points, Highlights, and Outcomes

To design IoT experiments that closely align with public safety's highest priority needs, PSCR briefed attendees on the draft testbed architecture pictured above and solicited feedback on how it could be improved. In addition, PSCR invited attendees to provide detailed input on each testbed component (Sensor Systems, Gateways / Databases, Connectivity, and Dashboards) using a common set of questions:

- **Technologies to Evaluate:** *What solutions could be brought to an IoT test bed?*
- **Goals and Measurement Approaches:** *How could R&D organizations best evaluate the effectiveness of these IoT capabilities?*
- **Key Performance Indicators:** *What metrics indicate the success, effectiveness, or lack thereof for capabilities brought to the testbed?*
- **Challenges to Consider:** *What challenges may arise when testing identified technologies?*

PSCR encouraged attendees to focus on the components and questions around which they were most interested. PSCR intends to reference input from this and other workshop sessions for direction in continued development of the IoT testbed for public safety. Attendee feedback on the potential IoT testbed is documented in the following tables:

Sensor Systems—*The end-devices in an IoT solution which provide data and / or any corresponding microprocessor which modifies the data before distribution.*	
Technologies to Evaluate	• Passive infrared sensors (for occupancy or people in a room) • Eddystone and beacon devices/ beacons • Hyperspectral imaging • Millimeter wave as part of 5G and/or high frequency location based sensing solutions

	• Trusted Execution Environment (TEE) • Gas, chemical, biological, radiological, environmental, physiological, location • Stand-off (non-contact) physiological sensors • Establish a software-based public safety IoT (version 1.0) to include data structure definition and API library—do this using today's off-the-shelf sensors, such as physiological, gun-holster, chemical, and other public safety related sensors. • Non-intrusive occupancy sensors • Sensors and alerts required by Public Law 116-9 (enacted March 12, 2019), Section 1114 (Wildfire Technology Modernization)
Goals & Measurement Approaches	• Ability to interface with 9-1-1 center/emergency communications • Common data format • Sensor to sensor communications and APIs • Dynamic orthogonal sensor communication • Understand how to integrate sensors to gateway • Back-channel to configure the sensor
Key Performance Indicators	• How easy to plug a sensor to a gateway via an open standard and start working (degree of plug and play)? • Ease of integration with gateway, e.g., level of effort • Battery lifetime • Sensors that can operate at high ambient temperatures (~350 degrees)
Challenges to Consider	• When defining "sensors," does public safety really understand the scale and volume of information this represents? • Non-standard interfaces • Getting manufacturers to standardize sensor outputs • Biometric sensors that work with dirty, wet, hot patients

Gateways and Databases—*The middleware processing and storage entities in an IoT solution.*	
Technologies to Evaluate	• Add public safety intelligence • Determine server and database necessary to support a local repository • Ingestion services especially for public safety IoT • Distributed computing • Commercial gateways and solid state computing • Datastream management systems (DSMS) • Hybrid architecture of public cloud tools, e.g., AWS IoT core, AWS Lambda and Local Systems • OGC: Sensor Things • CityGML (OCG City Geography Markup Language), Indoor GML, GeoPackage, OGC 3D Tiles

	• Hadoop data lakes

Goals & Measurement Approaches	• Goal: integrate into hand-held radio
	• Goal: sharing "events" in space and time among different apps (dashboards, AI, AR/VR)
	  ○ Sensor observation
	  ○ Alerts
	  ○ Tasks
	• Establish a framework for developing 3D building database
	• Goal: configure gateways via phone or tablet web interface
	• Multiple meshed gateways that can come on/off network dynamically
	• API/ Service Database standards in addition to context and data schema standards
	• Identify if there is a practical means to create a local data store
	• Self-synchronizing
	• Map distro—building data access

Key Performance Indicators	• What would be the "minimum, but useful" set of data, so that various public safety agencies can have a common operating picture? • Ease of deployment; rugged ability
Challenges to Consider	• Continuous integration • So many options already exist—what *should* the standard be? • On-responder local pattern recognition across worn and nearby sensors • Determining synchronization techniques with the agency

