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 4,000 hours responding to one federal audit***

State governments partner with the federal government to administer federal programs and deliver services to citizens. Due to this partnership, state governments must 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 topics, e.g. access control, but differ in their specific requirements. For example, consider the following:

Federal Regulation:	IRS Publication 1075	FBI-Criminal Justice Information Services	SSA Electronic Information Exchange Security Requirements and Procedures
Unsuccessful logins	Information system must enforce a limit of 3 consecutive invalid login attempts by a user during a 120 min period, and automatically lock account for at least 15 mins.	Where technically feasible, system shall enforce limit of no more than 5 consecutive invalid attempts, otherwise locking system for 10 mins.	SSA requires that state agencies have a logical control feature that designates a maximum number of unsuccessful login attempts for agency workstations and devices that store or process SSA-provided information…SSA recommends no fewer than three (3) and no greater than five (5).

Compliance with disparate regulations are an obstacle for state CIOs who are actively seeking savings for taxpayers through IT initiatives like consolidation/optimization (See, NASCIO testimony before Senate Homeland Security and Governmental Affairs Committee, June 2017). 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 compliance activity rather than activity which would proactively enhance the cybersecurity posture of the state.

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.

444 North Capitol Street, Suite 642 Washington, D.C. 20001 202.624.8477 YCooke@NASCIO.org