Risks to Connected Communities: Automation of Operations

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.

Municipalities interested in achieving efficiencies like consistency, reliability, and speed are increasingly procuring smart, emerging, and connected technologies to enable automation of operations and reduce the requirement for direct human control of systems. However, automation can introduce new vulnerabilities because it increases the number of remote entry points into the network. The volume of data and complexity of automated operations can reduce visibility into system operations and potentially hinder real-time incident response.

The integration of artificial intelligence (AI) and complex digital systems could introduce new unmitigated attack vectors and additional vulnerable network components. Reliance on an AI or other complex system may decrease overall transparency into the operations of networked devices as these systems make operational decisions based on algorithms rather than human judgment.

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

Mitigate the Risks

Communities implementing smart, emerging, and connected technologies should develop, assess, and maintain contingencies for manual operations of all critical infrastructure functions and train staff accordingly. Those contingencies should include plans for segmenting infrastructure systems to operate autonomously. In the event of a compromise, organizations should be prepared to isolate affected systems and operate other infrastructure with as little disruption as possible. Jurisdictions should ensure operational resilience through the implementation of the following best practices:

- Backup Systems and Data
- Develop and Exercise Incident Response and Recovery Plans
- Conduct Workforce Training

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 view CISA's schedule for free Industrial Control Systems Trainings:

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