# The Internet of Things:
# Impact on Public Safety Communications

The Internet of Things (IoT) is the network of physical devices and connectivity that enables objects to connect to one another, to the Internet, and exchange data amongst themselves.[1, 2] IoT allows connected devices to be sensed or controlled remotely across network infrastructures, creating opportunities for more direct, cross-platform integration and improved efficiencies for the transfer of data between devices.

***IoT goes beyond simply connecting objects to the Internet; it allows physical objects to intelligently self-identify and communicate with other devices, creating a new model of information sharing with a variety of potential applications.***

IoT presents undeniable implications for public safety communications. In turn, comprehensively addressing the ever-growing IoT environment presents a unique challenge to service providers, equipment manufacturers, and consumers. Harnessing network architecture changes and equipping everyday objects to be IoT-enabled will allow public safety stakeholders to maximize existing infrastructure investments and provide near-real time decision support experiences that can change how they operate.

## IoT Benefits

IoT-enabled devices can provide numerous benefits to public safety, as shown in Table 1. For example, a traffic accident response team could use the data collected from a variety of Internet-connected devices — such as the involved vehicles (e.g., speed sensors, occupancy sensors), surrounding infrastructure (e.g., utilities, traffic lights), and victims (e.g., health monitors, activity trackers) — to enhance their situational awareness and decision making before arriving on scene. In this scenario, first responders could utilize enhanced Multimedia Priority Services (eMPS) and Mission Critical IoT (MC IoT) devices to aggregate and gain access to this data.[3] IoT exponentially expands the realm of the possible while providing ubiquitous network connectivity, real-time response and control of autonomous systems, enhanced situational awareness, and process optimization.

| Benefit | Explanation |
|---|---|
| **Ubiquitous network connectivity** | In an IoT environment, devices can connect to everyday objects and each other to maintain a constant connection to the Internet. Resiliency and redundancy of communication paths – and the ability to communicate anywhere, any time (e.g., mobile command posts on demand) – can improve when a user is surrounded by physical objects employing standardized interactions with other IoT devices. |
| **Real-time response and control of autonomous systems** | Sensors can be embedded or integrated into nearly everything, and those sensors can be designed to perform analytics on the data being transmitted anywhere on the network. More advanced sensors can also calculate improvements to their own functions based on embedded machine learning algorithms |
| **Enhanced situational awareness** | Receiving accurate, secure, sensor-driven information can improve situational awareness. Incoming data can identify mission challenges and resources, and IoT devices can assist in processing and comprehending critical information. Public safety personnel can utilize a variety of Internet-connected technologies – such as drones, robots, and artificial intelligence (AI) – to gather information while maintaining a safe distance from immediate danger. |
| **Process optimization** | Cloud-enabled devices have already created an environment of nearly seamless information availability. IoT is an extension of that environment, but to every device and for all information. IoT devices can also provide decreased latency, allowing users to send and receive very high volumes of data. With IoT, not only humans, but also machines and AI, can participate in the decision-making and analysis process. |

**Table 1. IoT Benefits (Non-Comprehensive)**

[1] *Internet of Things Global Standards Initiative*. International Telecommunication Union (ITU), 2015. https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
[2] Brown, Eric. *Who Needs the Internet of Things?* Linux, 2016. https://www.linux.com/news/who-needs-internet-things
[3] Enhanced Multimedia Priority Services (eMPS) and Mission Critical Internet of Things (MC IoT) devices may require similar (or competing) resources to what is currently used by priority voice and data services (e.g., licensed LTE frequency bands, signaling channels, traffic channels).

## IoT Concerns

The challenges to implementing IoT within the public safety context are substantial. From cybersecurity to privacy risks, IoT is inspiring profound concerns for society in the Internet age. Addressing these concerns will require the collaboration of government, industry, and academia to provide ever-evolving risk assessment and mitigation of these consequences before they occur.

### CYBERSECURITY

- **Expanded attack surface:** Cars, refrigerators, medical devices, and gas meters are now potential entry points for attack. Malicious actors continue to mount larger scale attacks against a variety of Internet-connected devices.
- **Vulnerable legacy equipment:** Devices and systems not previously "connected" often have security, operability, and performance issues when transitioning to the "connected" state of IoT. These systems were never intended to interact with unauthorized users enabled by remote management. As a result, many of them do not have passwords, use default passwords, or have easily deduced passwords.

