Harmonize Disparate Federal Cybersecurity Regulations and Normalize the Audit Process

- ***One state reports receiving five different outcomes from federal auditors who reviewed the same IT environment***
- ***Another state reported spending 11,600 hours on responses to comply with regulations from six federal agencies***
- ***GAO currently reviewing federal cybersecurity regulations impacting state CIOs***

State governments partner with the federal government to administer federal programs and deliver services to citizens. Due to this partnership, 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 security regulations include: Internal Revenue Service (IRS) *Publication 1075*, Social Security Administration's (SSA) *Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the SSA*, Centers for Medicare and Medicaid Services (CMS) *Minimum Acceptable Risk Standards for Exchanges* (CMS MARS-E), FBI *Criminal Justice Information Services Security Policy* (FBI-CJIS), *Health Insurance Portability and Accountability Act* (HIPAA) and more. Federal security 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. This then requires that state CIOs dedicate precious security personnel time on redundant compliance activity rather than activities which would proactively enhance the cybersecurity posture of the state.

For the past few years, NASCIO has been working on this issue with our strategic partners and Congress to highlight these redundancies. In 2018, the U.S. Senate Homeland Security and Governmental Affairs Committee along with the U.S. House of Representatives Committee on Oversight Intergovernmental Affairs Subcommittee tasked the Government Accountability Office (GAO) to study the various federal cybersecurity regulations and issue corresponding findings.

State CIOs appreciate the serious responsibility of securing citizen information. State CIOs are committed to working with federal regulating agencies and auditors to harmonize disparate interpretations of security regulations where possible and normalizing the audit process to make efficient use of state cybersecurity personnel. Cybersecurity is a shared responsibility and NASCIO looks forward to collaborating with our federal government counterparts to further enhance the cybersecurity posture for states and the nation.