



NASPO[™] TECH NEXT SERIES

The Internet of Things (IoT)

In this edition of the Tech Next series, we will explore:

Quick Stats

Examples of IoT in the Public Sector

Considerations and Implications

Internet of Things Procurement Considerations Checklist

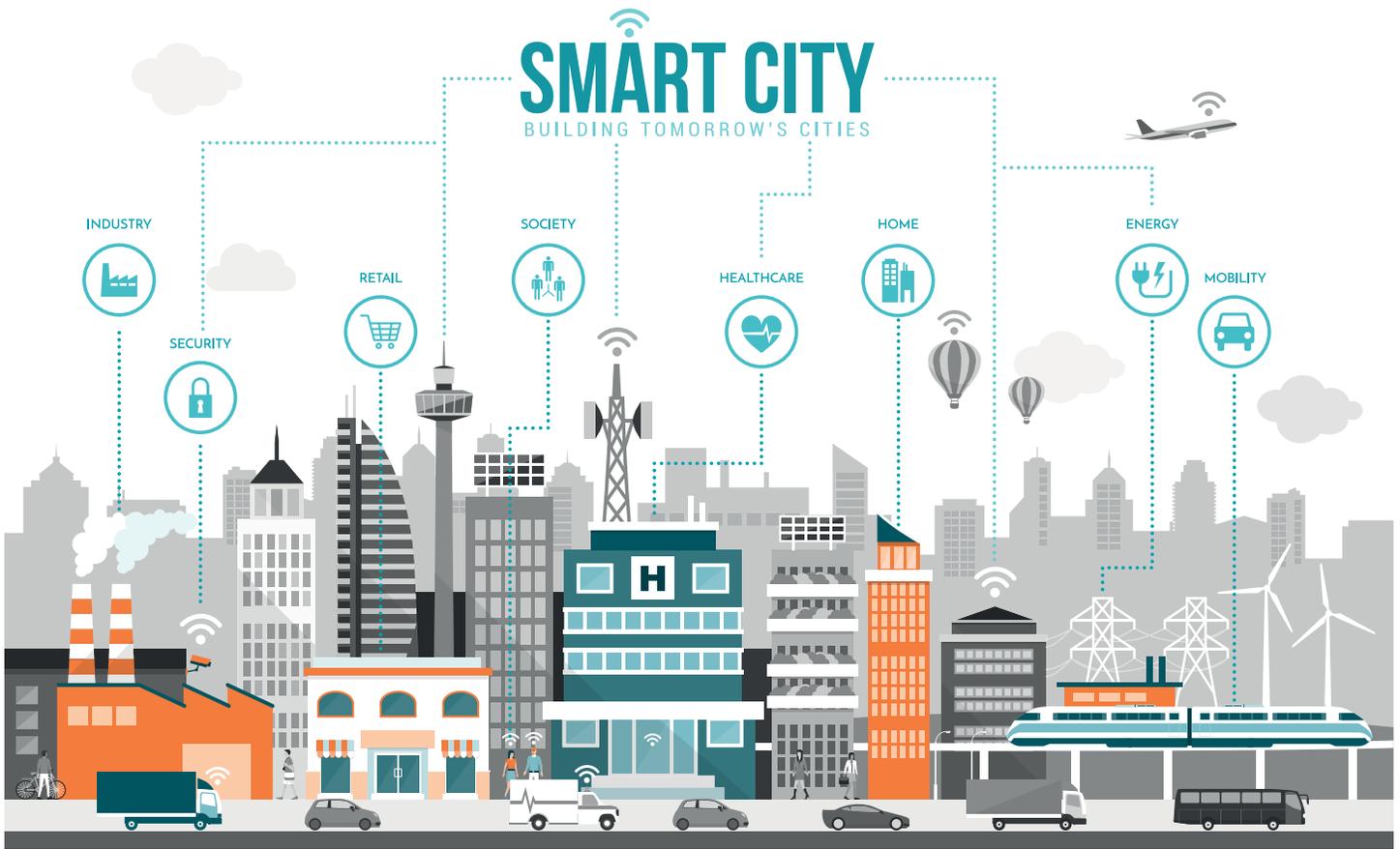
ARE YOU READY FOR WHAT'S NEXT?

