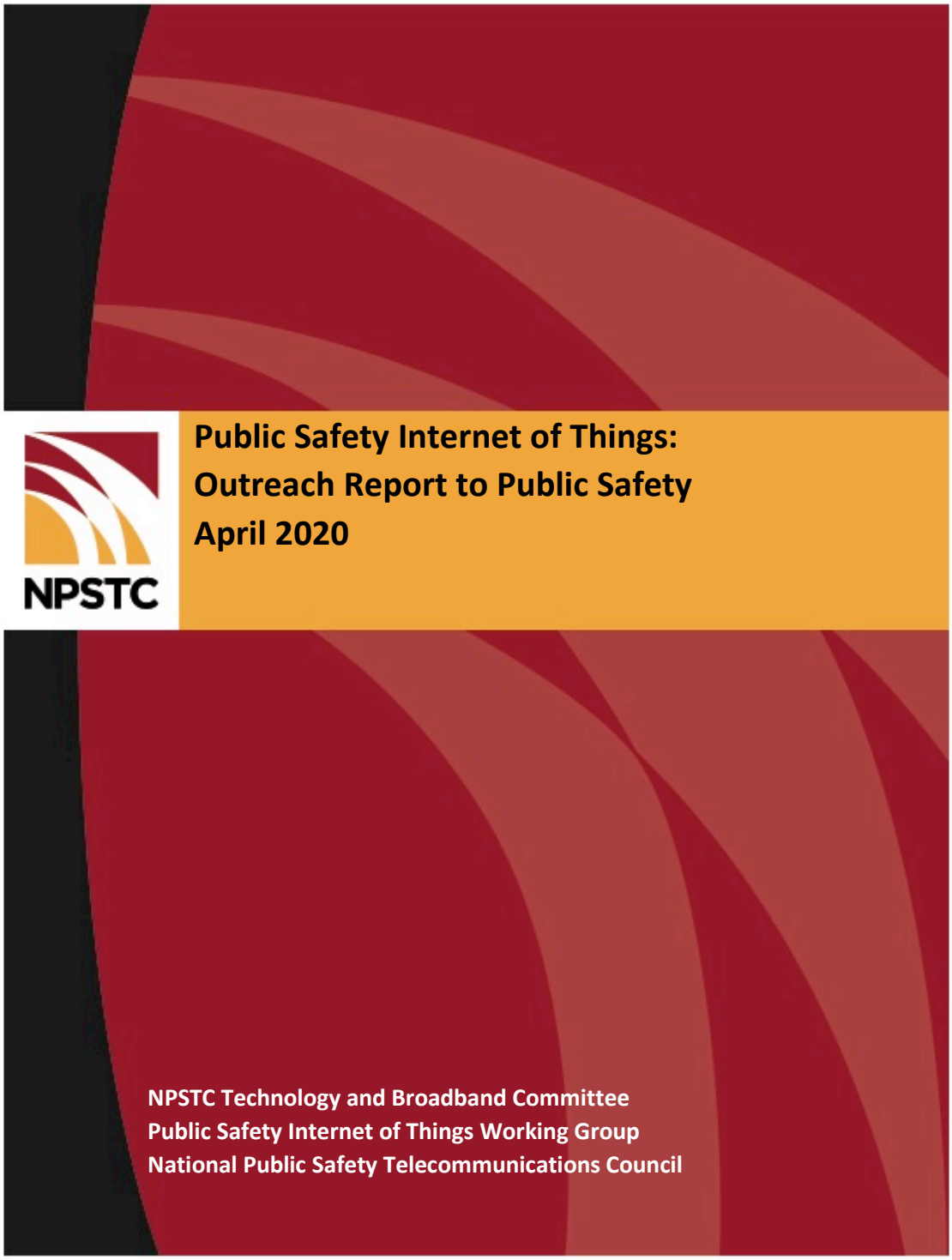


Public Safety Internet of Things: Outreach Report to Public Safety

April 2020

NPSTC Technology and Broadband Committee
Public Safety Internet of Things Working Group
National Public Safety Telecommunications Council

EXECUTIVE SUMMARY

The NPSTC Public Safety Internet of Things (PSIoT) Work Group and NPSTC staff have developed this *PSIoT Outreach Report* to complement the *PS IoT Use Case Book*.[1] This *Outreach Report* provides guidance to Public Safety and Information Technology agency leaders and technical staff who are considering adopting PSIoT technology.

PSIoT systems will quickly and effectively transform raw sensor data into **Actionable Intelligence** for first responders. Actionable intelligence will be aggregated from a virtually unlimited number of "things" and will provide benefits across every public safety discipline—increased situational awareness, enhanced common operating picture, improved responder health and safety, improved access to life-saving patient data, and efficiency and cost-saving benefits.

However, these benefits will not come without related challenges. This Outreach Report provides information and resources to help agencies navigate through the PSIoT planning and evaluation process.

Chapter 1 introduces the concepts of IoT, PSIoT and Actionable Intelligence, and also highlights the benefits of PSIoT to public safety. Chapter 2 identifies PSIoT governance considerations for public agencies. Chapter 3 provides background about the technology elements that make up the IoT "Ecosystem." Chapter 4 describes the key PSIoT challenges for agencies to consider in the planning process, and includes key questions for public safety stakeholders to ask their technical staff, their public and private partners and vendors, and even their mutual aid partner agencies.

Key Success Factors. PSIoT is still evolving, and clearly defined standards and requirements for public safety are often not available. Therefore, public safety agencies should begin the PSIoT planning process by identifying the agency's specific needs, and understanding the benefits, challenges and costs of adopting PSIoT to meet those needs. The Work Group identified these additional key success factors:

1. Identify and implement appropriate IoT security and cybersecurity **core baseline safeguards** to protect PSIoT devices, systems, networks and data;
2. Coordinate PSIoT planning and implementation tasks, and delineate **"ownership" responsibility** with Information Technology Departments and Smart Community Initiatives within the jurisdiction;
3. Follow the work of other local, state and federal agencies as they develop **governance policies and procedures** for PSIoT, including updates to Federal and State governance documents (e.g., SAFECOM Interoperability Continuum, Incident Command System (ICS), National Emergency Communications Plan (NECP) and Statewide Communications Interoperability Plans (SCIP));
4. Discuss **data interoperability and data sharing** needs, policies and procedures with regional mutual aid partners. Ideally, data sharing policies, standards, guidelines and MOU's should be in place before the first byte of data is transferred;
5. Understand the potential of **PSIoT analytics to create Actionable Intelligence** for real-time decision-making. Consider establishing a local or regional real-time analytics center either in the PSAP or elsewhere, to oversee the analysis of PSIoT data;
6. Understand the advantages and disadvantages of various **network connectivity options**, particularly the risks of using unlicensed spectrum (e.g., WiFi, Bluetooth).

[1] *NPSTC Public Safety Internet of Things (IoT) Working Group Publishes Use Case Report and Assessment Attributes,* June 17, 2019 [http://npstc.org/article.jsp?id=2321&cat=6407]

CONTENTS

EXECUTIVE SUMMARY ii
CONTENTS iii
1. INTRODUCTION 1
1.1. What is IoT? What is PSIoT? 1
1.2. What is Actionable Intelligence? 1
1.3. The Benefits of PSIoT 3
2. GOVERNANCE, POLICIES AND PROCEDURES 6
2.1. Governance 6
2.2. Policies 6
2.3. Standard Operating Procedures 7
3. PSIOT ECOSYSTEM AND TECHNOLOGY FRAMEWORK 7
3.1. IoT Devices – Sensor/Actuator, Gateway/Hub 8
3.2. IoT Network Connectivity - Wireless Network Options 9
3.3. IoT Applications (OTA, Edge, Core) 11
3.4. IoT Services 12
3.5. User Interface/Dashboard 13
3.6. PSIoT Physical and Wireless Security, Cybersecurity 13
4. THE CHALLENGES OF PS IOT 15
4.1. Ownership of the System and Control of the Data 15
4.2. Device and System Characteristics Required to Meet Agency Needs 16
4.3. Network Connectivity Options 17
4.4. Data Analytics 17
4.5. Data Interoperability 18
4.6. Data Sharing 19
4.7. Data Validity (Accuracy, Confidentiality, Integrity, and Accessibility) 20
4.8. PSIoT Physical and Wireless Security, Cybersecurity 21
4.9. Costs 24
ABOUT THE NPSTC PSIoT WORK GROUP 25
APPENDIX ONE: RESOURCES FOR MORE INFORMATION 26
APPENDIX TWO: SELECTED PSIoT WORK GROUP TECHNICAL PRESENTATIONS 28

1. INTRODUCTION

1.1. What is IoT? What is PSIoT?

The *Internet of Things* (IoT) is the network of physical devices and connectivity that enables objects to connect to one another and to the Internet (or a private network), thereby extending connectivity beyond traditional devices like computers, smartphones and tablets to almost any device or thing. While IoT technology has been used in some industry segments for several years, the benefits of applying IoT innovations in the field of Public Safety are only now becoming evident.

This *Public Safety Internet of Things* (PSIoT) promises to deliver important benefits to first responders such as improved situational awareness, operational efficiencies and a safer incident environment for both the responder and the general public. But these benefits will not come without related challenges.

For example, the Apple Series 4 Smart Watch can today be programmed to detect a hard fall by the wearer and initiate a call to emergency services if the wearer does not respond or show movement. While this action can result in a quicker response that may save the life of the wearer, public safety agencies must consider related challenges. PSAP personnel must determine the precise location of the wearer and ensure that the notification is not a false alarm, without the ability to question a human caller. Because the watch is a consumer product, there may be questions about the accuracy and reliability of the notification. Finally, PSAP personnel will have to determine how to manage the intake of these automated notifications and prepare for a rapid upsurge of notifications as the popularity of smart watches grows.

Or consider a "virtual knox box" for a smart building that would allow first responders to wirelessly connect to an array of sensors and actuators (heat, motion, barometric pressure, remote control of doors, lighting, and HVAC and gas/electric shutoffs), reporting detailed conditions in each room. How will the first responder gain access to such information, how can it be secured from unauthorized access and how will responders verify that the data is accurate and timely? Will the data be interoperable—capable of being displayed in a standard "dashboard" format on any responder's smart phone or tablet? How can this data be organized, filtered, prioritized and presented in a meaningful way, so that it is useful to responders?

