The Infrastructure Investment and Jobs Act (IIJA) is a once-in-a-generation federal funding opportunity for modernizing America's physical and digital infrastructure. With a focus on enhancing transportation, natural resources, and energy systems, the IIJA includes provisions aimed at improving cybersecurity, workforce development, and equity.

Cybersecurity
Increased attention to digital security and cybersecurity awareness is critical for the public sector. It is intended to help improve nationwide cybersecurity and address vulnerabilities in critical infrastructure sectors. State and local government CIOs are focused on building strong cyber defenses through increased spending on risk management, endpoint detection, and regular updates among other dynamic systems of technology.

State and local government CIO priorities
According to surveys of state and local government CIOs, they remain focused on supporting digital transformation, compared to 62% in the private sector. 85% of state government IT decision-makers have made, or are planning to make, organization-wide changes to IT investments to support digital transformation. This transformation is expected to result in cost savings and increased efficiency.


How can state and local governments securely make better use of the rising availability of data?

State and local governments face unique challenges in securely making the most of their data. The public sector's data is critical to improving services and decision-making, but it also needs to be protected. Cybersecurity awareness remains a priority, with increased spending on risk management, endpoint detection, and regular updates among other dynamic systems of technology.

The changing nature of state government cybersecurity programs reflects these challenges: Increased priority and adoption/expansion of cybersecurity awareness programs, increased modernization (up from 66% in 2020 to 80% in 2023), and increased use of analytical tools, AI, and machine learning (up from 41% in 2020 to 51% in 2023). Use of advanced technology for monitoring threats and vulnerabilities is also increasing (up from 41% in 2020 to 51% in 2023). The use of chatbots is becoming more common, with 69% of state government chatbots being utilized for cybersecurity.

According to Statista, the global smart city market is expected to grow 13.13% annually to be worth $165.80 billion by 2028; with the most revenue projected to be generated in the United States. There is a significant increase in government spending on smart city initiatives, with the number of smart city programs increasing from 23% in 2020 to 51% in 2023. 16% of Public Administration breaches are cyberattacks, highlighting the importance of cybersecurity in the public sector.

To learn more about how Verizon can help transform your organization to better serve your communities and constituencies, visit the Verizon website.