Setting Your Project Up for Success

It's important to narrow your scope, prioritize your projects and line up funding sources. This requires a comprehensive evaluation of the following areas:

Past projects

- ☐ What smart projects have already been executed?
- ☐ What were the results, positive and negative, particularly in the area of data sharing?
- ☐ Have technology platforms been launched that serve more than one department or agency?
- ☐ How successful were they?

Pain points

- ☐ What are your community's main pain points related to public services, transportation and utilities?
- ☐ Does the pain point affect only one part of your community or does it cross municipal boundaries?
- ☐ Which public and private entities does the pain point involve?
- ☐ Do you have a relationship with a public or private entity that can be leveraged again?

Processes

- ☐ Does a common smart cities vision exist in your community?
- ☐ What are your current constraints in procurement—e.g. difficulties collaborating across departments?
- ☐ Do you have open policies for data and processes for governance?
- ☐ Do you have a marketing plan? Think about how you plan to share updates publicly to raise awareness, increase visibility and build momentum.
- ☐ Do you have a modernized infrastructure plan?

People

- ☐ Do you have an assigned smart cities champion?
- ☐ Do you have relationships with local universities or innovation councils?
- ☐ Does your project deliver value across the community or only to a specific segment?

Community Collaboration

Step 1:
Know what you're working with.

- ☐ Does the city have any government-owned utilities that service residents?
- ☐ How much of the city's infrastructure is leased or shared by utilities?
- ☐ What are the modernization/IoT plans for the local utilities?
- ☐ What is the current relationship between the city and local utilities?
- ☐ Are there regular strategic planning meetings?
- ☐ What are the current financial arrangements between the city and utilities?
- ☐ What are the plans for future smart grid, distribution network and renewables projects?

Communities and utilities can leverage existing networks of poles and wires and existing rights-of-way to expedite deployment and reduce costs. For instance, utility poles, including light poles, can be used to mount various devices that enable other "smart" services. Partnerships with the wireless industry can provide the connectivity to power smart utility projects like:

- ☐ Remote-controlled LED street lighting
- ☐ Small cell sites
- ☐ Wireless LAN access points
- ☐ Audio sensors for gunshot detection
- ☐ Cameras for capturing photos of vehicle license plates
- ☐ Traffic enforcement
- ☐ Tracking systems for stolen vehicles/ fugitives/Amber Alerts

Step 2:
Get the technical specifications.

Is end-to-end encryption required?

- ☐ If a device is monitoring or controlling the grid or has access to critical information, enhanced end-to-end security features should be considered.
- ☐ End-to-end encryption can be built into the configuration as routers are deployed.
- ☐ If you are deploying modules/embedded chipsets into equipment like relays, capacitator banks and meter cans, the encryption must be developed and incorporated by the equipment manufacturer.

Are devices protected?

- ☐ Devices should be certified for supply chain protection.
- ☐ Ask who will have access to devices, from manufacturing to delivery.

How will you ensure system reliability?

- ☐ See if you will need a quality-of-service arrangement to ensure prioritization of utility traffic.
- ☐ Pay attention to antenna configuration, which is critical to increasing reliability, throughput, and capacity.
- ☐ Consider MIMO and cross-polarized antennas where applicable.

Step 3:
Prioritize security.

Security is paramount for reliable, resilient smart utility services. Implementing a cybersecurity plan during the design phase of your project can help keep your smart utility assets safe. Specific to wireless connectivity, smart utility devices should be IoT Network Certified for Smart Connected Infrastructure™—which includes a baseline of cybersecurity screening for your IoT devices being deployed on cellular networks.

Consider certifying devices that transmit over a cellular network, including:

- ☐ Gas, electricity, and water meters
- ☐ Industrial gateways
- ☐ Monitoring and control devices