This Report focuses primarily on PSIoT solutions—designed to reside on public safety broadband networks and based on authorized, authenticated, and secure access rights (not on consumer IoT). But PSIoT also exhibits significant benefits and challenges that public safety agencies must understand and prepare for. This Report is designed to serve as guidance for Public Safety and Information Technology (IT) Departments as they begin to evaluate various PSIoT solutions.

1.2. What is Actionable Intelligence?

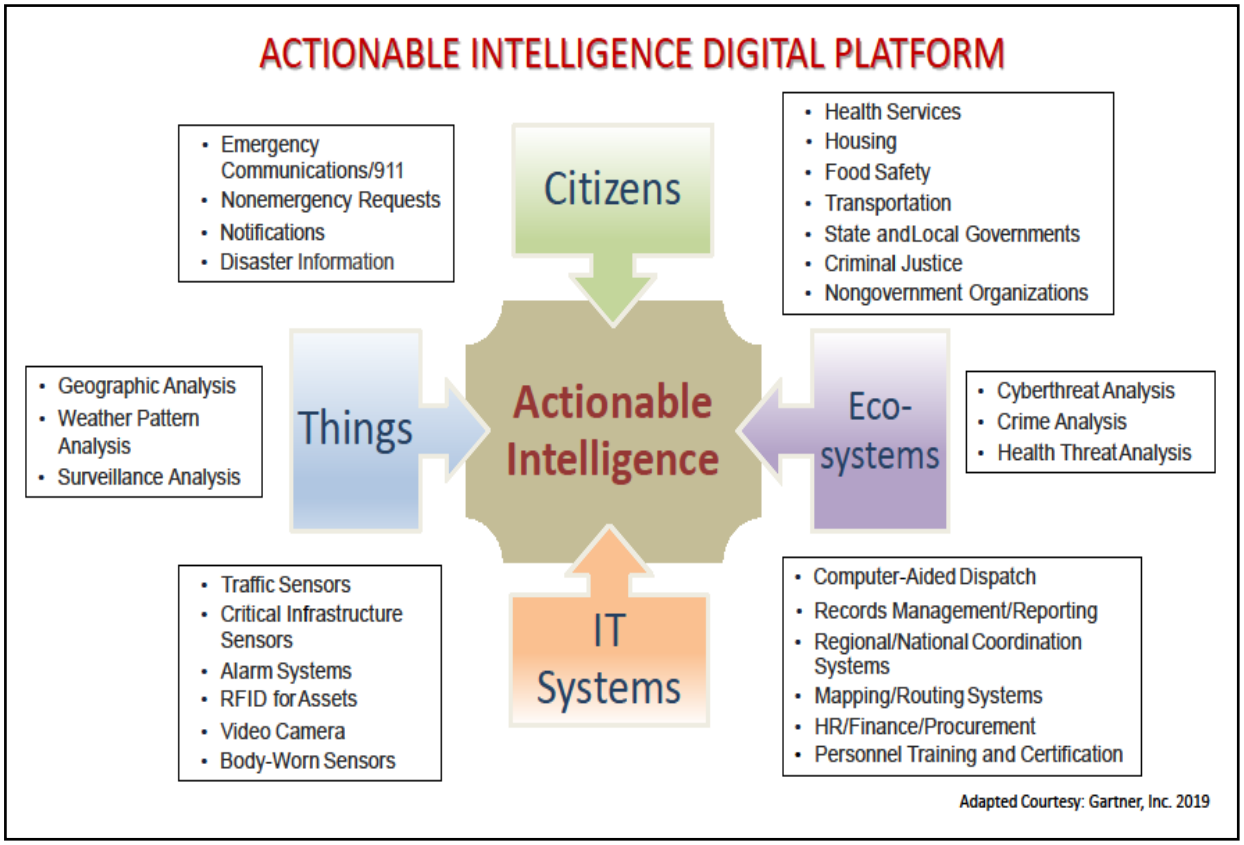
Ultimately, PSIoT is important because it can deliver extremely valuable, yet previously unavailable **Actionable Intelligence**. Just as the Apple Watch combines multiple data streams (heart rate, hard-fall sensors, movement sensors, voice recognition) to actuate a critical audio alert to the PSAP, PSIoT must

be capable of quickly and effectively transforming raw sensor data into actionable intelligence for first responders. Actionable Intelligence requires a process to extract critical and necessary information, combine key information from multiple sources, or organize data into prioritized order, to create usable information for real-time, critical decision-making in the field. This process will require analytics technology, and in the future, Artificial Intelligence (AI) capability[2], to ensure that PSIoT data is valuable and useful in real time to first responders.

ACTIONABLE INTELLIGENCE

Public Safety will use data streaming, existing databases, and analytics processing to convert raw IoT data into useful information for real-time, critical decision-making.

As Figure 1 illustrates, actionable intelligence may be aggregated from data from a virtually unlimited number of "things" and will provide benefits across every public safety and public service discipline.



[2] "Artificial Intelligence" (AI) is sometimes referred to as "Augmented Intelligence" or "Intelligence Augmentation," but we use the term "AI" throughout this document to mean all of these terms. Note that, in using these terms, we do not advocate replacing human decision-making with machine-based decision-making. Although computer-based data analytics will become a useful tool for first responders, any such tool will require ongoing review of the outputs by human analysts to ensure a valid and meaningful result. See Sections 3.3 and 4.4 for a more detailed discussion of analytics and AI.

1.3. The Benefits of PSIoT

The PSIoT Work Group developed **Eight Public Safety Use Cases** designed to identify how PSIoT might impact a variety of incident responses, from basic incidents to complex and escalating incidents involving multiple agencies and disciplines.

NPSTC PSIoT USE CASES

1. **Traffic Stop (Basic Law Enforcement)**
2. **House Fire (Basic Fire Response)**
3. **Medical Emergency (EMS response)**
4. **Video (Convenience Store Robbery)**
5. **Multi-Agency Incident (Vehicle Crash with Injuries/ Hazmat)**
6. **Smart Building Response (Nursing Home Fire)**
7. **School Shooting (Multi-Agency Response)**
8. **Severe Weather Event (Data Sharing with Secondary Responders; Off-Network)**

For each Use Case, the group discussed two key questions: (1) What **benefit** does this technology provide to public safety? And (2) What **risks** and **challenges** exist that may impact adoption of this technology? The following sections describe the benefits of PSIoT in more detail, followed by some specific examples from the Use Cases. More examples of these benefits can be found in the *Use Case Report*.

Improved Situational Awareness

First responders require information to gain actionable intelligence for an event. Currently, most data are gathered via manual input, verbal or visual observation, or communications from other responders, the dispatch center, and secondhand information from bystanders. These methods of intelligence gathering give first responders an idea of the situation, but critical information can be overlooked due to lack of access, lack of distribution or misinterpretation. As the scale of the event increases, it becomes progressively difficult to corroborate and accurately correlate information from multiple sources.

Public safety IoT devices will provide additional information to complement traditional inputs and expand improve situational awareness. By utilizing PSIoT, first responders will gain:

- **Contextual data**: Sensors are being incorporated into more areas of our lives, such as smart buildings, autonomous vehicles and traffic monitors. The ability to access and integrate this data prior to arrival on-scene will allow emergency responders to make intelligent and safe response decisions.
- **Information accuracy**: During an emergency, a great deal of information is coming in to the first responders to allow them to gain situational awareness. Much of the contextual data is provided by human sources today, and the accuracy of the information provided to first responders can vary. By utilizing data from PSIoT devices, the potential for human error can be removed from the data coming into the scene.

The NPSTC Use Cases provide many other examples of ways that PSIoT will improve and enhance situational awareness for small-, medium- and large-scale incident response.

Enhanced Common Operating Picture

Responders always have an "operating picture" of an incident or scene, based on the current situational status. Usually that picture is based upon experience with the location or people involved, and may be supplemented by information from dispatch or other responders. This Common Operating Picture (COP) constantly changes to reflect updates in the current situational status.

Public Safety IoT will significantly increase the number of inputs and amount of data available to improve the COP available for first responders in the field and for dispatchers and staff in the communications center or EOC. The Work Group identified several areas where PSIoT will enhance COP data available to incident commanders and dispatch:

- Precise, real-time location of responder, vehicle, resource, etc., at the incident scene;
- The health status of responders and the status of all equipment used by that responder;
- The "picture" inside buildings, as transmitted by cameras and other sensors inside that building;
- and much more.

With this improved COP, responders can be more effective when protecting lives and property. These improvements will be particularly important in escalating incidents, as additional mutual aid agencies and disciplines join the response.

Improved Responder Health and Safety

Today consumers and businesses use personal devices such as smart watches, medical pendants and other wearable biometric devices to improve and monitor their health, safety and awareness of their surroundings. These same technologies are starting to protect responders. Biometric monitoring and alerting devices can often detect a responder's need for help more quickly than a human.

The Use Cases detail how wearable IoT and other sensors can monitor the health of responders and their equipment such as weapons and Self-Contained Breathing Apparatus (SCBA) at the scene of a house fire, traffic stop or other incident, allowing them to stay out of harm's way.

Improved Access to Potentially Lifesaving Patient Data

The Work Group identified many ways that PSIoT will improve access to lifesaving patient data before, during and after an incident response. Smart watches now allow people to monitor their pulse, exercise and other health factors. Beyond smart watches, medical pendants, implanted pacemakers and insulin pumps and other devices monitor people and send information to family, friends and/or health care providers. Some devices can also track the location the wearer. With Public Safety often being the bridge between the public and healthcare facilities, it is imperative we be able to link and utilize data between them.[3]

Efficiency and Cost-Saving Benefits

In emergencies, time is of the essence to reduce loss of life and/or property. PSIoT will make response more efficient by providing early detection, notification, location, and other information to PSAPS, responders, and hospitals more quickly than previously possible. At the same time, PSIoT will reduce costs by reducing staff time currently used to manually gather and analyze of information and analysis, by automating inventory and medical supply monitoring, and streamlining reporting and after -action review.

The following Table highlights many examples of benefits to Public Safety IoT identified in the NPSTC *Use Case Report*.