Broadly speaking, the Internet of Things (IoT) is the digital connection of people, processes, data and things. Using the internet, IoT creates a seamless network of communication and productivity known as a smart connection. Governmental entities and municipalities that have embraced IoT are often referred to as Smart Cities or Smart States.



www.naspo.org





Governments employ IoT for diverse purposes, from monitoring building efficiency and traffic flow to tracking wildlife populations. Smart Cities or States may use IoT technologies like meters or sensors to collect and report data to city personnel who can then analyze and alter processes to benefit citizens. In turn, citizens can leverage connected technologies to access services, solve problems, increase efficiency, or save resources. Because all things are connected through the internet, these evidence-based changes can be made almost instantaneously.



Quick Stats



IoT is also called Internet of Everything (IoE), Industry 4.0 and smart connectivity, among many other terms.



In 2020, the global IoT smart cities market size is expected to grow at a compound annual growth rate of 18.1%, reaching \$260 billion by 2025.



Forecasting shows more than 75 billion IoT connected devices in use by 2025.



IoT's real-time routing and other based operations around IoT can lead to a 17 percent improvement in operating efficiency in logistics routing.



In 2019, 99% of companies participating in this study by Gartner Research maintained or increased their budget for IoT.



93% of enterprises will adopt IoT technology by the end of 2020.



Estimates show \$14.2 trillion added to the global economy by 2030 from the Industrial Internet of Things (IIOT).

Examples of IOT in the Public Sector

Transportation Systems

Upgrading state transportation systems to incorporate self-driving cars can lead safer roads and more efficient public transportation system. Self-driving cars work by connecting radar sensors to a network where they communicate with other sensors in other cars. This allows all the cars in the system to automatically detect each other and prevent accidents. According to [the National Highway Traffic Safety Administration \(NHTSA\)](#):

- 94% of severe automobile accidents are caused by human error.
- Human error automobile accidents accounted for 36,560 deaths in 2018 alone.
- A 2010 study by the NHTSA found that these accidents accounts for \$242 billion in economic activity.



Electric vehicles have become a viable option in fleet management and rely heavily on IoT connections to perform at maximum productivity. Vehicles continually update maps via a connected GPS system, vehicle maintenance issues can be fixed via “over-the-air” software downloads—much like updating a smart phone to resolve glitches—**and can communicate with connected manufacturers to order parts for repair or schedule routine maintenance.**

Smart parking systems allow users to find available parking spaces based on sensors located in parking spots. An electric vehicle can connect to the parking sensors, which instantly alert the driver as to how many parking spots are open and guide the driver to those spots through communication with the vehicle’s GPS system. This not only saves time but allows for data collection during big events to analyze the flow of traffic and help prepare for other large events throughout the state. A [McKinsey & Company study](#) found that automating vehicles could save the average person 50 minutes each day in their commute and reduce the need for parking space by 5.7 billion square miles nationwide.

[Read about Venture Beat’s Take on IoT and Transportation.](#)

Healthcare



Through IoT-connected devices such as smart phones and tablets, online appointments with doctors and self-service portals where patients can pay medical bills can reduce wait times and make travel to the doctor's office for a minor issue unnecessary. Upgrading to IoT-connected medical devices in state hospitals will also improve data collection and record keeping. This can lead to better overall care, fewer return visits, and reduced administrative demands on doctors and nurses—all of which save the state money.

A Medication Dispensing Device, which is tailored toward elderly patients who often struggle with maintaining regular dosages on their own can auto-fill dosage cups to ensure patients receive the proper amount per intake, and can alert physicians or family members if a dosage is skipped or a prescription requires a refill.

Business Insider's Evolution of Healthcare Technology

Public Safety



Connected IoT devices can communicate among ambulances, doctors' offices, police dispatch and fire departments to ensure that all necessary authorities are receiving the same information and updates during a crisis. This connectivity also standardizes the communication, ensuring first responders are speaking the same language—making for more effective communication between differing entities with specialized language.