### SCALE

- **Flood of input:** Not all information collected from IoT devices (e.g., parking meters, intelligent cars, robots, smoke detectors) is useful during a public safety event. In fact, much of it can be distracting or, worse, provide an inaccurate perspective of circumstances.
- **Torrent of data:** Analytics help to capitalize on the value of the volumes of data provided. Low-powered "things" may not have the computational resources for such activities, resulting in a web of backend systems/databases, all of which must be secured and managed. Also, traditional solutions like encryption require rigorous key management and, when trillions of "things" are involved, management of these keys can be cumbersome.

### CONGESTION

- **Congested networks:** Providing sufficient coverage and capacity for trillions of devices on network backhaul and core infrastructure is an undeniable risk. Though standard network management techniques, such as prioritization, queuing, and offloading, will assist in managing the load, it is imperative that incentives be provided for conscientious resource use, proper updates, and patch management.
- **Competition for resources:** Public safety and national security and emergency preparedness (NS/EP) communications will need to be routed to more resilient sites, technologies, and frequency bands with customized priority and preemption schema and network slicing, the specifications for which have not yet been determined.

### REGULATORY POLICY

- **Lack of policy/guidance:** Developing regulatory policy that clearly outlines the authority regarding access, use, and responsibility over IoT devices is challenging. In addition, the scope of IoT's impacts may be too broad to properly develop policies that address NS/EP and public safety operational mission requirements.
- **Privacy:** Ensuring individual privacy is imperative when collecting, distributing, and sharing personally identifiable information (PII) and other sensitive information. Best practices for safeguarding PII in IoT networks have not yet been codified in the public safety mission space.

### INTEROPERABILITY

- **Lack of cohesive standards:** A key premise of IoT is the interconnectedness between devices and other infrastructure. The complexity IoT ecosystems and divergent interests in IoT across international standards bodies are an obstacle to universal standards development.
- **Insight into industry efforts:** The rapid rate at which wireless service provider/vendors are planning and deploying IoT networks directly impacts public safety traffic, security, and feature development, and requires significant coordination between the public and private sectors.

### HUMAN IMPACTS

- **Potential health impacts:** Use cases regarding the interaction between humans and IoT devices, and IoT's potential impacts on user motivations, actions, and emotions have not been fully explored. The collaboration of humans and "things" can be highly beneficial, but can also carry unintended consequences on a user's intellectual and emotional well-being.
- **Physical risks:** IoT also has the potential to introduce physical risks. Just as smartphones have been evaluated for electromagnetic radiation risks, the long-term, heavy-use physical experiences of IoT devices are not yet known.

**Figure 1. IoT Concerns (Non-Comprehensive)**

## Harnessing IoT in the Public Safety Context

Public safety communications have already been adapting to IoT. Use of a smartphone, tablet, laptop, or navigational system has introduced some of the benefits and risks of an IoT environment. To ensure IoT can effectively support public safety communications, the community should promote information sharing, collaboration, and training, while also addressing the associated cybersecurity, privacy, and system design considerations.

***Information Sharing and Collaboration.*** Industry, academia, and public safety personnel across all levels of government must work together to ensure a cohesive framework for adopting IoT in the context of public safety, to include developing actionable guidance and standard operating procedures (SOP) on IoT governance, technology advancements, and service-level agreements.

Particularly in an environment where connectivity to trillions of devices can result in increased security, function, and performance risks, it is critical that all parties collaborate to accelerate the process of inserting public safety requirements into IoT discussions. Similarly, the increased availability of unstructured, uncoordinated information requires that public safety organizations work with IoT device vendors to counteract the potential organizational liabilities posed by managing this massive information overload.

As a result, the public safety community should share as much information as possible regarding their ongoing work, research, and development efforts related to IoT. Moreover, the community should continue to use existing resources to: (1) support further investigation into IoT's public safety applications; (2) provide subject matter expertise during standards development; and (3) participate or assist in the execution of any needed case studies of the implications of IoT on public safety communications. Such resources include existing government programs/working groups,[4] industry consortiums,[5] and independent practitioner groups.[6]

***Training and Exercise Planning.*** To promote the proper implementation of IoT, public safety officials will need to collaborate with a variety of stakeholder groups to stand up comprehensive training and exercise programs focused on effectively implementing IoT in support of public safety communications. These training and exercise plans will need to address/consider:

- The information flow to/from IoT devices to streamline public safety information sharing;
- How to best identify, provision, configure, connect, integrate, and interoperate IoT devices in different scenarios (e.g., daily operations versus active shooter); and
- The network conditions needed to guarantee that functional, performance, and operational requirements for leveraging IoT are met and do not negatively impact existing non-IoT emergency communications.

