Whole-of-state cybersecurity:
Three procurement considerations for the public sector

The National Association of State Chief Information Officers' (NASCIO) report on state CIOs' top 10 policy and technology priorities for 2023 showed that cybersecurity and risk management remain a top priority. As these officials plan and prioritize their spending for the remainder of the current fiscal year (FY) and plan for FY 2024, they have important procurement decisions to make to maximize governance and security, simplify vendor management, and accelerate the overall process within a heavily regulated procurement environment.

Below are three important considerations for public sector procurement of cybersecurity solutions.

1. Rethink the traditional cybersecurity approach

Traditionally, states use a federated model for cybersecurity, meaning that each public sector organization is responsible for the security of its own critical applications. This model doesn't allow for a holistic statewide approach to visibility, observability or risk management. Additionally, it doesn't provide government leaders with insights or the ability to identify, prioritize and fund efforts to reduce risks at scale.

Cyber events continue to heavily impact public sector organizations, compromising data and critical services. According to the Federal Bureau of Investigation (FBI)'s 2022 Internet Crime Report, the FBI's Internet Crime Complaint Center (IC3) received 870 complaints of ransomware attacks from organizations belonging to a critical infrastructure sector. States now are moving toward a whole-of-state model that provides visibility, risk reduction and shared support capabilities. The approach supports broad access to certain security controls and capabilities across the state's infrastructure to reduce cybersecurity gaps and to gain better visibility into threats at scale across the state.

2. Drive toward optimized cybersecurity programs

A more holistic security strategy can protect critical services within state borders. State and local governments are shifting to collective defenses, where public and private sector organizations work together to augment and train their security resources, acknowledge common risks and share information. One of these programs, the State and Local Cybersecurity Grant Program, allocated $1 billion to be distributed over four years to support state, local and tribal agencies implementing cybersecurity best practices. Similarly, in September 2022, the State of Arizona Department of Homeland Security launched the Arizona Statewide Cyber Readiness Grant Program, providing technical assistance and security software licenses through AWS Marketplace to help Arizona's most vulnerable cities, counties and K12 school districts reduce infrastructure risks.

3. Support agile responses to innovation and security

The most common challenge facing government technology procurement is following outdated regulations and policies that don't support agility. Speedy procurement enables government innovation; waiting for software can stall protective resources for implementation and can reduce experimentation opportunities.

State chief information security officers (CISOs) and Department of Homeland Security (DHS) leads rely on fast procurement to utilize grants and other types of use-it-or-lose-it funding associated with these programs that have short expiration and spending windows. Plus, delays in cybersecurity solution procurement can mean at-risk systems go longer without the appropriate security solutions.

According to the 2022 Total Economic Impact™ of AWS Marketplace study, AWS Marketplace provides 66 percent time savings due to procurement efficiencies. That's 66 percent time saved in gaining the resources organizations need to boost their defenses against cyber incidents. Reducing procurement time in a whole-of-state cybersecurity initiative can enable faster time to defense and cybersecurity solutions.

Conclusion

Whole-of-state cybersecurity models can help state and local governments optimize their cyber resilience efforts and support compliance standards across all agencies to make sure critical state infrastructure is protected. The AWS Marketplace can help support procurement efforts for this cybersecurity model by accelerating procurement timelines and more to help agencies get the technology they need.