2024 State Legislative Agenda

The Alliance for Digital Innovation (ADI) believes that governments must prioritize innovation to provide efficient and secure digital services to their citizens. ADI works to bring state-of-the-art information technology (IT) to help build a modern, 21st century digital government. We believe that a strong, collaborative partnership between state governments and private sector technology firms is essential to the effective delivery of critical government services.

Our key legislative priorities for 2024 include:

- Empowering state governments to invest in modern, cloud-based commercial technology that underpins critical public sector missions and creates an effective digital government
- Building smart cybersecurity policies, practices, and programs that encompass all of a state's public entities and critical infrastructure
- Promoting the adoption of a risk-based, technical approach to the use of artificial intelligence by state governments
- Ensuring that public sector acquisition practices encourage investments in emerging technology.
- Helping government agencies attract and grow a state's technology talent to maximize the efficiencies and opportunities created by modern, cloud-based technology

Investments in Modern Commercial Technology

As government services evolve to meet the demands of our digital lives, public sector agencies must be equipped with the best technology and cybersecurity tools available to deliver effective services to the people they serve. The unfortunate reality is that there are many outdated, legacy IT systems with weak security still in use across government. Through the implementation of cloud-based, commercial technology solutions that enhance cybersecurity, increase reliability of services, provide improved cost efficiency, and scale quickly to meet the ever-changing needs of citizens, government agencies better position themselves to serve their communities.

True digital transformation and the adoption of modern, agile development and procurement processes, coupled with the decommissioning of current legacy systems, is a time-consuming endeavor that typically crosses multiple budget cycles. Even when planned judiciously, worthwhile efforts to provide better, more secure citizen services through commercial capabilities are often hampered by inflexibilities in the appropriations process.

ADI urges state leaders to adopt policies that will promote long-overdue investments in government IT systems and networks by:

- Establishing funding models for technology modernization projects to transform legacy IT systems and improve the state's cybersecurity posture
- Requiring that any new IT system is interoperable within multi-vendor ecosystems to ensure the ability to appropriately share information and provide effective digital services
- Creating a single sign-on citizen portal with robust digital identity practices for individuals to access all state digital government services safely and securely

Advancing a "Whole of State" Approach to Cybersecurity

State and local government networks and systems face increasingly sophisticated cybersecurity threats every day. In recent years, we have seen cyberattacks that have imperiled election systems, shut down entire school districts, and crippled law enforcement networks. Ransomware attacks have increased greatly in recent years, especially against local governments, school districts, and critical infrastructure. State governments must have sufficient resources and adopt best practices that will protect against malicious activity and prepare for recovery from a cyberattack. In the cybersecurity realm, states are only as secure as their weakest link, and it's vital that leaders develop strong cyber policies that include not just state and local government, but also higher education, K-12 schools, and public utilities such as water and energy.

ADI urges state leaders to adopt policies that will promote partnerships between state and local governments and better protect public systems and citizen data by:

- Ensuring the universal adoption of trusted cybersecurity frameworks and "zero trust" cyber solutions across state governments, local governments, K-12 and higher education, and critical infrastructure
- Creating a reporting requirement for cybersecurity incidents at all public bodies and critical infrastructure across the state to promote information sharing about cyber vulnerabilities and reduce the risk of repeat attacks
- Providing funding for training and upskilling opportunities to address critical gaps in cybersecurity through the adoption of best practices such as multi-factor authentication, phishing prevention, and software vulnerability mitigation
- Requiring the use of the ".gov" domain for all government websites to bolster public trust in state government services

Responsible Use of Artificial Intelligence

ADI member companies have developed and used artificial intelligence (AI) and machine learning (ML) for years. These technologies have tremendous potential, and advances in research and development, coupled with security best practices, can solidify the United States' leading role in the evolution of AI. It is important to recognize the beneficial use cases of AI, particularly in products that leverage large amounts of data and focus on answering questions, improving user experiences, protecting sensitive data, and hardening networks against increasingly sophisticated cybersecurity attacks.