The key to successful training and exercise planning will be assessing the quantitative and qualitative value of IoT device interaction with human behavior and operational value.

***Cybersecurity.*** IoT stretches the limit, scale, and scope of many traditional cybersecurity products and practices. One of the most important aspects of cybersecurity in an IoT environment will be a comprehensive review of the standardized protocols and proprietary mechanisms connecting devices to and through the Internet. Not only will these mechanisms need to be secure, but device manufacturers and system administrators will need to understand the importance of cybersecurity in an IoT network environment, even when it impacts the simplicity and efficiency of their products.

Telecommunications service providers have recently begun to make strides towards developing actionable cybersecurity best practices for IoT. In August 2018, CTIA announced the creation of a new security

[4] Potential Government groups/programs include: SAFECOM, National Council of Statewide Interoperability Coordinators (NCSWIC), National Security and Emergency Preparedness Communications Executive Committee (NS/EP ExCom), and the National Institute of Standards and Technology (NIST) Cybersecurity Program for IoT
[5] Example industry consortiums include: ITU, Industrial Internet Consortium (IIC), and Institute of Electric and Electronics Engineers (IEEE)
[6] Practitioner groups include the National Public Safety Telecommunications Council (NPSTC)

certification program targeting the IoT space, which aims to offer "certification for IoT devices built from the ground up with cybersecurity in mind." When implemented, the program will seek to "protect consumers and wireless infrastructure, while creating a more secure foundation for…IoT applications."[7]

There are other existing cybersecurity practices that can be used in support of IoT. Data protection – at rest and in transit – has mature solutions such as encryption that can begin to address the cybersecurity risks posed by these technologies. Secure product and software development guidance also exists and may require only minor modifications to encompass IoT for public safety. Moreover, current network management techniques, such as virtual private networks, access control systems, firewalls, segmentation, and continuous monitoring and intrusion detection systems, can be adopted to decrease public safety networks' vulnerability to IoT cybersecurity threats.

IoT poses significant impacts on public safety cybersecurity governance as these devices increase the potential attack surface – both physical and virtual – of a network, and the complexity of user authentication and identity management. To counteract these consequences, the public safety community will need implement strict guidance regarding IoT device access to public safety wireless networks. New encryption schemes may also be required to protect PII traversing these devices to avoid compromising public safety operations. Further, SOPs will need to be developed for tracking network/device vulnerabilities and distributing patches once they are known.

***Privacy.*** To address the privacy concerns posed by IoT-enabled devices, it is important to combine self-regulation with strong data protection and privacy laws. Any laws regarding individual data use and collection conducted by IoT devices should include inputs from vendors regarding their feasibility as a means of promoting transparency. Most importantly, regulation must allow enough flexibility to capitalize on the innovation of data collection and analysis, without infringing on individual privacy.

***System Design.*** Prudent lifecycle management of IoT devices will require that service providers and device manufacturers work with public safety practitioners to develop cost-effective solutions. It is imperative that public safety requirements are incorporated into IoT devices to better enable these stakeholders' ability to collect large amounts of information on during an incident, parse through the data received, and quickly distill it into an actionable response plan for first responders. Vendors will need to consider appropriate spectrum use, network congestion, personnel access, sources of interference, power consumption, service reliability, resilient connectivity, and individual privacy when implementing their designs in support of public safety communications.

Resiliency. IoT devices and the networks supporting them must also provide the needed communications resiliency and redundancy required by public safety. In response, government, practitioners, service providers, and device manufacturers should work together to determine the incentives needed to ensure public safety requirements are accommodated into core network and system designs.

User Education. Stakeholders will need to determine how leveraging MC IoT and eMPS devices can allow public safety users to better meet their operational requirements, including secure, resilient, and continuous communications with the public, critical infrastructure owners and operators, and non-governmental organizations.[8] In addition, the public safety community must remain cognizant of the security, scale, and congestion challenges associated with IoT. Most importantly, IoT devices must be easy to manage by those using them in the field; therefore, vendors will need to assist the public safety community in educating first responders on how to effectively control and troubleshoot these devices.

