

NASCIO 2012 Advocacy Priorities

Information, technology and telecommunications issues will play a major part in the public policy landscape in 2012. Policymakers at all levels of government are seeking solutions and ideas to cut costs, reduce deficits, save taxpayer dollars and continue to provide services with limited resources and budget constraints. They are looking at technology for ideas on transforming service delivery, bolstering program results and delivering cost savings during these tough economic times. They are also looking for better ways to share and protect citizen data. IT allows all levels of government to support programs, enables effective and efficient services, creates transparency for citizens and supports the U.S. economy.

States are leading innovators in the execution of government services and play a critical role in administering federal programs that citizens depend on every day. The federal government will deliver over \$550 billion to the states to administer diverse programs ranging from Medicaid, homeland security, broadband expansion, unemployment to education. Part of this funding is used to fund IT solutions that the states have to purchase, develop, implement, maintain and make secure to carry out the federal programs. With limited resources in federal and state government to carry out critical and non-critical services, we must work together in a partnership with all levels of government and the private sector to find solutions and tools to get the maximum return on investment from information technology to deliver the type of government services that the American public expects.

The National Association of State Chief Information Officers (NASCIO) has been active in promoting a stronger state-federal partnership, especially in the areas of administrative flexibility, critical infrastructure protection, cyber security, information sharing, business process redesign and the advancement of enterprise architecture. With the emergence of new technologies, NASCIO advocacy priorities will help all levels of government collaborate and make certain IT investments will better serve the American people. NASCIO advocates the following policy positions, objectives and recommendations on behalf of the state CIOs:

I. More Administrative Flexibility Needed for States

Over the past several decades, federal program requirements and directives imposed by federal agencies have hindered state, local and tribal government efforts to modernize service channels, integrate program delivery and achieving better outcomes at lower cost. Specifically, the influence of federal directives, inflexible programmatic guidelines and lack of coordination of federal IT directives has had a significant impact on the strategies, operations and services of state CIOs. The foremost barriers to state innovation and implementation of an enterprise approach lies in the inconsistent interpretation and application of federal programmatic rules in [2 CFR Part 225, Cost Principles for State, Local, and Indian Tribal Governments](#) (OMB Circular A-87) for IT investments by the states.

Currently, the general guidelines attached to federal programmatic funding for services administered by the states do not promote enterprise IT consolidation, shared solutions, infrastructure optimization, virtualization or the integrated channels of services sought by

citizens. A top priority initiative of state CIOs today is budget and operational cost control. CIOs are implementing several enterprise strategies such as consolidation, cloud computing, virtualization and shared services environment for delivering and supporting IT services to their state agencies. Consolidation of IT infrastructure and services represents a significant opportunity for cost savings, energy efficiency and improved service levels. While progress is being made, the rules concerning the use of federal IT funds is a continuing challenge to further progress in this area and an impediment to reducing costs and more effective use of federal funds. Because of the siloed funding approach, there is no incentive for states to seek enterprise solutions. State CIOs need flexibility to prevent the creation of new “stove piped” systems, or systems with rigid boundaries that only allow for the transmission of information along strict vertical agency lines rather than a horizontal exchange of information across state organizational lines.

With the federal government overhauling federal information technology processes, procurement, directives and procedures, it is imperative that a process to harmonize federal programmatic rules, directives and mandates for IT investments by the states be undertaken. The federal government has begun to reform their IT programs, which will influence the states. States were early adopters of these reforms and have undertaken many of these efforts.

Although federal guidelines may be used as the rationale, specific technology requirements are interpreted and applied in an inconsistent manner by federal agencies and imposed on the states. This prohibits states from leveraging existing technology investments and implementing cost-saving enterprise services. States end up with costly stovepipe programs and mismatched technology solutions due to the lack of federal coordination. A prime example is the array of programs funded by the U.S. Department of Health and Human Services and administered by the states. Each state uses hundreds of millions in federal and state matching funds to build and support its own complex and expensive eligibility and benefits management system to support Medicaid and other publicly funded financial assistance programs. If coordinated, this could be a standards-based national development effort – delivered at the state level through a “federated” model, saving billions and resulting in more consistent service delivery outcomes.