Unfortunately, recent technological advances have greatly impacted the current dialogue around AI, which is now filled with hyperbole and sensationalism that obscures the positive impact of AI on government services. We believe that AI can – and should – be socially beneficial, accountable to its users, and have security and privacy incorporated into its design principles. ADI supports the adoption of a risk-based, technical approach to the use of AI by state governments.

ADI urges state leaders to adopt policies that embrace a technically driven approach to the responsible development and use of AI by:

- Embracing the voluntary use of the AI framework published by the National Institute for Standards and Technology (NIST) when considering and managing risks related to AI products and systems
- Working with experts from the private sector to develop informed guidance and governance frameworks that will encourage and empower the responsible and transparent use of AI by state governments

More Efficient and Effective Acquisition Policies

With the rapid move into digital environments, state and local governments must be able to quickly access commercial innovation to provide critical services and protect American citizens and interests. We must be able to acquire and deploy technology in a way that keeps pace with that innovation. Unfortunately, the government is often stymied in its efforts to quickly onboard and use modern commercial solutions by a legacy approach to purchasing and acquisition. The characteristics of technology, such as the rapid, modular, and iterative nature of modern IT design and deployment, are ill suited for traditional acquisition techniques. Acquiring digital services requires a much different approach than acquiring physical goods.

ADI urges state leaders to adopt policies that will modernize outdated IT systems, accelerate the digital transformation of state government services, and strengthen states' cybersecurity defenses by:

- Enabling agile and innovative approaches to the procurement of technology solutions that will promote the adoption of modern commercial technology
- Avoiding the "legacy tech" problem in the future by reinforcing a preference for commercial cloud technologies by leveraging market research and requiring justification for the use of non-commercial solutions
- Promoting the use of cooperative procurements and standardized cybersecurity compliance regimes to shorten the length of acquisition cycles, eliminate redundancies, and enable smaller government organizations to acquire services they otherwise cannot afford
- Preventing anti-competitive behavior by requiring fair, open, and non-discriminatory procurement frameworks to ensure agencies acquire best-of-breed solutions rather than favoring a preferred vendor
- Allowing for flexibility to select from the widest array of solutions and consider all relevant factors in addition to cost, such as short-term and long-term environmental impact and sustainability, the quality and security of goods and services purchased, performance history, and total cost of ownership solutions

Expanding the Public Sector Technology Workforce

While addressing these technological challenges of delivering modern digital services while protecting citizen data, state governments also face an unprecedented workforce shortage. By one estimate, at least 500,000 additional cybersecurity workers are needed in the U.S. to close current workforce gaps. As the demand for cyber workers increases yearly, this number is expected to grow ever larger. In fact, the federal government projects that demand for cybersecurity professionals will grow over 30% by the end of the decade, meaning that we'll need roughly a million additional cybersecurity workers by 2030.

This is a daunting task, and state workforce policies must deliver both short-term and long-term solutions. State leaders must develop and retain existing cybersecurity and IT talent while expanding today's talent pool and growing the next generation of cyber and IT workers.

ADI urges state leaders to adopt legislation and policies that will develop and retain cybersecurity and IT talent within their state in the present and future by:

- Expanding workforce opportunities for qualified applicants by eliminating arbitrary barriers to employment such as degree requirements
- Empowering state agencies to share critical expertise in IT and cybersecurity through the creation of rotational tours of duty in the state workforce
- Establishing formal job reskilling and apprenticeship programs to expand the talent pool in critical areas such as application development, cloud operations, and cybersecurity
- Planning for the future by creating cybersecurity centers of excellence at institutions of higher education to provide education, awareness, and training in cybersecurity for the public, private, and nonprofit sectors

About the Alliance for Digital Innovation

The Alliance for Digital Innovation (ADI) is a nonprofit alliance of technology companies focused on accelerating change in the public sector through the adoption of innovative commercial technology. We engage with government thought leaders to advocate for the removal of institutional and bureaucratic barriers to the operation of a modern digital government. We are currently the largest advocacy coalition in the country for providers of cloud-based services.

Contact:
Dan Wolf
Director of State Programs
Alliance for Digital Innovation
dwolf@alliance4digitalinnovation.org