Backhaul. IoT interactions may have different networking requirements than what is currently provided by many broadband network designs (e.g., low power with extended operation on batteries, low data rates with sensor reports rather than audio/video interaction, low latency to facilitate rapid response) and

[7] Dano, Mike. *AT&T, Verizon, T-Mobile, and Sprint rally around Security Standard for IoT*. FierceWireless, 2018. https://www.fiercewireless.com/iot/at-t-verizon-tmobile and-sprint-rally-around-security-standard-for-iot

[8] These efforts may require influencing the policy, priority, and preemption schema deployed by wireless carriers also supporting existing priority communications networks and services (e.g., Wireless Priority Service [WPS], the First Responder Network Authority [FirstNet], 911/Next Generation 911[NG911], alerts and warnings systems).

are asymmetric with many devices sending more data than they receive. These characteristics will determine which IoT devices should be on stand-alone networks using unlicensed spectrum versus which ones should be supported by integrated networks using licensed spectrum with support from commercial broadband networks. Making this determination will require identifying which IoT devices will run critical IoT applications versus massive IoT applications.[9, 10] Since the data generated by each device is important and conclusions drawn from aggregated data could prove valuable, any post-analytic, machine-to-machine interactions based on this data may warrant prioritization.

Prioritization. The effective prioritization of IoT-based communications necessitates the development of strong policy. Therefore, public safety stakeholders must collaborate with industry to technically assess and recommend what policy and priority/preemption schema should be followed to ensure that increased connectivity does not impact existing priority communications. Within the context of public safety communications, possible prioritization categories include, but are not, limited to the following:

| | |
|---|---|
| **Continuous Priority** | • Prioritizing communications anytime an IoT device is used.<br>• ***Example:*** Communicating patient readings between an ambulance and a hospital. |
| **Geographic Priority** | • Prioritizing communications to/from devices within a limited geographic area.<br>• ***Example:*** An electric company needs expedited readings from meters near a blackout zone. |
| **Temporal Priority** | • Prioritizing communicatons at certain times of the day or during specific events.<br>• ***Example:*** Prioritizing reports from traffic signal monitors during rush hour. |
| **Triggered Priority** | • Allowing devices to self-prioritize.<br>• ***Example:*** A video camera triggers priority when detecting group of armed individuals. |
| **Declared Priority** | • Authorities declaring which types of IoT communications are prioritized.<br>• ***Example:*** During a manhunt, a police department prioritizes the collection of Twitter messages containing information about the suspect being pursued. |

**Figure 2. Potential IoT Prioritization Categories (Non-Comprehensive)**

Governance. Over the next five years, IoT will greatly influence the governance of a variety of public safety communications systems and capabilities. Therefore, the public safety community will need to develop governance to accommodate the increased proliferation of these IoT-based networks. An additional layer of complexity will be required as IoT divides into massive IoT and critical IoT applications. Further, data interoperability and real-time and predictive analysis of sensors input must be reconciled in governance policy when leveraging this data in the public safety responses.

## Next Steps

The life-and-death costs of remedying security vulnerabilities and connectivity issues while operating in an IoT environment are too high for public safety to remain an observer. Measures must be taken now to ensure that public safety personnel can expeditiously and proficiently use IoT devices to carry out their missions. To accomplish this, all levels of government, industry, and academia must work together to investigate the impacts of IoT on public safety communications and develop best practice guidance that will allow public safety personnel to harness these technologies' benefits, while also preempting or mitigating the risks

[9] In this context, massive IoT applications refer to the "connection for a large number of devices and machines (potentially on the order of tens of billions) on a regular basis," while critical IoT applications are "other IoT applications which require high availability, coverage, and low latency…and could be enabled by LTE or 5G." For more information, please refer to: http://www.5gamericas.org/files/8415/1250/0673/LTE_Progress_Leading_to_the_5G_Massive_Internet_of_Things_Final_12.5.pdf

