Cybersecurity Best Practices for Smart Cities

Publication: April 19, 2023

United States Cybersecurity and Infrastructure Security Agency
United States National Security Agency
United States Federal Bureau of Investigation
United Kingdom National Cyber Security Centre
Australian Cyber Security Centre
Canadian Centre for Cyber Security
New Zealand National Cyber Security Centre

Summary

This guidance is the result of a collaborative effort from the United States Cybersecurity and Infrastructure Security Agency (CISA), the United States National Security Agency (NSA), the United States Federal Bureau of Investigation (FBI), the United Kingdom National Cyber Security Centre (NCSC-UK), the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), and the New Zealand National Cyber Security Centre (NCSC-NZ). These cybersecurity authorities—herein referred to as "authoring organizations"—are aware that communities may seek cost-savings and quality-of-life improvements through the digital transformation of infrastructure to create "smart cities." In this context, the term "smart cities" refers to communities that:

- Integrate information and communications technologies (ICT), community-wide data, and intelligent solutions to digitally transform infrastructure and optimize governance in response to citizens' needs.
- Connect the operational technology (OT) managing physical infrastructure with networks and applications that collect and analyze data using ICT components—such as internet of things (IoT) devices, cloud computing, artificial intelligence (AI), and 5G.

Note: Terms that also refer to communities with this type of integration include "connected places," "connected communities," and "smart places." The communities adopting smart city technologies in their infrastructure vary in size and include university campuses, military installations, towns, and cities.

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, communities considering becoming smart cities should thoroughly assess and mitigate the cybersecurity risk that comes with this integration. Smart cities are attractive targets for malicious cyber actors because of:

- The data being collected, transmitted, stored, and processed, which can include significant amounts of sensitive information from governments, businesses, and private citizens.
- The complex artificial intelligence-powered software systems, which may have vulnerabilities, that smart cities sometimes use to integrate this data.

The intrinsic value of the large data sets and potential vulnerabilities in digital systems means there is a risk of exploitation for espionage and for financial or political gain by malicious threat actors, including nation-states, cybercriminals, hacktivists, insider threats, and terrorists.

No technology solution is completely secure. As communities implement smart city technologies, this guidance 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.

The authoring organizations recommend reviewing this guidance in conjunction with NCSC-UK's Connected Places Cyber Security Principles, ACSC's An Introduction to Securing Smart Places, CCCS's Security Considerations for Critical Infrastructure, CISA's Cross-Sector Cybersecurity Performance Goals, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default, and Protecting Against Cyber Threats to Managed Service Providers and their Customers.

Risk to Smart Cities

Smart cities may create safer, more efficient, more resilient communities through technological innovation and data-driven decision-making; however, this opportunity also introduces potential vulnerabilities that, if exploited, could impact national security, economic security, public health and safety, and critical infrastructure operations. Cyber threat activity against OT systems is increasing globally, and the interconnection between OT systems and smart city infrastructure increases the attack surface and heightens the potential consequences of compromise.

Smart cities are an attractive target for criminals and cyber threat actors to exploit vulnerable systems to steal critical infrastructure data and proprietary information, conduct ransomware operations, or launch destructive cyberattacks. Successful cyberattacks against smart cities could lead to disruption of infrastructure services, significant financial losses, exposure of citizens' private data, erosion of citizens' trust in the smart systems themselves, and physical impacts to infrastructure that could cause physical harm or loss of life. Communities implementing smart city technologies should account for these associated risks as part of their overall risk management approach. The authoring organizations recommend the following resources for guidance on cyber risk management:

- An introduction to the cyber threat environment (CCCS)
- Control System Defense: Know the Opponent (CISA, NSA)
- Cyber threat bulletin: Cyber threat to operational technology (CCCS)
- Cyber Assessment Framework (NCSC-UK)

Expanded and Interconnected Attack Surface

Integrating a greater number of previously separate infrastructure systems into a single network environment expands the digital attack surface for each interconnected organization. This expanded attack surface increases the opportunity for threat actors to exploit a vulnerability for initial access, move laterally across networks, and cause cascading, cross-sector disruptions of infrastructure operations, or otherwise threaten confidentiality, integrity, and availability of organizational data, systems, and networks. For example, malicious actors accessing a local government IoT sensor network might be able to obtain lateral access into emergency alert systems if the systems are interconnected.

