Risks to Connected Communities: ICT Supply Chain and Vendors

Integrating public services into a connected environment can increase the efficiency and resilience of the infrastructure that supports day-to-day life in our communities. However, municipalities considering becoming smart cities/connected communities should thoroughly assess and mitigate the cybersecurity risk that comes with this integration.

For more detailed information on this risk and others, scan the code here to access the Cybersecurity Best Practices for Smart Cities guide.

Communities building smart infrastructure systems often rely on vendors in order to procure and integrate hardware and software linking infrastructure operations. Vulnerabilities in information and communication technology (ICT) supply chains can enable: (1) theft of data and intellectual property, (2) loss of confidence in the integrity of a connected system, or (3) system or network failure through a disruption of availability.

The aggregation of sensitive data needed to support the integration of infrastructure services may be an attractive target for malicious actors to expose vulnerabilities in critical infrastructure and put citizens at risk. A single connected component can introduce risk due to the interdependencies between technologies and basic or vital services. Illicit access gained through a vulnerable ICT supply chain could allow the disruption of infrastructure operations and the compromise of sensitive data.

Mitigate the Risks

Communities deploying smart, emerging, and connected technologies should proactively identify, assess, and manage risks for the components of the ICT supply chain identified below. Organizations should vet vendors carefully to avoid exposing citizens, businesses, and communities to both potentially unreliable hardware and software and deliberate exploitation of supply chain vulnerabilities. The ICT supply chain risk management process should include participation from all levels of the jurisdiction such as mayors, councils, procurement officers, and IT staff. Municipalities should also be transparent with citizens whose data the systems will collect and process.

- Software
- Hardware and IoT Devices
- Managed Service Providers and Cloud Service Providers

The Cybersecurity Best Practices for Smart Cities guide provides recommendations to balance efficiency and innovation with cybersecurity, privacy protections, and national security. Organizations should implement these best practices in alignment with their specific cybersecurity requirements to ensure the safe and secure operation of infrastructure systems, protection of citizens' private data, and security of sensitive government and business data.

Scan to access the CISA ICT Supply Chain Resource Library:

cisa.gov
connected.communities@cisa.dhs.gov
linkedin.com/company/cisagov
@CISAgov
facebook.com/CISA