[3] For example, the NPSTC-NASEMSO EMS Communication Working Group's *Sensor Based Medical Alarms* (December 2017) describes a variety of medical and telemetry sensors currently being used outside of hospitals and doctors' offices to monitor patient health status. http://npstc.org/download.jsp?tableId=37&column=217&id=4022&file=NPSTC_EMS_WG_Sensor_Based_Alarms_171211.pdf

Examples of Public Safety IoT Benefits from the NPSTC Use Case Report

Situational Awareness

- IoT devices near a hazmat spill monitor and analyze the air quality, and alert first responders to unseen toxic vapors in the air, thus enabling first responders in route to determine necessary tools and protective equipment in advance.
- During a multi-agency response to a school shooting, all data streams from school sensors and video can flow into the PSAP, allowing agencies escalate their responses appropriately.

Enhanced Common Operating Picture

- Responders arriving on the scene of an escalating incident can gain immediate access to a level of dashboard situational data rather than waiting for verbal updates, thus saving time for both incident command staff and mutual aid responders.
- Detailed Location-Based Services (LBS) data will give command staff the ability to assess deployment status, and to quickly and efficiently assign new arriving responders to fill needs.
- An improved operational picture provides a more accurate assessment of equipment needed at a scene, resulting in fewer requests for equipment that may be redundant or unnecessary.

Responder Health/Safety

- Biometric monitoring devices can provide real-time statue of responder health and alert command staff to a responder in distress
- Sensors, drones or robots can be used to monitor or take action in hazardous location, for example, in a burning building or at a hazardous materials site, without endangering humans
- Transportation-related IoT such as ice sensors accident detection mechanisms as well vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2x) help first responders understand road and traffic conditions to get to a scene faster and safer
- Location-based sensors can be used to track harmful material
- Real-time video analytics can provide immediate information (e.g., reading a hazard placard, facial recognition of a dangerous suspect)

Patient Lifesaving Data

- Data collected from patient care sensors in an ambulance allows hospital staff to effectively prepare for the arrival of a patient
- Medical alerting devices can often detect the need for help before a human can
  Smart watches and wearables can notify the PSAP when the wearer is unable to (ex. Takes a hard fall)

Efficiency and Cost Saving

- Alarms directly notifying a PSAP of a situation may eliminate the need for a 9-1-1 call to be made via 3rd party;
- IoT data can facilitate improved resource allocation of public safety assets, both equipment and human;
- Supply chain monitoring (automatically detecting when a syringe or other medical implement is used by EMS, for example) facilitates more efficient operational and supply processes;
- Many decisions will become automated thereby eliminating certain tasks - for example solutions with cameras that interpret license plate numbers perform a lookup without intervention by either the first responder or PSAP personnel reduces the workload for both;
- Managers/operations have more intelligence/justification at their fingertips to make better decisions on purchase/operations/initiatives.

2. GOVERNANCE, POLICIES AND PROCEDURES

2.1. Governance

Deploying PSIoT systems with the intent to share the benefits of the functionality across Agency and Department boundaries will require collaboration and cooperation at the highest levels of Agency Leadership. Implementing an effective governance model will help to ensure cross boundary collaboration and cooperation continues through the inevitable Agency Leadership changes that occur over time.

Perhaps the best place for agencies to begin is the *SAFECOM Interoperability Continuum*.[4] Developed with practitioner input by the Department of Homeland Security's SAFECOM program, the Interoperability Continuum is "designed to assist emergency response agencies and policy makers to plan and implement interoperability solutions for data and voice communications." This tool identifies five success elements that may be addressed to achieve the correct level of interoperability that best fits an Agency's mission: governance, standard operating procedures (SOPs), technology, training and exercises, and usage of interoperable communications. Agencies can use the Interoperability Continuum to identify gaps in their current communications environment and track progress in strengthening their interoperable communications.

Many additional Governance resources are available at https://www.dhs.gov/safecom/governance. The site contains templates and guides created with input from Public Safety practitioners.

Governance will be important (both within the local or state body and externally among regional agencies that share resources or support mutual aid assistance). Governance should include formal agreements on any factors that are determined to be important to the success of the mission, such as standards and funding requirements, security and cybersecurity safeguards. The Governance model used should be flexible enough to accommodate new technologies and innovations as they come into play.

2.2. Policies

Few models or guidelines for PSIoT policies are currently available. One early effort, from NIST, NIST-IR 8255*, Interoperability of Real-Time Public Safety Data*, provides an overview and recommendations for governance policies and procedures to ensure effective PS-IoT data sharing among agencies. One important takeaway from NIST-IR 8255 is that agencies *should begin by building on existing policy frameworks*.

Agencies should monitor updates to CISA's National Emergency Communications Plan (NECP).[5] In 2008, the initial NECP focus was on mission critical voice communications, and in NECP 2014 update, broadband data was introduced. The focus on broadband data has been expanded in the 2019 revision. PSIoT will represent the next evolutionary step of mission critical communications.

---

[4] SAFECOM *Interoperability Continuum* https://www.dhs.gov/sites/default/files/publications/interoperability_continuum_brochure_2.pdf

[5] NECP is the Nation's strategic plan that establishes a shared vision for and coordinates the complex mission of maintaining and improving emergency communications capabilities for the Nation's emergency responders. https://www.cisa.gov/sites/default/files/publications/19_0924_CISA_ECD-NECP-2019_0.pdf.

State and local agencies should plan to update the Statewide Communications Interoperability Plan (SCIP) and Tactical Interoperable Communications Plans (TICPs) to incorporate federal PS-IoT policies and procedures as well as State and local policy development.

The joint SAFECOM – NCSWIC Communications Section Task Force[6] was stood up to better understand present governance models and best practices within the *Incident Command System* (ICS) Communications Unit environment. The Task Force has recently proposed updates the *Incident Command System* (ICS) Communications Section to include a new role of IT System Liaison (ITSL) that complements the existing role of the Communications Unit (COMU). This change should improve the data management processes as Public Safety departments work with their IT Support organizations in planning, implementation and deployment of PSIoT and other data-driven technologies.

DEVELOPING DATA SHARING POLICIES BY *BUILDING ON EXISTING FRAMEWORKS*:

- **Agency leaders can build momentum for data sharing efforts and leverage shared infrastructure and expertise by collaborating with state and local open data and smart city initiatives.**
- **Agencies should take special care to build security and privacy protections into data sharing tools to meet legal requirements, operational needs, and public concerns.**
- **Key features of a data sharing initiative include agency leadership commitment, clearly articulated goals, strong collaborations, coordinated procurement requirements, and regular impact assessments.**

Source: NIST-IR 8255*, Interoperability of Real-Time Public Safety Data*

2.3. Standard Operating Procedures

According to the 2019 version of the NECP, "The fast-paced evolution of communications capabilities highlights a crucial need to develop and update standard operating procedures and operational plans to address entities, individuals, or organizations that provide or use communications during emergencies." PSIoT will be no exception. Clear and effective Standard Operating Procedures (SOPs) will be essential in the development and deployment of any PSIoT solution

Agencies can begin by following the SOP swim lane of the *SAFECOM Interoperability Continuum*. Individual agency SOPs for PSIoT should be shared with regional partners and revised to conform to future PSIoT additions to the National Incident Management System. Actionable Intelligence from PSIoT systems will play an increasing role in multi-agency/multi-discipline/multi-hazard responses, so coordinated efforts to implement SOPs should be developed before, rather than after, planning for PSIoT begins.

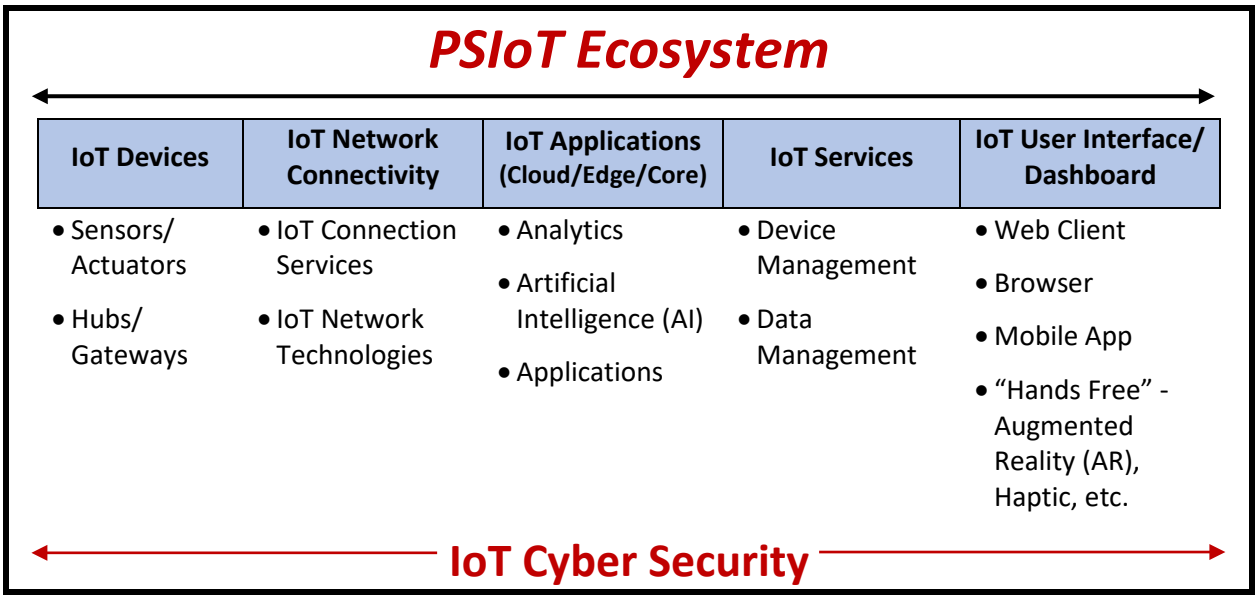
3. PSIOT ECOSYSTEM AND TECHNOLOGY FRAMEWORK

The Work Group, building on its comprehensive survey of the IoT Industry, developed the following high-level overview of the technologies and services that will combine to create the PSIoT ecosystem. As

[6] SAFECOM – NCSWIC Communications Section Task Force materials available at https://www.dhs.gov/safecom/communications-unit

discussed in the previous section, the complexity of the ecosystem will require collaboration and coordination between IT Departments and Public Safety Agencies, as well as other stakeholder groups.

The figure below provides a snapshot of PSIOT Ecosystem elements. Logical and physical design and data flow will vary widely across solutions, and not all elements will be required for all PSIoT solutions.



3.1. IoT Devices – Sensor/Actuator, Gateway/Hub

Sensors/Actuators

Internet of Things begins with a device of limited intelligence capable of reporting its environment or initiating an action that connects a "thing" to a network. Traditionally, the device itself is not capable of performing analysis of the information it receives and relies on elements in the network ("cloud") to determine if the information has value (i.e., to create actionable intelligence).

