NASCIO
Representing Chief Information Officers of the states

Government Affairs & Advocacy Overview

As a strategic goal of the association, NASCIO strives to be an effective advocate for information technology polices at all levels of government. NASCIO's primary advocacy efforts focus on building awareness and understanding of state IT policy issues, advancing the role of the state CIO, and expanding the association's visibility on Capitol Hill and with federal agencies. Advocacy and public policy actions are guided by NASCIO's public policy principles. To advance its mission, NASCIO interacts with many interested stakeholder organizations and strategic partner associations.

NASCIO develops calls to action to highlight federal government affairs, policy briefs and legislative alerts for members on key issues of importance to the association and its membership.

NASCIO 2018 Federal Advocacy Priorities

- Harmonize disparate federal cybersecurity regulations and normalize the audit process
- Recognize state authority and ongoing innovation with emerging technology
- Information sharing and safeguards: meeting citizen expectations

Links

- Recent Advocacy Actions
- Cybersecurity Awareness
- Cross-Jurisdictional Collaboration
- NASCIO D.C. Fly-In

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.

Recognize State Authority and Ongoing Innovation with Emerging Technology

- ***Within state government, there is a growing recognition of the need for state CIOs to address emerging technologies by design rather than default***
- ***Emerging networked devices are increasingly reflected in state IT strategic plans, up from nine percent in 2016 to 21 percent in 2017***
- ***In 2017, 67 percent of state CIOs stated that their role regarding emerging technology was to collaborate with agencies in decision-making***
- ***State CIOs predict that the Internet of Things (43 percent), artificial intelligence/machine learning (29 percent), digital assistants (10 percent), and blockchain (9 percent) technologies will be the most impactful in the next three to five years***

The business application of artificial intelligence, blockchain, the Internet of Things (IoT), unmanned aerial systems (UAS), autonomous/connected vehicles, and other networked devices continue to appear on the state CIO policy agenda. Specifically, state CIOs reported that IoT (43 percent), artificial intelligence/machine learning (29 percent), digital assistants (10 percent), and blockchain (9 percent) would be the most impactful in the next three to five years. As the top IT official for state government, state CIOs are engaged in advising (14 percent) and collaborating with state agencies (67 percent) on the business application of emerging technologies and their role in leading these decision is expected to increase (See, 2017 State CIO Survey).

The application of emerging technology within state government is one example of how states serve as laboratories of democracy. State CIOs regularly contemplate issues related to data standardization, privacy, security, communications infrastructure, and IT asset management. By embracing technological advances, state CIOs seek to enhance the effectiveness of state government in delivering services to citizens. It would be premature to regulate emerging technology when applications for it are still being contemplated and/or in development. A premature regulatory framework could stifle innovation and introduce unintended consequences. As such, **NASCIO supports the ability and authority of state governments to continue to serve as laboratories of democracy as it applies to emerging technology**.

Information Sharing and Safeguards: Meeting Citizen Expectations

Data management and analytics appears in NASCIO's Top Ten as a priority

States need an effective, efficient, and established method for sharing data especially as resource constraints demand increased cross-jurisdictional collaboration

The federal government should continue to support the National Information Exchange Model (NIEM), build new communities within NIEM to ensure it remains the standard of choice for state governments and our partners, and issue clear and consistent guidance on how to utilize and adopt NIEM

State governments must be able to respond efficiently and effectively when delivering services to citizens. In a digital age, citizens and government employees expect to receive services and information through multiple portals and integrate these elements, as necessary. This often requires multi-agency sharing of information in order to provide government services with ease to the citizen. Cross-enterprise collaboration and communication will continue to be routine and necessary in serving the citizen, as well as designing and deploying integrated government processes that require information from multiple agencies.

Common standards can maximize access to shared information among federal, state, local, and tribal governments—as well as among our partners in the private sector. Use of national standards will avoid redundant investment and unnecessary variation. What is needed is a common discipline for information sharing that is employed by all government lines of business, like the National Information Exchange Model (NIEM).

NIEM should be integrated into state government enterprise architecture and data management strategy specifically for planning and implementing intergovernmental information exchanges. NIEM provides a broad range of products and capabilities for planning and implementing enterprise-wide information exchanges. In addition, there is an impressive user-community surrounding NIEM that provides training and technical assistance to those looking to utilize it. Perhaps as important, it is an open-source solution. This allows the diverse actors at the federal, state, local, and tribal level to utilize diverse products while maintaining the same framework thus ensuring consistency.

NASCIO has long supported NIEM and recommends that states adopt NIEM to enable collaborative information exchange across the state government enterprise and with federal and local government partners. The federal government should continue to build and deploy new communities within NIEM to ensure NIEM remains the standard of choice for state governments and our partners and continue to issue guidance on how to adopt and deploy NIEM for those seeking an information sharing methodology.