Your Foundation

How is your city connected?

As IoT devices autonomously capture data, intelligently self-configure to events in their environment and become active participants in public, commercial, scientific and personal processes, broadband availability will be key to success. These networks will be the backbone of your project's infrastructure.

As you begin your smart cities project, evaluate connectivity in your community.

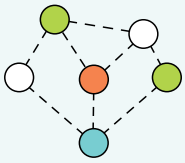
- ☐ Look at the networks and contracts: fixed broadband, mobile wireless service and/or others. How many are there and for what services?
- ☐ Evaluate your residents' connectivity. How many have broadband/wireless?
- ☐ Does your community understand the economic impacts of broadband availability?
- ☐ What are the plans for future broadband and 5G?
- ☐ What kind of permits do you require? Who could benefit from a "dig once" policy?

With a basic understanding of how city systems are connected, you'll be able to evaluate which type of network to use to connect your project.

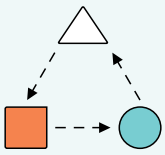
Think about your coverage and range needs. To decide what level of network connectivity you will need for your project, consider the distance, robustness and security required to power your application.

How fast does your network need to be? Uplink or upload speed refers to how fast a network receives data from a device. Downlink or download speed is the reverse—how fast a network can send data to a device. The important thing is to think about whether speed will be a critical performance factor for your smart cities technology. Smart streetlights may not need lightning-fast networks, but your emergency response department's drone fleet might.

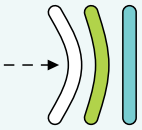
Things to bring up with your smart cities vendor



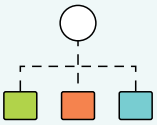
Connectivity



Interoperability

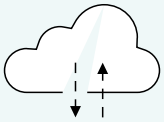


Resiliency



System management

Emergency services



IT considerations

How will you secure your services?

Security, privacy and resiliency are essential to smart cities success.

Security can be impacted by physical factors, like technology placement, or invisible ones, like the security of underlying networks and systems. From inception, your project should be secure by design with privacy built in. Such proactive security measures protect your connected infrastructure and critical information.

Additional security measures, such as certifying the devices powering your IoT ecosystem to meet certain standards, may be a logical next step. The CTIA IoT Cybersecurity Certification Program provides a common baseline of validated cybersecurity functions and compatibility standards that allow certified devices to be securely managed and integrated into community systems.

Develop a cybersecurity plan. This plan should include:

- ☐ A programmatic approach to evaluating cybersecurity control and effectiveness
- ☐ A published cybersecurity roadmap
- ☐ A platform for 24/7 continuous cybersecurity monitoring
- ☐ An operations team to identify risks and test response capabilities
- ☐ Ongoing observations of simulated attacks to discover and mitigate gaps in threat detection

For privacy, understand and create a plan for using and storing sensitive data—on an individual citizen level as well as a macro community level.

To ensure resiliency, plan how you will manage outages, back up systems and mitigate security concerns. Also keep resiliency in mind when you evaluate different technologies, with consideration to prerequisites, maintenance challenges and lifecycle timelines.

Evaluate risks. Perform an initial security risk assessment of systems and services. Are some a higher security concern than others?

CTIA certification levels of security for IoT devices

Level 1 Device Examples

GPS Trackers

GPS Dog Collars

Washing Machines

Level 1

Meets the needs of consumer-grade devices.

Elements include:

- Terms of service and privacy policy
- Password management
- Authentication test
- Access controls
- Patch management

Level 2 Device Examples

Mobile Payment Devices

Security Systems

Connected Streetlights

Level 2

Well suited for business and enterprise-managed devices.

Elements include:

- Level 1 elements
- Audit log
- Encryption of data in transit
- Multi-factor authentication
- Remote deactivation
- Secure boot
- Threat monitoring
- IoT device identity

Level 3 Device Examples

Traffic Controllers

Gas Meters

Industrial Router

Level 3

Offers features designed to protect infrastructure-managed devices.

Elements include:

- Level 2 elements
- Digital signature validation
- Encryption of data at rest
- Tamper resistance
- Design-in features

Establish requirements. Determine the security requirements for each smart municipal service or project, along with privacy principles for how data will be treated.

Secure your environment. Work with service providers and equipment vendors to understand what they're doing to keep networks and devices secure. Create safeguards and protocols for incorporating new IoT devices and networks. You should also make a plan for how you will respond to a breach.

Maintain security posture. Set up regular tests to assess security and resiliency responses. Schedule recurring network risk assessments and penetration tests across the smart cities network ecosystem.

How will you manage assets and data?

One big part of a smart cities project is accurately monitoring and maintaining project assets, from infrastructure to light poles, and the data they produce, like traffic flows.

Here communities can deploy low-cost, low-bandwidth devices that use GPS to precisely determine the locations and condition of city-owned assets. Asset management solutions usually require engagement of city planning, transportation and IT departments and an overarching process for maintaining electronic files, databases and records with the asset description, service year, location to the nearest street address or GPS coordinates and other relevant information.

7 steps for managing assets and data

1. Create an asset management database and plan, complete with timeline and success criteria.
2. Give key departments assignments for asset identification, collection and tagging by criteria such as age, size, location, appearance and last maintenance.
3. Create a standard data curation process to ensure consistency across asset information and classes.
4. Determine a set of common field requirements for populating and building performance reports.
5. Use tools such as secure web portals and mapping (visualization) software to make the process secure, user-friendly and engaging.
6. Keep your city-owned asset database current, and maintain working knowledge with a review process for validating asset information.
7. Assign access, permissions and guidelines, and consult with a cybersecurity firm for other ways to secure this valuable information.