Additionally, as a result of smart cities integrating more systems and increasing connectivity between subnetworks, network administrators and security personnel may lose visibility into collective system risks. This potential loss of visibility includes components owned and operated by vendors providing their infrastructure as a service to support integration. It is critical that system owners maintain awareness and control of the evolving network topology as well as the individuals/vendors responsible for the overall system and each segment. Ambiguity regarding roles and responsibilities could degrade the system's cybersecurity posture and incident response capabilities. Communities implementing smart city technology

should assess and manage these risks associated with complex interconnected systems.

Risks From the ICT Supply Chain and Vendors

Communities building smart infrastructure systems often rely on vendors to procure and integrate hardware and software that link infrastructure operations via data connections. Vulnerabilities in ICT supply chains—either intentionally developed by cyber threat actors for malicious purposes or unintentionally created via poor security practices—can enable:

- Theft of data and intellectual property,
- Loss of confidence in the integrity of a smart city system, or
- A system or network failure through a disruption of availability in operational technology.

ICT vendors providing smart city technology should take a holistic approach to security by adhering to secure-by-design and secure-by-default development practices. Software products developed in accordance with these practices decrease the burden on resource-constrained local jurisdictions and increase the cybersecurity baseline across smart city networks. See the following resource for guidance on secure-by-design and secure-by-default development practices:

- Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default (CISA, NSA, FBI, ACSC, NCSC-UK, CCCS, BSI, NCSC-NL, CERT NZ, NCSC-NZ)

The risk from a single smart city vendor could be much higher than in other ICT supply chains or infrastructure operations, given the increased interdependencies between technologies and basic or vital services. Organizations should consider risks from each vendor carefully to avoid exposing citizens, businesses, and communities to both potentially unreliable hardware and software and deliberate exploitation of supply chain vulnerabilities as an attack vector. This includes scrutinizing vendors from nation-states associated with cyberattacks, or those subject to national legislation requiring them to hand over data to foreign intelligence services.

Illicit access gained through a vulnerable ICT supply chain could allow the degradation or disruption of infrastructure operations and the compromise or theft of sensitive data from utility operations, emergency service communications, or visual surveillance technologies. Smart city IT vendors may also have access to vast amounts of sensitive data from multiple communities to support the integration of infrastructure services—including sensitive government information and personally identifiable information (PII)—which would be an attractive target for malicious actors. The aggregation of sensitive data may provide malicious actors with information that could expose vulnerabilities in critical infrastructure and put citizens at risk. See the following resources for guidance on mitigating supply chain risks:

- Information and Communications Technology Supply Chain Risk Management (CISA)
- Supply chain security guidance (NCSC-UK)

- Identifying Cyber Supply Chain Risks (ACSC)
- Cyber supply chain: An approach to assessing risk (CCCS)

Automation of Infrastructure Operations

Smart cities can achieve efficiencies by automating operations, such as wastewater treatment or traffic management. Automation reduces the requirement for direct human control of those systems. Automation can also allow for better consistency, reliability, and speed for standardized operations. However, automation can also introduce new vulnerabilities because it increases the number of remote entry points into the network (e.g., IoT sensors and remote access points). The volume of data and complexity of automated operations—including reliance on third-party vendors to monitor and manage operations—can reduce visibility into system operations and potentially hinder real-time incident response.

Automation for infrastructure operations in smart city environments may require the use of sensors and actuators that increase the number of endpoints and network connections that are vulnerable to compromise. The integration of AI and complex digital systems could introduce new unmitigated attack vectors and additional vulnerable network components. Reliance on an AI system or other complex systems may decrease overall transparency into the operations of networked devices as these systems make and execute operational decisions based on algorithms instead of human judgment.