Smart street-lights can conserve energy and save electricity by adjusting the brightness of the lights based on the presence of cars or pedestrians. Sensor-driven, smart street-lights can also collect data, trigger cameras to record video or alert officials in the case of suspicious activity. Smart streetlights could even benefit from a connection to parking sensors, remaining lighted if a sensor detects a car in the nearest parking spot. This could help deter crime and enhance the safety of citizens.

Read more about how police departments benefit from IoT

Workforce Implications

For example, California's Innovation Lab exists within California's private cloud service, or CalCloud, and allows "programmers to experiment with developing Web applications using open source code." If an innovator's code is considered a success, **California can use this code to solve statewide issues where applicable**.

Updating technology devices such as laptops, cell phones and workstations within state agencies will attract a more innovative workforce. Students graduating from universities that offered IoT technology labs will be drawn to jobs that employ similar devices, and can continue to provide a **fresh perspective on how connectivity benefits the state**. Individuals who join state government after working in the private sector may bring valuable experience and new and innovative problem-solving methodologies with them based on technologies used in their prior workplace. Having connected devices will allow these employees to seamlessly transition from one sector to the other.

Industry Week asks: Are Smart Cities a Way to Attract a Smart Workforce

State Facilities Maintenance

IoT technologies within facilities management reduces costs, risks, and improve the occupants' experience. Like technologies used in smart homes, but on a commercial scale, facility components such as HVAC, lighting, security and/or plumbing can be connected and in constant communication. For example, if an issue occurs with

the HVAC in a state building, the device could either correct itself through a software update or alert a facilities manager of the exact issue. This process reduces the risk of the HVAC leaking or shutting down for several days, allows for monitoring over weekends and holidays, and reduces the costs associated with manually finding and fixing the issue.

In the private sector, [IBM's TRIRIGA](#) automates demand and preventive maintenance services, tracks and evaluates facility component performance, such as HVAC or security systems, to identify possible issues or processes that can be improved to ultimately extend the lifecycle of these systems.

[Read more about IBM's TRIRIGA program](#)

Illinois: The Smart State

In 2016, Illinois began implementing changes that would help them become a Smart State, modeled after what local governments are doing to turn their cities into Smart Cities. For Illinois, adopting several types of connected technologies—including IoT devices—was one of the first steps down that path. Illinois is creating a template that could be used and applied in other states, leading to a smarter and more connected country. Three main ways in which state agencies can support the transition to a Smart State were identified through a collaborative effort, which included representatives from the state's Department of Innovation and Technology, the Smart Cities Council and Chicago-based business incubator UI Labs. Those recommendations include:

1. Fostering economic development and attracting innovative companies to Illinois;
2. Using IoT to improve state government operations; and
3. Helping local governments start using the technology as well

In October 2016, when these recommendations were established, there were approximately 90 companies in the Midwest categorized as "IoT companies." As of 2019, [that number has increased to 156 in the Midwest](#), the majority of which are in Chicago. Establishing itself as a Smart State has benefitted Illinois by improving the IoT market, creating IoT jobs, and becoming more connected as IoT devices are created and implemented within the state.

Illinois' first Smart State initiative procurement was for smart street lighting for Illinois municipalities. Under the guidance of Illinois' CPO Ellen Daley, the Department of Central Management Services produced an RFP for a statewide master contract available for joint purchasing by local governments and municipalities to provide upgraded street lighting.

In brief, the RFP seeks:

- Turn-key services for street-light upgrades to light-emitting diode (LED) luminaires, with implementation and financing options;
- Luminaires; and
- Adaptive controls for Illinois municipalities, forming the basis of a smart infrastructure and supporting the inclusion of additional value-add features

To see an example of specifications for such a project, you can view the RFP below.

[Click here to view the RFP](#)

CONSIDERATIONS AND IMPLICATIONS

Security

Citizens may be concerned that too much data means too much personal or financial information in the government's hands, or a lack of privacy. States should remain transparent about how data is being collected and used, and vigilant about cyber security measures to protect that data.

Security is a huge concern when implementing the IoT model in state-level purchases. Although increased connectivity is valuable to citizens, it also poses the risk for both malicious and unintentional breaches. If several devices are connected, the malicious breach of one device means the breach of many other devices, and all data stored on these devices is at risk of exposure. Unintentional breaches, such as a power outages or shutdowns, could lead to one or more devices losing connectivity, interrupting a web of IoT-connected devices.