Sensors act as inputs to the environment, whereas actuators act as outputs to the environment. An example of a public safety sensor is a vest penetration sensor, which detects if a bulletproof vest has been punctured either through knives, bullets, or shrapnel. An example of an actuator is a remotely activated tornado warning siren or natural gas shutoff valve.

IoT sensors/actuators may be mobile (e.g. carried by an individual, a vehicular platform, an aerial platform, etc.) or stationary (e.g. set up on a pole at a fixed location). They can be further distinguished by their traffic behavior and their bandwidth demand—sensors monitoring physiological parameters will generate much less traffic than streaming video cameras.

Hubs and Gateways

Hubs are typically devices located on the user or vehicle at the incident that aggregate information locally and provide network connectivity to devices that may not natively support it. Alternatively, gateways may be used in the field to collect information from multiple devices of the same type in a small area to provide network connectivity. An example is the data from heartrate sensors deployed at a fire scene being wirelessly aggregated by an external device and made available to incident command and dispatchers. Gateways may also be deployed by cloud providers to aggregate disparate sensors and actuators into a single user interface/dashboard.

These "SmartHubs"[7] will become an essential element of the IoT Ecosystem, allowing efficient and secure collection of data from multiple sensors or sources at the incident. SmartHub modules will create a **Personal Area Network (PAN)** for each responder, with multiple on-body or in-vehicle hubs further interconnecting to create an **Incident Area Network (IAN)** or **Wide Area Network (WAN)** connecting to the rest of the agency's communications and information systems.

As computer processing power and memory increases, hubs and gateways will serve two additional critical functions. First, they will support more advanced edge analytics processing, which can provide actionable intelligence in real-time at the scene of an incident. Second, an IoT device that is properly shielded from outside network intrusion by an IoT gateway or hub can only be accessed remotely through the IoT gateway or hub, so that IoT device effectively inherits network logical access protection from the IoT gateway or hub.[8]

3.2. IoT Network Connectivity - Wireless Network Options

IoT Connection Services

IoT sensors, actuators, hub and gateways must be interconnected by one or more networks, and will most often also be connected to the PSAP or communications center using a carrier-based network. The PSAP or Communications Center is the primary destination for situational awareness and decision making.

Wireless connectivity requires that the sensor (or gateway) device is recognized by the network and allowed to connect; in 3GPP. A (removable or non-removable) subscription module, which is provided, and provisioned, by the network operator, must be embedded in the device to allow such connectivity.

IoT Network Technologies

Today's wireless IoT technologies leverage either unlicensed or licensed spectrum bands with service delivery through a private network or a commercial service provider. Available technologies are generally targeted at wide area coverage and, because of stringent needs on power savings, they are generally low-power; hence the term Low Power Wide Area (LPWA)[9]. Technologies such as Bluetooth, Zigbee (IEEE 802.15.4x), or WiFi (IEEE 802.11x) with relatively short radio range do not fall in this class. In public safety though, the use of such short-range technologies is quite common. A typical example is in

[7] See, Next Generation First Responder (NGFR) Integration Handbook Version 3.0 https://www.dhs.gov/publication/st-frg-ngfr-integration-handbook-version-20. The NGFR technical team determined that "the minimum components an on-body system would need to include: a controller, communications, sensor inputs, user input/output and power."

[8] See, Draft NISTIR 8259 - *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers*, 2019. "Dependency on an IoT gateway/hub has other positive security implications, such as a greater chance of malicious activity involving the IoT device being detected (because its network traffic passes through the IoT gateway/hub). *However, shifting features from the IoT device to an IoT gateway or hub makes the cybersecurity of that gateway or hub critical to the cybersecurity of the IoT device*." (Emphasis added)

[9] The focus herein is on long range IoT, i.e. in the few miles capability. When applicable, the use of mesh protocols can increase the communications range of WiFi, Bluetooth (BLE profile) or Zigbee (802.15.5 profile) but the reach remains below typically-centralized, wide-area technologies. They are commonly used for non-mobile, local and personal area networks.

the creation of a body network, or PAN,[10] where data streams may be conveyed, (e.g. via Zigbee), to a LPWA-connected PSIoT hub or gateway.

Available long-range technologies fall into the unlicensed and licensed categories. SigFox and LoRa belong to the former. Achievable data rates range from a few 10's bps to a few 10's of kbps. Both operate in the 900 MHz spectrum, but coverage is not ubiquitous across the country.

When licensed spectrum is available, i.e. whether through auction, assignment or leasing, long-range technologies in use today are mainly based on 3GPP standards. **NB-IoT** and **LTE-M** standards[11] have been developed to leverage an existing LTE network infrastructure while ensuring interoperability and roaming; operators may opt to deploy a separated dedicated core network.

The following table is a snapshot of the network technologies most likely used in the PSIoT ecosystem.

Network	Characteristics	Spectrum
	SHORT RANGE	
Bluetooth, Zigbee (IEEE 802.15.4x), WiFi (IEEE 802.11x)	• Low Power • Variable data rates • Must be connected to PAN, hub or gateway to ensure secure connection	Unlicensed 2.4 GHZ 5.0 GHz
	LOW POWER WIDE AREA (LPWA)	
SigFox, LoRa	• Low data rate (10's bps to a few 10's of kbps)	Unlicensed, generally in 900 MHz band
	CARRIER-BASED	
NB-IoT	• Long Range • ~200 KHz occupation bandwidth • Designed to serve large number of devices per base station sector • Low data rates, mid-to-high roundtrip latency, minimal power consumption, and to ensure IoT traffic does not overload the network.	Licensed
LTE-M	• Long Range • Peak data rates greater than 1 Mbps (at the expense of radio range). • Also designed to serve large number of devices per base station sector, but will support higher data rates. • Requires more device power, shortening battery life	Licensed
LTE	• Full broadband capabilities • Designed for highest data rate applications, such as high-resolution streaming video	Licensed

[10] See, Draft NISTIR 8196, *Security Analysis of First Responder Mobile and Wearable Devices.* "PANs use a completely different set of wireless networking protocols than cellular or LMR devices such as WiFi or Bluetooth. The security interactions between these devices and protocols need to be understood to ensure public safety activities are not adversely affected."

[11] Spectrum bands of use for NB-IoT have been defined in 3GPP, with Band 14 (FirstNet) included in Release 15 of the standard. NB-IoT can be deployed in-band, i.e. within a LTE spectrum block, in the guardband of an LTE operating bandwidth, or in a standalone mode. Likewise, for LTE-M, there are Release 13 devices (Cat-M1) and release 14 devices (Cat-M2). Cat-M1 are limited to a 1.4 MHz bandwidth with peak data rates of up to 3 Mbps, and Cat-M2 would support 5 MHz and even 20 MHz, to achieve data rates from 4 to 27 Mbps.

NB-IoT and **LTE-M** standards will enable the creation of a large eco-system of devices and the possibility of roaming across service providers. From a basic architecture standpoint, there is no difference between NB-IoT and LTE-M. LTE-based systems support both IP and non-IP data which can be carried over the control plane or the user plane; however, LTE-M specifications also include support for connected mobility and voice services.[12]

3.3. IoT Applications (OTA, Edge, Core)

Analytics/Artificial Intelligence (AI)

Analytics is an essential component of the PSIoT Ecosystem. Analytics applications transform raw data from one or many sources (including IoT devices) into useful information—Actionable Intelligence—that will benefit public safety agencies before, during and after incident response. Analytics can take place at any point along the communications path, at the sensor, at the hub or gateway, in a cloud-based application or at the agency's PSAP or a real time analytics center.

IoT data can be analyzed historically and in real-time depending on the specific needs. Historical analytics looks at data from the past to conduct statistical analysis, including trends and patterns in the data set(s). Real-time analytics is configured to analyze data as it becomes available to the cloud environment.

Artificial intelligence (AI), sometimes referred to as "Augmented Intelligence," is an area of computer science that emphasizes the development of advanced analytics programming capable of automatically sifting through vast amounts of data, identifying the most appropriate information and delivering only the most useful knowledge to the end user. Although not available to first responders today, AI may someday provide a sort of automated assistant for first responders that can retrieve crucial data from disparate sources (including IoT data sources), dispatch analytics to extract information, and apply "human-like reasoning" to synthesize and deliver the most relevant actionable intelligence to the first responder.

For example, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) is partnering with the NASA Jet Propulsion Laboratory (JPL) to investigate the use of JPL's state-of-the-art human-like reasoning system, the Assistant for Understanding Data through Reasoning, Extraction, and Synthesis (AUDREY), to perform data fusion and provide tailored situational awareness information to first responders. [13]

Applications

Public safety and other third-party applications can be integrated with IoT cloud environments through software interfaces or data transfer services to enhance situational awareness. These applications can

[12] Long-range non-3GPP standards such as CBRS, narrowband P25, TETRA and DMR Tier III, and IEEE 802.16s are additional options public safety agencies may consider. 4.9 GHz spectrum licensed to public safety may be another viable network option for PSIoT. See Comments of NPSTC in response to the Sixth Further Notice of Proposed Rulemaking (Sixth FNPRM) regarding Amendment of Part 90 of the Commission's Rules. (Seeking comment on alternatives to stimulate expanded use of and investment in the 4.9 GHz band.), filed July 6, 2018. http://npstc.org/download.jsp?tableId=37&column=217&id=4129&file=NPSTC_Comments_4.9GHz_SixthFNPRM_20180706.pdf

[13] https://www.dhs.gov/publication/st-frg-audrey

provide additional data sources for IoT cloud environments and function as a consumer of IoT cloud data to further improve or automate application services. Examples include:

- Weather and traffic flow data integrated with IoT data to enhance situational awareness.
- License plate readers (LPR) integrated with traffic violation and stolen vehicle databases to provide additional first responder insights during a routine traffic stop.

3.4. IoT Services

Device Management

Device Management services include all network connectivity requirements in addition to other necessary functions, such as sensor management, provisioning, data collection and analysis, decision support etc. The ability to install firmware upgrades or software patches for IoT devices is particularly challenging, and deserves special consideration by agencies evaluating PSIoT devices and systems. [14] Services may be provided by the network operator, a jurisdiction or a third-party service provider. These functions may be distributed in distinct locations, e.g. in public clouds, private clouds, closer to the edge of the network etc.