[10] Critical IoT applications require reliable delivery of information, over a high availability infrastructure with very low latency (e.g., traffic safety, remote healthcare). On the other hand, massive IoT networks 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, automobile traffic supervision). In some cases, these devices may have value of data from each sensor may be too low to warrant priority. Many IoT applications are likely to have rich feature sets, with each IoT device sending and receiving large amounts of data (e.g., search and rescue robotics, drones). However, even low data rate IoT devices – such as earthquake sensors – will require low latency and priority when operating on shared networks.

associated with wide-scale deployment. Any guidance regarding IoT usage in support of public safety communications should:

- Be developed in collaboration with the broader public safety community;
- Encourage available, resilient, prioritized, and secure communications;
- Align with operational requirements and evolving wireless broadband technologies (e.g., 5G);
- Consider/participate in existing policies, technical standards, testing, trials, and vendor research and development trends;
- Incorporate public safety user community use cases and operational requirements for IoT; and
- Provide direction on IoT issues and concerns to be addressed through governance, technology advancements, service agreements, SOPs, and/or training and exercises.

These best practices should also outline high-level system design, cybersecurity, and privacy considerations for deploying IoT in support of public safety communications. Practitioners could use these best practices to familiarize themselves with how to deploy these increasingly connected and improve their organization's use of IoT devices.

## Additional Resources

Below is a non-comprehensive list of publications and initiatives that provide additional information on the current state of IoT and its potential applications for public safety communications.

| Resource | Overview |
|---|---|
| ***Internet of Things: Status and Implications of an Increasingly Connected World (2017)*** | In this report, the U.S. Government Accountability Office (GAO) provides a high-level introduction to IoT and "describes: (1) what is known about current and emerging IoT technologies; (2) how and for what purpose IoT technologies are being applied; and (3) potential implications of the use of IoT technologies."[11] |
| ***Industrial Internet of Things Connectivity Framework (2018)*** | The Industrial Internet Consortium (IIC) developed the Framework to help "practitioners unlock data in isolated systems; enable data sharing and interoperability between previously closed components…and subsystems; and to accelerate the development of new applications within and across industries."[12] |
| ***Considerations for Managing IoT Cybersecurity and Privacy Risk (2018)*** | The National Institute of Standards and Technology's (NIST) Cybersecurity Program for IoT issued this draft guidance to provide "practical risk management considerations for IoT product selection, deployment, and operation" within federal information systems.[13] |
| ***Next Generation First Responder Integration Handbook (2018)*** | In this handbook, the DHS Science and Technology Directorate (S&T) offers a standards-based architecture that can be used to help guide industry in the development, design, test, and integration of commercially-developed technologies (e.g., IoT-enabled devices) with existing first responder infrastructure.[14] |
| ***Strategic Principles for Securing the Internet of Things (2016)*** | In 2016, DHS developed these strategic principles to better "equip stakeholders with suggested practices that help to account for security as they develop, manufacture, implement, or use network-connected devices."[15] |
| ***IEEE IoT Initiative's IoT Scenarios Effort*** | As part of its larger IoT Initiative, the Institute of Electrical and Electronics Engineers (IEEE) has created a platform to allow its partners to "engage with [one another on] use cases, service descriptions, business models, and reference implementations that will be key to developing a vibrant IoT industry." To date, several participants have proposed a variety of scenarios with a public safety communications nexus.[16] |

**Table 2. Additional Resources (Non-Comprehensive)**

[11] U.S. Government Accountability Office (GAO) Center for Science, Technology, and Engineering. *Internet of Things: Status and Implications of an Increasingly Connected World*. GAO, 2017. https://www.gao.gov/products/GAO-17-75
[12] IIC Technology Working Group. *Industrial Internet of Things Connectivity Framework*. IIC, 2018. http://www.iiconsortium.org/IICF.htm
[13] NIST Cybersecurity Program for IoT. *Considerations for Managing IoT Cybersecurity and Privacy Risk*. NIST, 2018. https://www.nist.gov/sites/default/files/documents/2018/04/13/iot_program_discussion_draft_april_2018.pdf
[14] DHS Science and Technology Directorate (S&T) First Responders Group Apex Program. *Next Generation First Responder Integration Handbook (Parts 1 – 3)*. S&T, 2018. https://www.dhs.gov/science-and-technology/ngfr/handbook
[15] *Strategic Principles for Securing the Internet of Things*. DHS, 2016. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf
[16] IEEE IoT Initiative. *IoT Scenarios*. IEEE, 2018. https://iot.ieee.org/iot-scenarios.html