When purchasing IoT-enabled devices, procurement officers should consider what type of security is necessary to protect against malicious attacks and what can be done in the case of an intentional or unintentional breach.

New policies should be drafted to ensure all connected devices are protected from cyber breaches and what the statewide procedure will be in the case of a breach. States should revisit these policies annually or on another pre-determined basis to ensure they remain valid and up to date.

Compatibility and Connectivity

IoT-specific jargon, such as "cloud computing" "big data" or "sensor networks" should be included and defined in IoT policies to ensure all parties are on the same page. Procurement officers should work with their information technology officers to determine standardization, such as a software platform or broadband specifications. Doing so will help ensure that all devices can connect, avoid costly mistakes and improve processes rather than slow them down.

Broadband connectivity must be reliable and robust to seamlessly support IoT devices. Procurement officers should consider what is necessary to support this level of connectivity, such as staff members who can produce an RFP for large-scale broadband systems. In addition to internet connectivity, electricity must flow continuously through some devices to ensure performance without error or interruption. States may need to consider redistributing or changing their energy supply level to accommodate this demand. Cost sheets should take into consideration both the power supply panels and software upgrades necessary to ensure continuous power supply.

Implementation

The lifecycle of an IoT device should also be considered during the procurement process. For example, solar road panels may only need to be replaced every 10-20 years. However, the software that collects or interprets data from solar panel roads may become outdated within two years. It is important to know these potential issues upfront to plan for any interruptions or necessary replacements. When identifying specifications, it is important to think long term and consider the overall cost of ownership rather than the purchase price of an individual IoT device.

Rather than procuring all elements of an end-to-end IoT system at once, procurement staff should consider procuring devices in a phased approach to allow for integration and testing of compatibility before procuring another component. Procuring in smaller stages may also increase competition by allowing more than one vendor an opportunity to bid at each stage, but can limit competition if you choose a device that is not compatible with any other system or device. This could unintentionally set up a sole source arrangement and could lock the state into contracts that do not promote the long-term goal of establishing an IoT connection state-wide.

Workforce

Some more traditional jobs may be lost to automation, while others will be created to support and maintain complex technologies. As factories and even construction sites are moving toward an IoT business model, procurement officers should review preference laws to ensure small, women-owned and minority-owned (SWAM) businesses are considered.



INTERNET OF THINGS PROCUREMENT CONSIDERATIONS CHECKLIST

Having a seamlessly connected Smart State is great in theory, but every purchase has its considerations. The following checklist includes several aspects a state CPO should consider when procuring IoT devices or systems. Check it off!

- Have you developed or considered a cyber breach policy with your chief information officer (CIO) or chief information security officer (CISO)?
- Have you collaborated with your CIO or CISO to ensure the IoT device you are procuring will solve the issue at hand?
- Have you considered what technology foundation or platform you may need? For example, will all the devices run on the same software?
- Have you considered the workforce implications? Have you considered preference laws?
- How will this procurement impact SWAM (Small, women-owned and minority-owned) business?
- Are you ensuring that each device you procure is compatible and will seamlessly connect with all other devices?
- Does the state have the infrastructure in place to ensure this procurement will succeed?
- Have you researched local entities that have adopted Smart City regulations?
- What were their lessons learned?
- Have you considered this long term, in terms of budget implications or future commitments?
- Are you limiting yourself in terms of competition?
- Ensure that whatever device your state needs can be procured through a fair and open competition.



Suggestions for Future Reading:

- [Cyber Liability Insurance 101, NASPO](#)
- [Philadelphia: Smart Cities Council Readiness Challenge Grant, Philadelphia Government Press Release](#)
- [Value and Vulnerability: The Internet of Things in a Connected State Government, NA-SCIO](#)
- [10 Cyber Security Steps to Protect Smart City Technologies, State Scoop](#)
- [Securing Smart Cities, Trend Micro](#)
- [Illinois Partnership to Bolster Talent Pipeline Grow Smart State Initiatives, GovTech Magazine](#)
- [Internet of Everything: \\$4.6 Trillion Opportunity for the Public Sector, Cisco](#)
- [Internet of Things in Healthcare. Business Insider](#)