Most Public Safety agencies have either an IT department or work closely with their IT Department to perform the management/provisioning/usage functions associated with mobile device management. Mobile Device Management (MDM) applications, also known as Enterprise Mobility Management (EMM), provide a centralized capability to manage mobile devices, including any security risks associated with them. [15] MDM/EMM will also play an important role for PSIoT device management. A number of specialized IoT management platforms, often called "IoT control centers" have emerged to help IT departments manage their IoT devices.

Cloud-based IoT platforms manage IoT devices in the cloud environment and provide a set of tools to configure, connect, and process IoT data and services. Cloud IoT platforms may offer a suite of IoT device management services to fully support IoT devices in a cloud environment. In situations where IoT devices are managed by other software platforms, IoT data can be integrated into the cloud environment through system interfaces or data transfer services.

Data Management

Cloud IoT data management is handled through the provisioning of storage services in the cloud environment. There are multiple types of cloud storage and pricing options depending on the type of data and planned use cases. Cloud object databases are structured in a virtual storage environment to optimize cost and performance for IoT applications. The Cloud IoT data management platform should include the following functionality to support public safety applications and services:

- Security and privacy
- Access and authentication

---

[14] See National Telecommunications and Information Administration (NTIA*), Stakeholder-Drafted Documents on IoT Security* for detailed information on security risks associated with upgradability and patchability of IoT devices. https://www.ntia.doc.gov/IoTSecurity

[15] DHS Science and Technology Directorate (S&T), "*Evaluating Mobile App Vetting Integration with Enterprise Mobility Management in the Enterprise*". https://www.dhs.gov/sites/default/files/publications/4681_evaluatingmobileappvettingintegrationwithemm-clean-r4-508c.pdf."EMM can provision security policies to devices, provision devices with credentials to access enterprise resources, and monitor aspects of device state, i.e., gathering an inventory of installed applications."

- System Resiliency
- Data formatting
- Data storage options
- Analytics services

3.5. User Interface/Dashboard

The main purpose of the user interface/dashboard is to provide a consolidated access point for IoT and situational awareness information. The Cloud user interface/dashboard enables public safety users to access IoT data through a set of web services. The implementation of a web services architecture enables cloud IoT data and analytics to be accessed from multiple types of applications or devices. For example, cloud IoT data and analytics can be accessed from a web client browser, mobile application, or central management system to assist with public safety situational awareness communications and coordination.

Situational awareness information may also be provided via a web client, browser, mobile application, or via a "hands-free" device, using augmented reality or haptic interaction. Detailed discussion of such technology is beyond the scope of this Report; however, several other entities are conducting extensive research and testing of hands-free interface applications that may be appropriate for PS IoT. [16]

3.6. PSIoT Physical and Wireless Security, Cybersecurity

Security and Cybersecurity are critical to the success of the PSIoT Ecosystem, with points-of-failure possible with any of the previously described ecosystem elements. Security must be viewed from an end-to-end perspective, encompassing physical security, wireless security and cybersecurity.

The Work Group identified a number of PSIoT Ecosystem characteristics that require special security planning and consideration:

- IoT devices often must be positioned in physical locations that have uncontrolled and/or unsupervised access (public buildings, transportation rights-of-way, remote outdoor locations);
- The sheer volume of IoT sensors, hubs, and gateways deployed and operating may stretch the limit, scale, and scope of traditional cybersecurity products and practices.[17]
- Many IoT sensors are designed to be small, inexpensive, with little processing power, and may not support the required level of security (such as hardening) or necessary updates and support from the manufacturer;
- IoT devices present a point of access for public safety networks, and thus pose a risk to the greater network it may be connected to.
- Consumer and industrial connected devices and systems may not be designed as critical IoT services, yet may become critical data sources in an emergency that cannot be inherently

[16] See, for example, NIST Public Safety Communications Research Division, User Interface/ User Experience Publications (https://www.nist.gov/ctl/pscr/user-interface-user-experience-publications).

[17] See CISA *Internet of Things: Impact on Public Safety Communications,* March 2019 (https://www.cisa.gov/sites/default/files/publications/CISA%20IoT%20White%20Paper_3.6.19%20-%20FINAL.pdf)

trusted. DHS CISA delineates between Critical IoT and Massive IoT as categories, but terminology varies within the industry.[18]

Minimum security requirements may vary depending on the agency itself, the information being transported (such as HIPAA), and the network connection used. When planning for PSIoT, agencies are encouraged to enhance or augment existing security and cybersecurity policies to address these risks.[19]

Physical and Wireless Security

At a high level, physical security restricts access to the device itself (i.e. physical controls). For example, wearable devices would be kept in a secure location when not in use, and fixed devices would include physical mechanisms such as hardened enclosures and locks. Tamper protection indicates whether the device is being physically accessed and reporting to infrastructure, and ensures access by only authorized personnel. Restrictions on the device itself should prevent resetting the device to factory defaults from unauthorized personnel. All default passwords from manufacturers should be changed.

Wireless security starts with the identification of the frequency band that best meets the public safety agency's minimum mission requirements. See Sections 3.2 and 4.3 for a discussion of IoT frequency options, and considerations for identifying the preferred band.

Attacks on air interfaces typically involve jamming (preventing access), monitoring (passive interception of communications), and impersonation (pretending to be either an IoT device or the infrastructure). IoT is particularly vulnerable to jamming due to the low power emitted from the devices, and vulnerable to monitoring and impersonation because of the low-cost design of the devices precludes more advanced security safeguards.

IoT Cybersecurity

At a high level, there are four category types with respect to cybersecurity:

- Eavesdrop – Unauthorized sampling or altering the data stream while being transmitted, either due to unencrypted transmissions, weak encryption or vulnerabilities in the encryption method, or strong encryption that has been used for a long duration.
- Impersonate – An attacker's device pretends to be an IoT device or the infrastructure itself.
- Service Attacks – This is either preventing the connections from occurring (Denial of Service [DoS]) or disrupting the process by inserting an attacker's device in the communications process (Man-In-The-Middle [MITM]). Neither the device nor the infrastructure is directly compromised, but the communications between them are necessarily compromised. However, an uncompromised device may initiate service attacks due to the illegitimately issued commands.
- Compromise – The device or infrastructure is directly compromised (e.g., an unauthorized entity has gained access to the IoT device and is able to control it). This may be used to listen to

[18] **Critical IoT** applications require reliable delivery of information, over a high availability infrastructure with very low latency (e.g., body-worn cameras and biometric sensors), while **Massive IoT** applications contain typically large numbers of inexpensive devices, each of which transmits a small amount of data on a rather infrequent basis (e.g., air quality monitoring, flood level measurements). However, some low data rate IoT devices – such as earthquake sensors – will require low latency and priority when operating in an emergency. See CISA *Internet of Things: Impact on Public Safety Communications.*

[19] See Section 4.8. Also, in Appendix One we provide links to several reference materials from both federal government and private industry sources, as guidance for agencies seeking to update existing policies to address IoT risks.

communications, perform Distributed Denial of Service (DDoS) attacks, or as an entry point for an attacker into a secure network, as examples.

These attacks may occur at any point throughout the communications chain, and the unique vulnerabilities of PSIoT discussed above will increase the risk of such attacks. Minimizing the number of steps in communication along with the number of communication parties in the process will reduce the attack surface. While there are many methods used for cyberattacks, the two most common attacks are various forms of Denial of Service (DoS) and using the IoT device as an entry point into a secure network. Best practices in this area include, but are not limited to, continuous monitoring of IOT devices and network infrastructure for anomalies and recurring training for cyber security and network maintenance staff.

4. THE CHALLENGES OF PS IOT

The Work Group identified 22 "Assessment Attributes" to focus its discussion on the challenges to public safety of adopting PSIoT. These attributes are described in more detail in the Use Case Report.

NPSTC PSIoT Assessment Attributes

- **Ownership**
- **Form Factor**
- **Device/Application Characteristics**
- **Number of Users**
- **Number of Devices**
- **Device Location**
- **Device Network and Connectivity**
- **Device and User Identification**
- **Device Management**
- **Data Ownership**
- **Data Usage**
- **Data Sharing**
- **Data Validity and Authenticity Factors**
- **Data Privacy Factors**
- **Data Interoperability**
- **Data Filtering and Analytics**
- **Data Storage and Evidence Management**
- **Cyber-Security and Physical Security**
- **Multi-Vendor Device/Application Environments**
- **Actuator Capabilities**
- **Implementation/ Operational Issues**
- **Cost Benefit Analysis**

The following sections summarize some of the most important challenges, and pose key questions for public safety stakeholders to ask their technical staff, their public and private partners and vendors, and even their mutual aid partner agencies, as they consider PSIoT solutions.

4.1. Ownership of the System and Control of the Data

In determining "IoT ownership" and "control of data produced by IoT solutions, public safety agencies will confront the same issues they do today with other devices and systems and the data those systems produce. IoT networks simply multiply the problem, as it will be easy for communities to deploy hundreds or thousands of connected devices, such as cameras, equipment tags, acoustic (gunshot) sensors, generating enormous amounts of data.

Historically, most public safety agencies exercised total control of their equipment and information. Weapons, fire apparatus, paper police reports and almost all other aspects of operations were under control of the agency chief. With the advent of information technology, and particularly computers and smart mobile devices, some of the control passed to a central information technology (IT) department.

Agencies found themselves sharing control and data from traffic or surveillance cameras, building control systems and broadband networks. Today, many systems used by public safety agencies – particularly software applications and their databases, but also networks and sensors – are managed by other departments, other government agencies and private companies.

With IoT solutions, this loss of direct control of such systems, networks and the corresponding data will accelerate. No formula exists to guide agencies to make decisions about purchasing, leasing, sharing control or simply using (with no control) third-party IoT devices, networks and the data they collect.

The following sections of this Report raise many considerations for agencies as they evaluate new IoT solutions. Agencies should be even more diligent in investigating and asking the right questions as they consider solutions owned by third parties.