Connectivity—*Protocols or interfaces through which data travels in an IoT solution.*	
Technologies to Evaluate	• Assess existing building's communications network (Wi-Fi, ethernet, LTE, etc.) to enable indoor/outdoor sensors for two-way communications • Provide a mesh network to enable IoT sensor communications—inside a building, campus, or office park • LTE-M vs. NB-IoT • NB-IoT • 5G & mmWave • Hardwired Bluetooth • Ultra-wide band • Mesh networks with multiple LTE connections/gateways
Goals & Measurement Approaches	• Provide a secure method for connecting sensors to a cloud server • Ability to interact/interface with 9-1-1 center / emergency command • Self-healing, self-provisioning mesh network • Minimal responder setup • Data format standards (object-oriented)

	• Assess ease of turn-up and ability to integrate data into gateway • Connectivity between sensor and gateway and between gateway and dashboard should be a two-way arrow • Back-channel configurability • Single SSL certificate server
Key Performance Indicators	• Data Availability • Ease of connectivity, level of effort to make operable • Maximum range • Maximum # of hosts • Power consumption required to stay connected
Challenges to Consider	• Deep indoor • Regulatory • Too many options • Expanding incidents • How many nodes/ channel • How many channels supporting • Redundancy and avoiding net overload • Implementations may be very proprietary • Optimizations for narrowband protocols

Dashboards—*The visual or other interface by which the sensor data is presented to the end user.*	
Technologies to Evaluate	• Xamarin (cross platform software development) • Fail safe mechanisms from database to backend and dashboard
Goals & Measurement Approaches	• Sharing the same view (including symbology) among different dashboards • Validate ability to filter data to declutter views • Intuitive, simple user-driven design • 3D indoor location and visualization • Symbology standards • Ability to interact or interface with 9-1-1 central communications • End user created dashboards • Relevance • Single pane of glass • Rapid swarming—speed of classification • Discovery services—what is out there?
Key Performance Indicators	• Mass adoption metrics • Usability • Reliability • Ability to set alerts and thresholds so if, for example, heart rate exceeds 150 an alert is generated • Dashboard user must be able to filter sensor data to meet the

	needs of the incident response, and also to check the status of sensors (operational or not working, etc.) and time stamp
Challenges to Consider	● Interoperability and vendor engagement ● Responder buy-in (police, fire, EMS, EOC) ● User issues in challenging settings or circumstances ● Dashboards may need hands-free or eyes-free user interface ● Ease of configurability ● Conflicting needs (PD vs FR vs EMS vs OEM) ● Integrating real-time notifications ● Bring mode of operations back to responders, source (architecture is one-directional right now) ● Sensors and alerts required by Public Law 116-9 (enacted March 12, 2019), Section 1114 (Wildfire Technology Modernization)

Discuss Opportunities to Improve IoT Data Access and Exchange Between Industry and Public Safety

Session Design and Highlights

PSCR chose to close the workshop with an open-ended plenary discussion that enabled attendees to reflect on the data and conclusions reached during the previous two days and think big-picture about how PSCR could facilitate improved data exchange between industry and public safety. Attendees were invited to bring up topics not previously discussed, or further elaborate on the importance of technical details related to gaps and solutions identified earlier. PSCR used a series of prompts to collect final thoughts from stakeholders related to three themes.

Sensor Data Needed by Public Safety: There is a need to develop discipline-specific sensor data handbooks or dictionaries that summarize the key data attributes for sensors used in law enforcement, fire service, or emergency medical services. Attendees noted that there is a robust community of first responders from all three of these disciplines that would participate in an effort to document the sensors used during common use cases and compile the data types and formats used by these sensors into a shared glossary. R&D organizations supporting public safety should tap into existing channels (NPSTC, PSAC working groups) to improve understanding of data classification efforts currently underway or already completed. Emergency managers and incident commanders would benefit from having access to each discipline's IoT data glossary, and solution architects would benefit from systems and data processing models that interoperate with fire, law enforcement, and EMS sensors.

Attendees also recommended that industry or government issue a formal survey to first responders to learn what sensors and data they would need to access. Attendees noted that several data cataloging efforts have taken place to date that the R&D community can build

upon. These include *Standard 950 for Data Development and Exchange for the Fire Service* developed by the NFPA[11] and the *Project Responder 4* effort sponsored by DHS S&T FRG.[12]

IoT Tools Available Today that Apply to Public Safety: Attendees saw great potential in public safety's ability to leverage existing intelligent routing software (e.g., Waze, Google Maps) together with meteorological data provided by outlets such as the National Weather Service. This capability would optimize the type of vehicles and route taken to an emergency weather event (e.g., flood) depending on the storm path, height of vehicles, image / video analysis, and other factors.