Recommendations

Secure Planning and Design

The authoring organizations strongly recommend communities include strategic foresight and proactive cybersecurity risk management processes in their plans and designs for integrating smart city technologies into their infrastructure systems. New technology should be deliberately and carefully integrated into legacy infrastructure designs. Communities should ensure any "smart" or connected features they are planning to include in new infrastructure are secure by design and incorporate secure connectivity with any remaining legacy systems. Additionally, communities should be aware that legacy infrastructure may require a redesign to securely deploy smart city systems. Security planning should focus on creating resilience through defense in depth and account for both physical and cyber risk as well as the converged cyber-physical environment that IoT and industrial IoT (IIoT) systems introduce. See the following consolidated, baseline practices that organizations of all sizes can implement to reduce the likelihood and impact of known IT and OT risks.

- Cross-Sector Cybersecurity Performance Goals (CISA)

See the following additional resources for guidance on accounting for risks in the cyber, physical, and converged environments:

- Improving ICS Cybersecurity with Defense-in-Depth Strategies (CISA)

- Cybersecurity and Physical Security Convergence (CISA)
- Consequence-Driven Cyber-Informed Engineering (INL)

Apply the principle of least privilege.

The organizations responsible for implementing smart city technology should apply the principle of least privilege throughout their network environments. As defined by the U.S. National Institute of Standards and Technology (NIST), the principle of least privilege is, "The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function." Administrators should review default and existing configurations along with hardening guidance from vendors to ensure that hardware and software is only permissioned to access other systems and data that it needs to perform its functions. Administrators should also immediately update privileges upon changes in administrative roles or the addition of new users or administrators from newly integrated systems. They should use a tiered model with different levels of administrative access based on job requirements. Administrators should limit access to accounts with full privileges across an enterprise to dedicated, hardened privileged access workstations (PAWs). Administrators should also use time-based or just-in-time privileges and identify high-risk devices, services, and users to minimize their access. For detailed guidance, see:

- Defend Privileges and Accounts (NSA)
- Restricting Administrative Privileges (ACSC)
- Managing and controlling administrative privileges (CCCS)

Enforce multifactor authentication.

The organizations responsible for implementing smart city technology should secure remote access applications and enforce multifactor authentication (MFA) on local and remote accounts and devices where possible to harden the infrastructure that enables access to networks and systems. Organizations should explicitly require MFA where users perform privileged actions or access important (sensitive or high-availability) data repositories. Russian state-sponsored APT actors have recently demonstrated the ability to exploit default MFA protocols. Organizations responsible for implementing smart cities should review configuration policies to protect against "fail open" and re-enrollment scenarios. See the following resource for guidance on implementing MFA:

- #More Than a Password (CISA)
- Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability (FBI, CISA)
- Transition to Multi-Factor Authentication (NSA)
- MFA for online services (NCSC-UK)
- Implementing MFA (ACSC)

- Zero trust architecture design principles - Authenticate and authorize (NCSC-UK)

Implement zero trust architecture.

Implementing zero trust network design principles will create a more secure network environment that requires authentication and authorization for each new connection with a layered, defense-in-depth approach to security. Zero trust also allows for greater visibility into network activity, trend identification through analytics, issue resolution through automation and orchestration, and more efficient network security governance. See the following resources for guidance on implementing zero trust:

- Zero trust architecture design principles (NCSC-UK)
- Zero Trust Maturity Model (CISA)
- Embracing a Zero Trust Security Model (NSA)
- A zero trust approach to security architecture (CCCS)
- Zero Trust security model (CCCS)

Note: Both zero trust architecture and MFA should be applied wherever operationally feasible in balance with requirements for endpoint trust relationships. Some OT networks may require trust-by-default architectures, but organizations should isolate such networks and ensure all interconnections with that network are secured using zero trust and related principles.

Manage changes to internal architecture risks.

The organizations responsible for implementing smart city technology should understand their environment and carefully manage communications between subnetworks, including newly interconnected subnetworks linking infrastructure systems. Network administrators should maintain awareness of their evolving network architecture and the personnel accountable for the security of the integrated whole and each individual segment. Administrators should identify, group, and isolate critical business systems and apply the appropriate network security controls and monitoring systems to reduce the impact of a compromise across the community. See the following resources for detailed guidance:

- CISA Vulnerability Scanning (CISA)
- Vulnerability Scanning Tools and Services (NCSC-UK)
- Security architecture anti-patterns (NCSC-UK)
- Preventing Lateral Movement (NCSC-UK)
- Segment Networks and Deploy Application-aware Defenses (NSA)

Securely manage smart city assets.