KEY QUESTIONS TO ASK

- **What are the agency's minimum requirements for system operations and maintenance and how will the agency verify compliance?**
- **Who owns the data, who stores the data, who is authorized to share and use the data, who controls the release of data?**
- **Will the agency have the necessary access to the data when it is needed?**
- **Can the owner provide guarantees for reliability, accuracy and timeliness of the data, and resiliency of the system?**
- **Is the solution proprietary, or standards-based (capable of interfacing with other IoT solutions)?**

4.2. Device and System Characteristics Required to Meet Agency Needs

KEY QUESTIONS TO ASK

- **What are the agency's minimum requirements for physical system design, including access controls, power needs, storage capacity, number of sensors, environmental conditions, reliability, etc.**
- **Requirements for upgrading, patching, remote troubleshooting, etc.?**
- **How much downtime anticipated for maintenance and what is the operational fallback plan during downtime?**
- **What is the expected useful lifetime of the sensor devices?**
- **How will devices be named or identified on the network?**
- **Considerations for Data Management: Cost; Performance; Accessibility; Analytics and processing; Scalability; Security; Retention and Backup.**

The Work Group reviewed a large number of IoT device and system characteristics and configurations available to public safety agencies. Agencies must consider these many alternatives and choose the right "fit" of characteristics that will provide the level of actionable intelligence required to meet the agency's specific purpose. IoT solutions should also provide public safety agencies with sufficient flexibility in configuration and customization in order to meet local operational requirements.

IoT devices display a wide range of characteristics, such as size, weight, power source and consumption, data processing and storage capability, whether the device is mobile or fixed, how often the device transmits status, and even whether the device is reporting a condition or taking an action.

Likewise, PSIoT system characteristics must fit the anticipated public safety use, for example the system may be required to operate in hard environmental conditions, over a long period of time, or with more stringent reliability, ruggedness, and resilience

requirements than available with current consumer or industrial IoT systems. Other important characteristics include battery life under stress conditions, the number of users to be equipped with the IoT solution, the total number of devices that will be purchased and that will be in active use at any given time, and the expected coverage range for wireless connectivity.

Devices and systems **must have a standardized IoT device and user naming convention** to allow rapid awareness of device and user identity, activation status, and accurate tracking of each device deployed, who has it, and what its purpose/capable range is, and ability for off-network operation.

Finally, systems must include secure and reliable device and data management processes for quick and dependable configuration and operations, and for maintenance tasks such as diagnostics, repair, patching, and upgrading. [20]

There are no "one-size-fits-all" guidelines. Agencies planning PSIoT systems must carefully consider all these factors, and more, before purchasing a system or contracting with a third-party provider.

4.3. Network Connectivity Options

The PSIOT use cases demonstrate that data may originate via more than one IOT device, IOT network infrastructure, and/or more than one IOT service provider. As highlighted in Chapter 4, the reliable and secure delivery of an IoT service can involve multiple systems, multiple stakeholders, and multiple networks connecting the sensor to the end user.

Public safety agencies should understand the differences between various IoT spectrum options, and the proposed connectivity solutions proposed by IoT Ecosystem providers. Agencies must ensure that all spectrum used in the IoT system will meet minimum performance requirements for the proposed solution, including coverage, data throughputs, reliability, and security. For example, when relying on sensors connected by unlicensed networks (e.g., WIFI or Bluetooth), the sensors should be connected to, and the data aggregated through an IoT gateway or hub (SmartHub) with proper security features (e.g., SIM card), to protect against unauthorized network intrusion.

Understanding network capabilities and limitations, and choosing the best network solutions will be a critical step in the PSIoT planning process.

KEY QUESTIONS TO ASK

- **What network(s) are the best choice for secure and reliable connectivity?**
- **How will the analytics SmartHub be connected to the devices and the Users? Will unlicensed networks be used only for routing data to a secure SmartHub?**
- **How will data be transferred across disparate networks and platforms?**
- **How is the user alerted to connectivity failures?**
- **Are the PSIoT devices certified against a set of relevant standards?**
- **Can I manage my own devices?**

4.4. Data Analytics

Real-time analytics are important in the public safety environment. Instead of drawing conclusions based on historical data, public safety systems need to process and display situational awareness data

[20] See National Telecommunications and Information Administration (NTIA*), Stakeholder-Drafted Documents on IoT Security* for detailed information on security risks associated with upgradability and patchability of IoT devices. https://www.ntia.doc.gov/IoTSecurity

on-scene and in real time. Analytics software performs these functions quickly and efficiently. For example, an EMS SmartHub connecting various patient care sensors and historical patient health records can provide first responders with patient care recommendations based on an analysis of this data compared with EMS treatment protocols.

The role of analytics to aggregate and summarize information for use by public safety agencies is evolving. While software analysis of vast amounts of real-time, complex data can be beneficial for public safety, agencies should carefully evaluate the accuracy of any proposed analytics solution. Software applications can today perform review of simple data sets with few errors, but more complicated analysis, particularly review of complex data sources can produce both "**false positive**" and "**false negative**" results. In the EMS SmartHub example, treatment recommendations based on false positives or false negatives could prove disastrous and deadly for the patient.

Today, complex data analysis will require review of the results by human analysts to eliminate false positive and false negative errors, to ensure a valid and meaningful result. When considering an IoT solution that involves real-time analytics agencies must weigh the efficiency benefits of the solution with the accuracy of the analysis and potential time and cost of additional review by staff analysts.

An agency may consider developing a "Real-Time Analytics Center"—a place where data from IoT (including non-PS commercial and smart community IoT) is assimilated, analyzed and compared with existing databases and other sources (using both machine and human analysts). This center can take one of several forms, depending upon the community:

- Center in the PSAP. A special unit in the PSAP, similar to the real-time crime centers we are seeing develop today.
- Smart City (or County) Operating Center. In this model, a medium-sized-to-large city would have an operating center to manage all its smart city functions ranging from water delivery, to transportation to public safety, including all its IoT on infrastructure.
- The Fusion Center. Fusion centers could become real-time crime centers and PS-IoT analytics centers. This could work well for multiple cities in a single metro area.

KEY QUESTIONS TO ASK

- **What requirements has the agency identified for analytics solutions?**
- **How may the agency measure or validate the accuracy of analyzed data?**
- **Where will the "edge analytics" reside--worn by the first responder, in a vehicle trunk, or in a remote location, such as the PSAP or data center.**
- **Will the analytics solution use human analysts to validate results? What level of resources will be required?**

4.5. Data Interoperability

"Data Interoperability" refers to the technical ability to access and display PSIoT data between IoT systems. Data Interoperability is closely aligned with Data Sharing, but can also include interoperability among multiple systems used within a single department, or among users in multiple departments that may need access to each other's data.

Data Interoperability and Data Sharing are complex topics, and agencies seeking detailed information should consult ***NIST IR-8255: Interoperability of Real-Time Public Safety Data: Challenges and Possible Future States***.[21] NIST IR-8255 identifies comprehensive technological, economic and governance challenges and recommendations for agencies "that will allow first responders to derive maximum operational benefits from the capabilities provided by emerging technologies and the NPSBN, and to encourage technology developers to support more interoperable data sharing technologies for public safety."

Agencies should consider sensor systems and IoT platforms that implement open standards when possible. However, newer IoT solutions today are often proprietary, or the format used by a leading company in the field is not adopted by others. This means that agencies must access the data of one system via one dashboard and another system via a separate dashboard. In the future, public safety should have access to one dashboard that allows access to all necessary sensors. But this is not the case today.

To guarantee interoperability today, multiple agencies or departments would need to acquire a specific technology from the same company. While this is often not feasible, creative procurement plans, e.g. piggy-backing RFPs, leasing equipment or using third-party cloud services, can often mitigate incompatibility issues.

If complementary providers are not used, or if systems are changed in the future, agencies would need to conduct manual system integration to move data from one platform to the other. Some companies do make Application Programming Interfaces (APIs) available. Agencies should also understand how APIs can be used to translate non-standardized information to share between agencies with disparate systems. Such requirements should be included in RFPs.

Agencies must also collaborate to ensure that the information being shared is interpreted correctly. The simplest method is to allow the assisting agency access to the information dashboard, which aggregates the information from the sensors. This will require secure connections between the agencies or the cloud, if implemented, and may require an internet-connected computer at each user location. Providing access to the raw sensor feeds presents additional challenges.

KEY QUESTIONS TO ASK

- **Has the Agency asked the vendor/service provider if it provides an interoperability solution?**
- **Does the proposed PSIoT solution operate on an open platform, or will the vendor provide an API?**

4.6. Data Sharing

"Data Sharing" involves both the technical and policy requirements necessary to transfer internally owned data sets to outside agencies. The PSIoT Use Cases demonstrate that public safety agencies will often need to share IoT data before, during and after an incident response, especially in incidents involving multiple responding agencies. Ideally, Policies, Standards, Guidelines and MOU's should be in place before the first byte of data is transferred.

[21] NIST IR 8255, https://www.nist.gov/publications/interoperability-real-time-public-safety-data-challenges-and-possible-future-states

Generally, agencies should consider policies to define and understand what each agency will do with the information provided. No clear-cut formula exists to guide public safety agencies in making such policy decisions. As a starting point, agencies may apply many of the similar policies and procedures they presently use to share existing data, for example, dashcam video data or police/fire/EMS reports. Agencies will want to use their existing regional relationships – often developed during disasters or when creating Tactical Interoperable Communications Plans (TICP) – to discuss and make decisions regarding data sharing.

KEY QUESTIONS TO ASK

- **Does the agency have a clear understanding of what types, and how much, data needs to be shared?**
- **Does the agency have existing policies in place that can be leveraged to support PSIoT data sharing?**
- **Has the agency discussed data sharing needs, limitations and policies and procedures with regional mutual aid partners?**

From a technical standpoint, agencies should favor sensors and platforms that implement open standards (See Data Interoperability discussion in the previous Section).

In addition to the data itself, the format of the information and its meaning must be shared. The content of text information, particularly real-time IoT information gathered from *ad hoc* systems, can cause issues if agencies enter the information in different formats, interpret the output differently, or if typos occur.

4.7. Data Validity (Accuracy, Confidentiality, Integrity, and Accessibility)

First responders must have confidence in and trust the data output. Accuracy, integrity and time-sensitivity intertwine to ensure that data provided to the first responder accurately reflects their surroundings and real-time conditions. Most importantly, agencies must know the source of the data output and ensure that the source is authenticated and is a reliable source.

However, even with a trusted source, various conditions may cause IoT sensors and actuators to provide inaccurate readings. Sensors may stop working or become uncalibrated or damaged during an incident. Sensor data may be intentionally altered due to physical or cyber-intrusion. Or, the sensor may register an accurate reading, but conditions may be abnormal (e.g., match lighted near a heat sensor—giving a false reading indicating a building fire). Analytics and artificial intelligence technology may provide some protection against inaccurate data, such as flagging sensor readings data that are out of range compared with other available information.