Attendees also saw significant value in developing a "virtual Knox Box" that would enable owners of building, environmental sensor, or other IoT data to selectively allow responding public safety agencies to tap into their databases during emergency events. After an event concludes, the data owner could remove access from responding agencies if the data were sensitive or no longer relevant.

Data Sharing for Interoperability: Attendees closed with a discussion on the impediments created by agencies' refusals around sharing data. While understanding that jurisdictional or geographical boundary-separated data is oftentimes separated due to criminal investigations and privacy concerns, attendees expressed the need for governance structures to facilitate future data sharing. Some participants wondered whether agencies could be incentivized to share data by creating dual-purposed data stores. If data has multiple uses for public safety and independent users, agencies might be more open to exchanges. Suggestions came up for integrating data sharing into insurance policy requirements and rewards or tying it to grants that include requirements for open data sets. This closing comment left PSCR with an area to consider for future grant awards.

[11] https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=950
[12] https://www.dhs.gov/publication/project-responder-4

Conclusion

PSCR intends to publish the findings from this workshop to the PSCR website for public download and review. They mean to consider all event data while continuing to develop the current IoT Testbed Architecture and will course correct as informed by workshop discussions. Using several new leads introduced by participants, PSCR will review opportunities for resulting research initiatives, whether executed internally in existing focus portfolios or launched in a prize challenge to inspire industry partners. PSCR considers the output from this event invaluable and looks forward to engaging with workshop participants—and other stakeholders looking to support public safety's future use of IoT capabilities—at future events.

Contact Alison Kahn (alison.kahn@nist.gov), Sam Ray (samuel.ray@nist.gov), Marc Leh (mleh@corneralliance.com), or Brianna Vendetti (bvendetti@corneralliance.com) for more information on this workshop and future opportunities to engage with PSCR.

Appendix 1: Smart City IoT Use Case

Active Violence in a Commercial Building

This use case represents an active violence scenario in a high-rise commercial office building in the Washington D.C. metro area. For this use case, it is assumed that smart city technologies are deployed within the city for public safety access and operation, including, but not limited to an integrated IoT-enabled transportation infrastructure, building control systems, autonomous vehicles, and wearable devices. It is also assumed that law enforcement and D.C. SWAT respond to the scenario to identify and detain the shooter, emergency medical services respond to assess and treat injured victims, and fire responds to rescue trapped persons and provide resources and assistance, such as pre-captured building maps. The commercial building is centrally located near public transit systems and is highly populated.

Pre-Event Tasks

The D.C. 911 Call Center receives one, then several, then overwhelming calls and texts from employees and the friends and families of employees working in the Randall Center, a high-rise commercial office building in downtown D.C. Police, SWAT, Fire, and EMS are deployed and (1) **travel to the scene in emergency vehicles**, some of which host V2X communications technologies. After interacting with various transportation infrastructures, departments (2) **arrive on the scene and establish the area perimeter and incident command**. Each jurisdiction comes prepared with their shared radio devices, wearable technology, and pre-planning resources. SWAT and police turn on and begin (3) **authenticating communication devices and access Smart City cyber-physical systems** such as building sensors. Fire locates and (4) **accesses their most recent in-building map** and shares it with the SWAT team.

During Event Tasks

Police begin victim and witness interviews to (5) **collect orienting information about the identification and location of the perpetrator(s)**. While referencing building and personnel records, and security systems, they (6) **transmit updates to the SWAT unit** (that has since taken post at building exits) **and to central command.** Responders continuously (7) **receive situational awareness information** from others on scene and incident command. After the unit confirms the identity and location of all perpetrators, (8) **all responders receive an alert to the location of offenders and possible victims**. SWAT responders confirm receipt of this message and (9) **coordinate a response to the location point of interest**. In coincidence with internal communications, responders on the scene interact with trapped victims to provide them direction and minimize trauma. (10) **All disciplines can control the Smart Building alerts** to communicate with victims on which exits are safe to use and where to stay hidden. As survivors escape the building, emergency medical response (11) **assess and treat injured victims, prioritizing treatment of victims based on the available data**. Each discipline is able to (12) **connect to building systems and share accurate, real-time information about the building HVAC and electric status**.

