CONNECTED COMMUNITIES PROCUREMENT and IMPLEMENTATION GUIDANCE

QUESTIONS TO ASK VENDORS

SLTT governments are increasingly pursuing cost savings and operational efficiency by adopting Internet connected technology solutions. Integrating these technologies—including Internet of Things, Artificial Intelligence, 5G, and cloud computing—in connected communities offers the potential for enhanced and sustainable services to citizens. However, it also brings about new risks to critical infrastructure and the potential compromise of the security of sensitive government and personal data.

CISA has multiple resources available to support SLTT partners including: (1) ICT Supply Chain Risk Management Task Force Resources, (2) voluntary cross-sector Cybersecurity Performance Goals (CPGs), (3) Risk Considerations For Managed Service Provider Customers, and (4) State And Local Cybersecurity Grant Program (SLCGP).

Below are questions State, Local, Tribal, and Territorial (SLTT) officials can pose to third-party vendors to help ensure alignment with cybersecurity, incident response, data protection and privacy, and supply chain risk management.

CYBERSECURITY RISK MANAGEMENT:

- Q: What is your approach to risk management for your products and services?
    - How do you identify, assess, and mitigate risks?
- Q: What references (e.g., previous customers) can you provide to validate the security of your products and services?
- Q: How do you test and validate the security of your products and services before and after deployment?
- Q: What measures do you have in place to prevent and detect insider threats, including employee and contractor misconduct?
- Q: What access control measures do you have in place to prevent unauthorized access to your products and services?
- Q: How do you manage and secure the communications networks used by smart city devices, such as cellular and wireless networks?
- Q: What cybersecurity and privacy features were designed into these products?
- Q: Are there any planned upgrades to available cybersecurity and privacy features scheduled?
- Q: What are your patch management standards and processes?
- Q: How often do you push firmware updates and how do you ensure the integrity of software and firmware updates?
    - Do your firmware updates apply to all devices in the architecture?
    - How can I push security updates to all my deployed devices?
    - Are updates manual or automatic?
    - Can updates be made while the system is in use or will the system need to be taken offline to be updated?
- Q: Do your products offer interoperability with products from other vendors?
    - If so, is this interoperability specific to other vendors or customizable for each customer?
    - Are your products built with future interoperability in mind?

INCIDENT RESPONSE:

- Q: Do you provide 24/7 real-time support for your product?
- Q: What is your plan to detect and respond to security incidents involving data breaches?
    - How do you train your staff on incident response and preparedness?
- Q: What is your experience managing incident response? How effective has your incident response planning been in previous incidents?
- Q: How will you communicate with the customer in the event of such an incident?
- Q: How do you ensure the resilience and continuity of smart city systems and services in the event of a cybersecurity incident or disaster?
- Q: What cybersecurity mitigation and recovery features do you offer? Do you maintain off-site backups of all system data?

DATA PROTECTION AND PRIVACY:

- Q: What measures do you have in place to ensure the confidentiality, integrity, and availability of the data generated by the smart city technologies?
- Q: Is your product compliant with relevant data protection regulations and standards, such as the NIST Cybersecurity Framework or ISO 27001 standard for information security management?
- Q: What data is collected by this product and supporting systems?
- Q: In what ways does your company use or sell the data generated from these systems?
    - Does your company sell the collected data to any foreign companies or governments?
    - Does the sale of data expose members of the community to safety or security risks?
- Q: Who owns and manages the data and where is it stored?
- Q: How is data encrypted in transit?
- Q: Is all customer data stored in a single repository or is data storage segmented?
- Q: How long is the data stored?
- Q: How is the data backed up?
- Q: Will you provide training to customer staff on how to manage and secure the data generated by the smart city technologies?

SUPPLY CHAIN RISK MANAGEMENT:

- Q: How do you ensure the security of third-party vendors supporting your product or services?
- Q: Does your due diligence for vendors include assessments of percentage of ownership by a foreign corporate group, makeup of their board, where their workforce is based, where your data is housed and routed, and where the products used by your supplier are produced?
- Q: How far down the hardware and software supply chain do you check for known vulnerabilities?
    - Do your hardware and software products come with a component or software bill of materials?
    - Does your product use open-source libraries or packages?
    - Have there been known vulnerabilities reported with any product line?

cisa.gov | connected.communities@cisa.dhs.gov | @cisa.gov | @CISACyber | @cisa.gov