As part of the planning process, agencies must determine what standards for data validity accuracy will be required for the system to achieve its purpose. When evaluating PS IoT systems, departments should follow these best practices:

- Ensure accuracy standards for of the data made available to first responder.
  - Devices must be appropriately maintained (calibrated, repaired, etc.) in order to provide accurate data.
  - Process for identifying and alerting operators of a sensor malfunction or abnormal data variance compared to other available data inputs. Users should be aware of the minimum and maximum values reported by the sensor.

- Carefully consider the level of maintenance required by a system when making purchasing decisions. The system manufacturer should provide standard maintenance requirements for the components of the system, and guarantee maximum variance ranges for data inputs

- Ensure that timeliness of the data is appropriate to meet first responder needs. A reading provided 30 minutes ago is probably no longer accurate to a first responder who needs to rely on near real-time updates.
  - Departments should consider a system's ability to provide time date stamp or minimum update periods to ensure that the information provided is accurate given the parameters of the system
- Ensure the integrity of the data provided to a first responder. Data integrity refers to the ability to maintain recorded data in its original state, preserving it from intentional or unintentional modification. Some requirements to maintain the integrity of the data include:
  - Physical security – ensuring that the physical location of the data remains secure, thus preventing unauthorized access to the data.
  - Software security-ensuring that only the appropriate people with the appropriate credentials have access to the data
  - Data quality-upon recording the data, ensure that it is entered as intended (appropriate format, range, etc.), save to a secure location and backed-up periodically
  - Understanding and ensuring that the source of the data is authenticated, i.e., is a trusted source.
- When data is accessed, ensure that it is identical to when it was recorded. This is the true marker for data integrity in a system.

KEY QUESTIONS TO ASK

- **Has the agency identified minimum requirements for data accuracy, authenticity, integrity, latency and real-time access to time sensitive data, etc.?**
- **Will the data need to meet chain of custody requirements for court cases?**
- **Does the agency understand the source of the data?**
- **How is recorded data stored and protected from intentional or unintentional modification? How long is it stored?**
- **For analytics, will the agency have access to both the raw data in addition to the analyzed information?**

4.8. PSIoT Physical and Wireless Security, Cybersecurity

As discussed in Chapter 4, physical security, wireless security and cybersecurity are critical to the success of PSIoT services, and security must always be considered from an end-to-end perspective.[22] The following considerations highlight a few of the most important PSIoT security and cybersecurity

[22] The primary onus for providing secure IoT devices other IoT ecosystem elements to Public Safety falls on the IoT device manufacturers and IoT communications providers (i.e. Verizon Wireless, AT&T, T-Mobile, Sprint). Industry testing and certification organizations such as CTIA, NTIA, GSMA and FirstNet have published or should publish extensive Certification Test Plans for connecting IoT Devices. There is much guidance available for commercial IoT certification and testing, but not for PS certification and testing. See Appendix One for useful references on the commercial side.

Top 5 IoT Networking Security Mistakes

5. **Not controlling access and authorization**
4. **Failure to update firmware regularly**
3. **Inadequate device awareness**
2. **Inadequate user training**
1. **Using default passwords**

Source: *NETWORKWORLD*
https://www.networkworld.com/article/3433476/top-5-iot-networking-security-mistakes.html

concerns that agencies may anticipate and plan for, with references to additional resources for more information included where available.[23]

PS IoT Physical Security

Physical risks are reduced if a device is primarily worn on a trusted individual and stored in a secure location when not in use. Risks increase when the devices are in a location that is not continuously monitored and are greatest when the IoT device is in a remote open location (e.g. a camera mounted on a utility pole or weather station sensor mounted on a building).

Physical access restrictions such as locks and tamper-resistant covers present the first line of physical defense. Multiple sensors may be located in the same enclosure and tamper-resistant physical switches placed inside of the enclosures or on the room's door provide immediate and accurate notification if the enclosure or door has been opened.

Special and/or proprietary connectors and dongles for the programming interface represent an additional hurdle for would-be attackers. Connections to the device should require password authentication for any access along with notifying the infrastructure that the configuration is being modified. In addition, time lockouts for repeated failed password attempts are beneficial. When the configuration is complete, all changes should be reported to the infrastructure.

IoT devices must have configuration reset protection, and should require configuration software to be connected to perform a reset of the device's configuration. This is especially critical for resetting passwords to default within the device. Default passwords and resetting to default remain a common method for compromising unsecured devices.

PSIoT Wireless Security

Wireless security requires the selection of equipment that supports the features necessary for secure communication and avoids outdated and/or vulnerable methods (such as those that cannot prevent replay attacks, or retransmission of valid commands). In addition, wireless data transmissions should be encrypted using a current NIST approved algorithm.

Additionally, the PSIoT device should authenticate to the PSIoT infrastructure and vice versa. This is typically done through a Public Key Infrastructure (PKI) configuration. While SIM cards can be used for authentication, particular care must be taken if the SIM is not embedded within the device.[24] The cellular infrastructure should be capable of notifying a public safety agency that a SIM has been

[23] A large number of reference materials is available to public safety from both federal government and private industry sources. We provide a library of documents in Appendix One as a starting point for additional research.
[24] Today, mobile smartphones and tablets use physical Subscriber Identity Modules (SIM) for authentication and encryption safeguards. IoT devices are often too small to include a physical SIM card, so an embedded SIM (eSIM) or integrated SIM (iSIM) is required for every new PS IoT device that will access the PSBN. For discussion of eSIM/ iSIM applied to IoT, see, *Industry backs eSIMs but needs to learn the benefits of iSIM deployment, says Arm survey* https://www.iot-now.com/2019/08/14/98197-industry-backs-esims-still-needs-learn-benefits-isim-deployment-says-arm-survey/

removed and placed into a different device, particularly from one device type to another (IoT device to a cell phone as an example).

Compatibility to legacy communications remains a risk as downgrade attacks can cause secure devices to transmit insecurely, such as the Dragonblood attack which downgrades Wi-Fi's WPA3 to WPA2[25]. The device's initial configuration should be protected since IoT devices are most vulnerable during this stage and any initial pairing (if required) and initial configuration should be performed in a secure location and by a secure method to minimize risks.

PS IoT Cybersecurity

Agencies must address Cybersecurity - in every single step within the communications ecosystem to avoid information compromise, including Sensors/Actuators, Hubs and Gateways, Clouds, and the User Interfaces. A compromise at any point in this path could easily and quickly allow unauthorized access to all areas, including systems and devices other than PS IoT. Cybersecurity risk should be addressed in both the planning and procurement phase and as part of ongoing operations and risk mitigation.

Planning/Procurement. Agencies are encouraged to begin the planning process with a review of existing security policies and identification of improvements necessary to ensure the security of the IoT service. NIST IR 8259 (Draft), *Core Cybersecurity Feature Baseline for Securable IoT Devices*, outlines specific features to request and where it coincides with various standards[26]. For overall cybersecurity, the NIST Cybersecurity Framework provides guidance, but agency policy should be followed. Sensors/Actuators should have the capability to authenticate themselves to the infrastructure and vice versa. Sensors/Actuators should have programming restrictions and should verify the integrity and the authenticity of any firmware updates. Whether the firmware should accept lower version numbers is left to the agency. The risk of a firmware downgrade introducing vulnerabilities versus implementation issues with the latest firmware needs to be weighed carefully. Commands to the device should be verified for authenticity along with ensuring that the message method is not being sent again (replayed), either through timestamps or random session keys.

Some sensors may have additional intelligence capabilities and use a common micro-Operating System (OS) or other common platform. These underpinnings should be identified and assessed before procurement and likely require additional monitoring to manage vulnerabilities in addition to managing firmware updates.

Operations/Risk Mitigation. The same physical and cybersecurity protections needed for PS IoT devices also apply to Hubs, Gateways and Sensors/Actuators. Utilizing additional encryption and/or VPN connections assists in mitigating certain cybersecurity threats. Cloud solution vendors must ensure that their networks remain secure and that any anomalies are dealt with swiftly and with transparency to the affected agencies. To the extent possible, access by cloud company personnel (if a private cloud) should be monitored and restricted to prevent unauthorized access or direct access to IoT sensor information. Cloud company personnel with network and device access should have an initial and recurring background check that match contracting requirements for the agency.

[25] https://papers.mathyvanhoef.com/dragonblood.pdf

[26] (DRAFT) NIST IR 8259 Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers, https://csrc.nist.gov/publications/detail/nistir/8259/draft

Cybersecurity operational controls for PSIoT infrastructure should build on those employed today for IT operations, but with some additional considerations. IoT cybersecurity risk management is identified within NIST IR 8228, *Considerations for Managing IoT Cybersecurity and Privacy Risks,*[27] a detailed resource for PSIoT cybersecurity planning. Risk assessments and risk management should always be aligned with the agency's overall IT strategy and policy.

KEY QUESTIONS TO ASK

- **Are there any hardcoded passwords in the device, and if so, can they be removed? Have all default passwords been changed?**
- **What management ports are open on the device?**
- **Are commands and information encrypted during transmission?**
- **Are commands verified for authenticity?**
- **Do the sensor devices have intrusion protection/detection or do the devices rely only on network-based security?**
- **What security updates are made for the device? Who is responsible for the updates?**
- **Does the service provider(s) have recurring cyber training in place for all network support staff?**
- **VPN support?**
- **Rate limitations – Flooding of messages**
- **Auditing/logging of configuration changes – rollback of unapproved configurations**

4.9. Costs

The Work Group has identified many ways that the efficiencies of PSIoT can reduce agency costs. However, these cost-savings will require some trade-off for start-up and operations costs. Although the Report does not attempt to resolve cost and funding challenges, in this section we highlight some of the PSIoT costs to agencies and ideas for identifying cost-mitigation opportunities.

Planning. This is probably the most important step in selecting a single or set of IoT applications, devices, and/or solutions. Upfront costs in the planning effort will pay big dividends through the rest of the process since there is consensus among stakeholders and a plan in place.

Procurement. Local procurement policy will dictate the means by which the desired applications, devices, and/or solutions will be obtained. This is usually by a request for proposal (RFP) process, a bid process, or direct purchase. It is recommended to research the feasibility of purchasing off an existing contract (state, local, cooperative agreement, etc.) to minimize time and effort. The RFP scope should include appropriate requirements, standards and metrics to ensure validity, reliability and interoperability of IoT data, which will save time and cost in the long term.