Secure smart city assets against theft and unauthorized physical changes. Consider implementing physical and logical security controls to protect sensors and monitors against manipulation, theft, vandalism, and environmental threats.

Improve security of vulnerable devices.

See the following resources for guidance on protecting devices by securing remote access:

- Selecting and Hardening Remote Access VPN Solutions (CISA, NSA)
- Using Virtual Private Networks (ACSC)
- Virtual private networks (CCCS)

Protect internet-facing services.

See the following resources for guidance on protecting internet-facing services:

- Protecting internet-facing services on public service CNI (NCSC-UK)
- Strategies for protecting web application systems against credential stuffing attacks (CCCS)
- Isolate web-facing applications (CCCS)

Patch systems and applications in a timely manner.

Where possible, enable automatic patching processes for all software and hardware devices that include authenticity and integrity validation. Leverage threat intelligence to identify active threats and ensure exposed systems and infrastructure are protected. Secure software assets through an asset management program that includes a product lifecycle process. This process should include planning replacements for components and software nearing or past end-of-life, as patches may cease to be developed by manufacturers or developers. See the following resources for guidance on protecting systems and networks via asset management:

- Known Exploited Vulnerabilities Catalog (CISA)
- Asset management for cyber security (NCSC-UK)

Review the legal, security, and privacy risks associated with deployments.

Implement processes that continuously evaluate and manage the legal and privacy risks associated with deployed solutions.

Proactive Supply Chain Risk Management

All organizations responsible for implementing smart city technology should proactively manage ICT supply chain risk for any new technology, including hardware or software that supports the implementation of smart city systems or service providers supporting implementation and operations. Organizations should use only trusted ICT vendors and components. The ICT supply chain risk management process should include participation from all levels of the organization and have full support from program leaders implementing smart city systems. Procurement officials from communities implementing smart city systems should also communicate minimum security requirements to vendors and articulate actions they will take in response to breaches of those requirements. Smart city technology supply chains should be transparent to the citizens whose data the systems will collect and process.

For detailed supply chain security guidance, see:

- Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (CISA, ACSC, NCSC-NZ, NCSC-UK, CCCS)
- Supply chain security guidance (NCSC-UK)
- ICT Supply Chain Library (CISA)
- Cyber-Physical Security Considerations for the Electricity Sub-Sector (CISA)
- Cyber Supply Chain Risk Management (ACSC)

Software Supply Chain

The organizations responsible for implementing smart city technology should set security requirements or controls for software suppliers and ensure that potential vendors use a software development lifecycle that incorporates secure development practices, maintains an active vulnerability identification and disclosure process, and enables patch management.

Product vendors should also assume some of the risk associated with their products and develop smart city technology in adherence to secure-by-design and secure-by-default principles and active maintenance for the products they provide. Vendors adhering to these principles give the organizations responsible for procuring and implementing smart city technology more confidence in the products they introduce into their networks.

For detailed guidance, see:

- Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default (CISA, NSA, FBI, ACSC, NCSC-UK, CCCS, BSI, NCSC-NL, CERT NZ, NCSC-NZ)
- Software Bill of Materials (CISA)
- Supply Chain Cyber Security: In Safe Hands (NCSC-NZ)
- Securing the Software Supply Chain: Recommended Practices Guide for Customers (ODNI, NSA, CISA, CSCC, DIBSCC, ITSCC)
- Coordinated Vulnerability Disclosure Process (CISA)
- Protecting your organization from software supply chain threats (CCCS)

Hardware and IoT Device Supply Chain

Organizations responsible for implementing smart city technology should determine whether the IoT devices and hardware that will enable “smart” functionality will require support from third-party or external services. These organizations should perform due-diligence research on how parts are sourced and assembled to create products. They should also determine how the devices store and share data and how the devices secure data at rest, in transit, and in use. Organizations should maintain a risk register that identifies both their own and their vendors’ reliance on cloud computing support, externally sourced components, and similar dependencies. For detailed guidance, see:

- Cyber supply chain: An approach to assessing risk (CCCS)
- Cybersecurity for IOT Program (NIST)
- Defending Against Software Supply Chain Attacks (CISA, NIST)

Managed Service Providers and Cloud Service Providers

Organizations should set clear security requirements for managed service providers and other vendors supporting smart city technology implementation and operations. Organizations should account for the risks of contracting with third-party vendors in their overall risk management planning and ensure organizational security standards are included in contractual agreements with external parties. Similarly, organizations should carefully review cloud service agreements, including data security provisions and responsibility sharing models. For detailed guidance, see:

- Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default (CISA, NSA, FBI, ACSC, NCSC-UK, CCCS, BSI, NCSC-NL, CERT NZ, NCSC-NZ)
- Protecting Against Cyber Threats to Managed Service Providers and their Customers (NCSC-UK, CCCS, NCSC-NZ, CISA, NSA, FBI)
- Six steps toward more secure cloud computing (FTC)
- Choosing the best cyber security solution for your organization (CCCS)

Operational Resilience

The organizations responsible for implementing smart city technology should develop, assess, and maintain contingencies for manual operations of all critical infrastructure functions and train staff accordingly. Those contingencies should include plans for disconnecting infrastructure systems from one another or from the public internet 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.

Backup systems and data.

The organizations responsible for implementing smart city technology should create, maintain, and test backups, both for IT system records and for manual operational capabilities for the physical systems integrated in a smart city network. These organizations should identify how and where data will be collected, processed, stored, and transmitted and ensure each node in that data lifecycle is protected. System administrators should store IT backups separately and isolate them to inhibit the spread of ransomware—many ransomware variants attempt to find and encrypt/delete accessible backups. Isolating backups enables restoration of systems/data to their previous state in the case of a ransomware attack.

The organizations responsible for implementing smart city technology should have plans in place and training for staff so operations managers can disconnect normally connected infrastructure systems and operate manually in an "offline" mode to maintain basic service levels. For detailed guidance, see:

- Offline backups in an online world (NCSC-UK)

Conduct workforce training.

Though implementation of smart city technology may include extensive automation, employees responsible for managing infrastructure operations should be prepared to isolate compromised IT systems from OT and manually operate core functions if necessary. Organizations should train new and existing employees on integrated, automated operations as well as isolated, manual backup procedures, including processes for restoring service after a restart. Organizations should update training regularly to account for new technologies and components. For detailed guidance, see:

- ICS Training Available Through CISA (CISA)

Develop and exercise incident response and recovery plans.

Incident response and recovery plans should include roles and responsibilities for all stakeholders including executive leaders, technical leads, and procurement officers from inside and outside the smart city implementation team. The organizations responsible for implementing smart city technology should maintain up-to-date and accessible hard copies of these plans for responders should the network be inaccessible (e.g., due to a ransomware attack). Organizations should exercise their plans annually and coordinate with continuity managers to ensure continuity of operations. For detailed guidance see:

- Incident Response Plan Basics (CISA)
- Effective steps to cyber exercise creation (NCSC-UK)
- Incident Management: Be Resilient, Be Prepared (NCSC-NZ)
- Preparing for and Responding to Cyber Security Incidents (ACSC)
- Developing your incident response plan (CCCS)
- Developing your IT recovery plan (CCCS)

Purpose

This guidance was developed by U.S., U.K., Australian, Canadian, and New Zealand cybersecurity authorities to further their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations.

Acknowledgements

Microsoft, IBM, and Nozomi Networks contributed to this guidance.

Disclaimer

The information in this report is provided "as is" for informational purposes only. CISA, NSA, FBI, NCSC-UK, ACSC, CCCS, and NCSC-NZ do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise does not constitute or imply endorsement, recommendation, or favoring.

Contact Information

U.S. organizations: report incidents and anomalous activity to CISA 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office, the FBI's 24/7 CyWatch at (855) 292-3937, or CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. **United Kingdom organizations:** report a significant cyber security incident at ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973. **Australian organizations:** visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and to access alerts and advisories. **Canadian organizations:** report incidents by emailing CCCS at contact@cyber.gc.ca. **New Zealand organizations:** report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.