Harmonize Disparate Federal Cybersecurity Regulations

Issue and Background

- As the primary agent of the federal government, states administer dozens of crucial federal programs and deliver vital services to citizens. As a result, state governments must store data and exchange data with federal programmatic agencies and thus become subject to federal security regulations that govern the use and protection of shared data.
- Federal cybersecurity regulations largely address the same controls and outcomes but differ in their specific requirements. Compliance with disparate regulations is an obstacle for state CIOs who are actively seeking savings for taxpayers through IT initiatives like consolidation/optimization.Further, when state data centers are audited for compliance, states receive inconsistent findings from federal auditors despite reviewing the same IT environment.
- As state IT agencies have become increasingly centralized across the country – whereby the state CIO has greater purview over the IT operations of each state agency – compliance with duplicative requirements of federal cybersecurity regulations has grown significantly in cost, both financial and in personnel time.
- In 2018, Congress tasked the Government Accountability Office (GAO) to study the various federal cybersecurity regulations and to issue corresponding recommendations.
- In May 2020, GAO issued their report, Selected Federal Agencies Need to Coordinate on Requirements and Assessments of States, which found that between 49 and 79 percent of federal agency cybersecurity requirements had conflicting parameters and urged the federal agencies to collaborate on cybersecurity requirements.
- At this time, only four of the twelve recommendations for strengthening cybersecurity have been addressed, and much additional work remains.
- During a June 2021 hearing before the U.S. House Oversight Subcommittee on Government Operations, Chairman Connolly and Ranking Member Hice, as well as numerous other members of the Subcommittee, expressed frustration with the burdensome and duplicative regulations.

Recommendation

- **Congress and the federal agencies should continue to implement the recommendations of the GAO report** and urge the Office of Management and Budget (OMB) to coordinate collaboration among federal agencies on the development and implementation of cybersecurity regulations.
- **Congress should empower OMB with requisite authorities** to ensure OMB can mandate consultation by federal agencies before updating their cybersecurity regulations.
- Federal agencies should work with State CIOs and CISOs to streamline cybersecurity regulations. Addressing duplicative regulations and inconsistent audit practices will not only save taxpayer funds but will also improve our nation's cybersecurity posture. State CIOs and CISOs remain committed to working with federal agencies and auditors to harmonize disparate interpretations of security regulations and to normalize the audit process.