Operations & Maintenance. Operations and maintenance costs will be highly dependent on the level of complexity of the IoT solution, how many devices are involved, and how many users. Costs will be associated with the following tasks and replacements:

- Receive devices and review against contract/purchase order
- Install devices
- Install software (if necessary)
- Scheduled and unscheduled maintenance (including software updates and revisions as applicable)

[27] https://csrc.nist.gov/publications/detail/nistir/8228/final

- Replacement, typically every 7 years for devices with software and 20 years for devices with no software

Public Safety Staffing. Staffing needs will also vary according to the complexity of the solution, number of devices, and number of users. Some tasks may be extensions of current public safety staff responsibilities, some may require new skills.

Training. Training needs will be based on the gap between existing personnel's skills and what is needed for the IoT solution. Training may be needed in the following areas:

- IoT devices and applications
- Networks and network interface
- Data collection and storage mechanisms
- Data analysis and presentation

Funding. Funding for public safety IoT projects will primarily be locally-driven; but developing regional, collaborative projects between local governments, healthcare entities, and public-private partnerships will enhance effectiveness, uniformity, portability, and interoperability. New or ongoing "smart city" initiatives may make valuable partnership opportunities. This will enable agencies and governments to share costs and gain interoperability. Agencies should identify and monitor the activities of surrounding government initiatives, and especially the availability of Smart City grant funding, and consider ways to leverage these initiatives to lower cost and increase efficiency by partnering with other government users of IoT.

KEY QUESTIONS TO ASK

- **Public safety agencies must consider the full cost of acquisition, implementation, and the on-going operations.**
- **What are the costs and benefits of an agency-owned system vs. a third-party solution?**
- **How many additional staff to operate and maintain?**
- **Who provides training?**
- **Do the IoT solution's benefits justify the cost for equipment, training, maintenance and operations?**
- **Can the public safety agency leverage other initiatives to lower their cost or increase efficiency by partnering with other government users of IoT?**

ABOUT THE NPSTC PSIoT WORK GROUP

The NPSTC *Public Safety Internet of Things Work Group* ("PSIoT Work Group") was established in September 2016 and is charged with examining the current state of IoT, identifying public safety specific issues, focusing on the use of devices, sensors, and analytics, and highlighting specific issues and concerns for NPSTC's Governing Board review. The Work Group surveyed government research agencies such as NIST, PSCR and DHS, commercial vendors actively producing IoT technology and solutions, and experts from law enforcement, fire, EMS and PSAP/dispatch centers. A list of selected Work Group presentations is available in *Appendix Two*. Building on this research, the Work Group developed eight comprehensive public safety IoT "use cases" to highlight the use of PSIoT technology by first responders in the field. The Work Group also developed 22 assessment attributes— considerations used to focus discussion around each use case—which are referenced throughout this document.

Contributor Acknowledgement. NPSTC wishes to thank all the members of the Public Safety Internet of Things Working Group for their hard work in the development of this report. More than 200 members of the public safety community contributed to, or reviewed, this report including representatives from public safety agencies, individual first responders, academia, industry and government.

APPENDIX ONE: RESOURCES FOR MORE INFORMATION

NPSTC's PSIoT Work Group has compiled a large number of documents and links on the web page, http://npstc.org/IoT.jsp. These documents informed the Work Group during its initial research and investigation phase. Since that initial research in 2017, we have compiled these additional resources to assist agencies in PSIoT decision-making.

- Department of Commerce, National Telecommunications and Information Administration (NTIA), – *Fostering the Advancement of the Internet of Things, (*IoT Green Paper) *(January 12, 2017).* http://npstc.org/download.jsp?tableId=37&column=217&id=3886&file=DOC_IoT_Green_Paper_01122017.pdf
- NIST IR 8255, *Interoperability of Real-Time Public Safety Data: Challenges and Possible Future States*, by Britta Voss and Eric Anderson (June 19, 2019) [https://www.nist.gov/publications/interoperability-real-time-public-safety-data-challenges-and-possible-future-states]
- Georgia Technology Authority (GTA), PM-07-003.02 Statewide Data Sharing. Example policy on how any type of data sharing would be handled. https://portal.georgia.gov/document/statewide-data-sharing/download
- Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) – *The Internet of Things: Impact on Public Safety Communications* (March 2019) https://www.cisa.gov/sites/default/files/publications/CISA%20IoT%20White%20Paper_3.6.19%20-%20FINAL.pdf
- DHS, Next Generation First Responder (NGFR) Integration Handbook Version 3.0 https://www.dhs.gov/publication/st-frg-ngfr-integration-handbook-version-20
- DHS, Science and Technology (S&T) Directorate, *Assistant for Understanding Data through Reasoning, Extraction and Synthesis* (AUDREY). https://www.dhs.gov/publication/st-frg-audrey
- CTIA Internet of Things Cybersecurity Certification Program, https://www.ctia.org/news/ctia-iot-cybersecurity-certification-program-certifies-first-device
- ETSI releases first globally applicable standard for consumer IoT security https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security
- NTIA Stakeholder-Drafted Documents on IoT Security https://www.ntia.doc.gov/IoTSecurity

Security and Cybersecurity Resources

- GSMA IoT Security Guidelines, https://www.gsma.com/iot/iot-security/iot-security-guidelines/
- DHS CISA, *Steps to Safeguard against Ransomware Attacks*, https://www.us-cert.gov/ncas/current-activity/2019/07/30/steps-safeguard-against-ransomware-attacks
- NIST IR 8200 Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT) https://csrc.nist.gov/publications/detail/nistir/8200/final

- NIST IR 8222 Internet of Things (IoT) Trust Concerns (Withdrawn, lives on as draft white paper here: https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft)
- NIST IR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks https://csrc.nist.gov/publications/detail/nistir/8228/draft
- NIST IR 8196 Security Analysis of First Responder Mobile and Wearable Devices https://csrc.nist.gov/publications/detail/nistir/8196/draft
- DRAFT NIST IR 8259 Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers, https://csrc.nist.gov/publications/detail/nistir/8259/draft
- CTIA Internet of Things Cybersecurity Certification Program, https://www.ctia.org/news/ctia-iot-cybersecurity-certification-program-certifies-first-device
- ETSI releases first globally applicable standard for consumer IoT security https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security
- National Telecommunications and Information Administration (NTIA), Stakeholder-Drafted Documents on IoT Security (detailed information on security risks associated with upgradability and patchability of IoT devices). https://www.ntia.doc.gov/IoTSecurity
- IETF's RFC 8576 Internet of Things (IoT) Security: State of the Art and Challenges, https://datatracker.ietf.org/doc/rfc8576/
- Additional NIST cybersecurity documents:
    - Risk Management Framework: https://csrc.nist.gov/Projects/Risk-Management/rmf-overview
    - SP 800-18 Guide for Developing Security Plans for Information Technology Systems
    - SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
    - SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing
    - SP 800-154 Guide to Data-Centric System Threat Modeling
    - SP 1800-15 Securing Small Business and Home Internet of Things (IoT) Devices: Mitigating Network-Based Attacks Using Manufacturer Usage Description (MUD)
- *NETWORKWORLD, Top 5 IoT Networking Security Mistakes* https://www.networkworld.com/article/3433476/top-5-iot-networking-security-mistakes.html
- TELIT, *IoT Devices for EMS: What First Responders Need to Know* https://www.telit.com/blog/iot-devices-for-ems-what-first-responders-need-to-know/
- DHS Science and Technology Directorate (S&T), *Evaluating Mobile App Vetting Integration with Enterprise Mobility Management in the Enterprise*, https://www.dhs.gov/sites/default/files/publications/4681_evaluatingmobileappvettingintegrationwithemm-clean-r4-508c.pdf
- *IoTNOW, Industry backs eSIMs but needs to learn the benefits of iSIM deployment, says Arm survey* https://www.iot-now.com/2019/08/14/98197-industry-backs-esims-still-needs-learn-benefits-isim-deployment-says-arm-survey/

APPENDIX TWO: SELECTED PSIoT WORK GROUP TECHNICAL PRESENTATIONS

1. April 6, 2017 Meeting - Introduction to IoT and PS IoT, Barry Fraser and Dean Skidmore
2. May 4, 2017 Meeting - Department of Commerce IoT Green Paper – Travis Hall, NTIA
3. June 1, 2017 Meeting - Role of FirstNet in the IoT – Bill Schrier, Senior Advisor, FirstNet
4. August 3, 2017 Meeting:
    - Next Generation First Responder Internet of Things, John Merrill, Director, Office for Interoperability and Compatibility, Next Generation First Responder Apex Program, First Responders Group, DHS Science and Technology Directorate
    - Audrey for First Responders, Edward Chow, Mark L. James, George Paloulian, et al, NASA / Jet Propulsion Laboratory, California Institute of Technology
5. August 31, 2017 Meeting:
    - Presentation – IoT and Sensor Data and NG91, Roger Hixson, NENA
    - Presentation – APCO "Broadband Implications for the PSAP" Report, Barry Luke
6. Sept. 21, 2017 Meeting:
    - Presentations – Cybersecurity and Device Super Identity, DHS S&T
        - John Anil, Program Manager, Identity Management and Data Privacy Research, Development and Transition Program, Cyber Security Division, Homeland Security Advanced Research Projects Agency (HSARPA)
        - Chase Garwood, Program Manager, Cyber Security Division, Homeland Security Advanced Research Projects Agency (HSARPA)
    - Presentation – Multi-stakeholder Process: Internet of Things Security Upgradability and Patching, Megan Doscher, Senior Policy Advisor, NTIA
7. Oct. 5, 2017 Meeting - IoT and the Fire Service, Chief Ray Lehr, retired Assistant Chief with the Baltimore City Fire Department
8. Nov. 2, 2017 Meeting - “EMS Broadband: The Internet of the Tricorder & Other Lifesaving Things” – Kevin McGinnis
9. Dec. 7, 2017 Meeting - Presentation – Law Enforcement and IoT
    - Jonathan H. Lewin, Chief, Bureau of Technical Services, Chicago Police Department
    - Francesca Schuler, PhD, Motorola, Director, Command & Control Business, Software Enterprise
10. March 29th 2018 Meeting - Special Call - Industry panel on IOT networks and services
    - AT&T
    - Verizon Wireless
    - LinkLabs