Post-Event Tasks

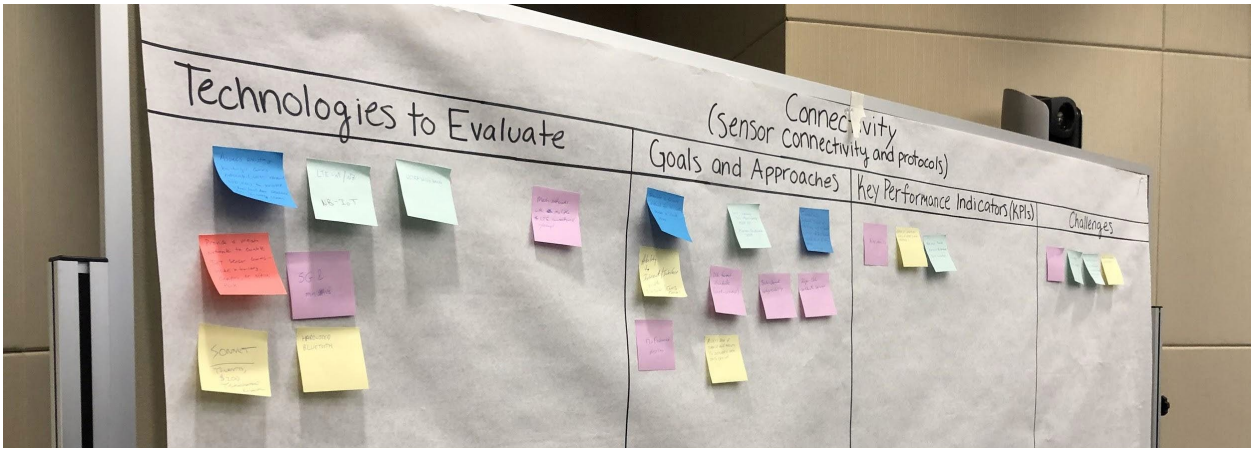
SWAT detains the two perpetrators and alerts all scene responders and center command. EMS begins **(13) transporting victims to emergency care, optimizing routes based on traffic, hospital capacity, and injury severity**. Police continues capturing victim and witness statements and creates a record of the event and response for their after-action report. Incident command **(14) returns the Smart City / Building cyber physical systems to a "neutral" state and returns control of the smart city systems to their proper authorities**.

Environmental Parameters for Consideration:

- A "high-rise" building is defined as at least 7 stories tall. Assume that the building includes an underground parking garage and a limited perimeter of mixed indoor / outdoor spaces at ground level that can be used to set up incident command upon arriving on the scene.
- The building is made of dense, heavyweight materials (thick concrete, glass) that may inhibit outdoor-to-indoor RF signal penetration. The downtown location of building also implies responder communications must operate in a high-density urban canyon communications channel.
- Assume that each floor contains multiple IoT devices that monitor and control building activity (temperature, foot traffic CCTV video, utility controls) that responders can leverage during emergency.
- Assume office floor plans vary at different floors of the building, but that utility placement (electrical, elevator, water, HVAC lines) remains consistent across the entire structure.
- Assume that multiple wireless capabilities are in place, including widespread next generation wireless network capabilities (5G and beyond), in the building and throughout surrounding city. As a result, high bandwidth components such as broadband or fiber will need to communicate seamlessly with ad-hoc deployable networks, sensor networks at the edge, and high-performance data servers to create an exceptional wireless experience for first responders.
- Building also features network infrastructure that supports communications transmission (voice, text, social media, video recording) from people inside. Assume that responding public safety agencies are responsible for ensuring interoperability with in-building network components, commercial networks (core and distributed high-frequency endpoints installed in surrounding city), and public safety networks from different jurisdictions and disciplines.

Appendix 2: Workshop Photos

PSCR utilized poker chips in an activity where participants prioritized the list of technology and standards gaps inhibiting public safety from currently realizing IoT commercial solutions.



Participants provided feedback on the PSCR IoT Testbed Architecture in a sticky note exercise.

Several existing resources such as the DHS Next Generation First Responder Handbook, NFPA Standards, and prior PSCR Roadmaps were available for attendees to reference during the event.