A second illustration of the lack of coordination relates to information security directives and audits of federal programs administered by the states. State IT environments must comply with multiple sets of information security requirements and compliance audits which are inconsistent and at times conflicting. There exists a failure to apply the FISMA risk management framework in a consistent manner, or to even use it for the protection of agency information. Clearer understanding of information security requirements is needed. States could lower costs by having a better ability to share security controls across multiple environments.

Recommendation: The [February 28, 2011 Presidential Memorandum on Administrative Flexibility](#) instructed agencies to work closely with State, local, and tribal governments to identify administrative, regulatory, and legislative barriers in federally funded programs that currently prevent States, localities, and tribes, from efficiently using tax dollars to achieve the best results for their constituents. NASCIO recommends that the Office of Management and Budget (OMB) and Congress implement the Intergovernmental Working Group on Administrative Flexibility recommendations contained in the September 2011 report titled

Implementing the Presidential Memorandum on Administrative Flexibility for State, Localities, and Tribes.

NASCIO also encourages Congress to continue funding for OMB's Partnership Fund for Program Integrity Innovation. This program fund allows Federal, state, local, and tribal agencies to pilot innovative ideas for reducing improper payments, improving administrative efficiency, improving service delivery and protecting and improving program access for eligible beneficiaries. The pilots can evaluate and test whether state, local and tribal governments need more flexibility and relief from regulatory programmatic rules to improve outcomes with federal state administered programs.

II. Secure and Protect Citizen Data and State Digital Assets

As states slowly recover from the Great Recession, vital services and programs like cyber security have been cut and continue to be under invested based on accepted benchmarks. The protection of government and citizen data, as well as state information technology and communication assets and resources is vital, since they depend on this cyber infrastructure to operate. Protecting this digital infrastructure is an economic imperative. Cyber security is not only essential to preserve the states' ability to effectively serve citizens, but is also necessary to protect federal programs administered by the state, preserve the privacy of personal and sensitive information, and to support mission-critical homeland security activities. As part of the nation's critical infrastructure, the state government IT sector demands attention, prioritization and investments necessary to prevent the disruption of services and continuity of government. Cyber-attacks have disrupted state government networks, systems and operations, and could potentially affect first-responder communications during an attack on our homeland. According to [the 2010 Deloitte-NASCIO Cyber Security survey report](#), the states are not making the appropriate investments in strengthening their cyber security posture and the dynamic nature of the threats continues to make it challenging.

NASCIO firmly believes that all levels of governments and the private sector must partner and collaborate in cyber security protection, recovery and restoration. This is a complex issue and no single program or effort will address the problem. In recent years, the Department of Homeland Security engagement on the cyber security agenda with the states has significantly improved. Opportunities for limited federal funding for cyber threats have been included in the State Homeland Security Grant program. DHS convenes and supports a number of committees and sector specific councils on critical infrastructure protection and state and local government entities are represented. Most recently, NASCIO collaborated with the MS-ISAC to assist DHS in the development and execution of the National Cyber Security Review (NCSR), completed. Nevertheless, based on the daily attacks, known threats and risks, cyber security does not receive adequate attention and prioritization.

Without a specific and dedicated federal homeland security grant program that does not compete for funding with more tangible physical security requirements, cyber security will most likely not receive the resource commitment it desperately requires. Cyber security is not only essential to preserve the states' ability to effectively serve citizens, but is also necessary to protect federal

programs (such as Medicaid, TANF and others) administered by the state, preserve the privacy of personal and sensitive information, and support mission-critical homeland security activities.

NASCIO is concerned about the Administration's cyber proposal containing provisions prohibiting states from requiring that state citizen data be kept within states. Ninety five percent of state CIOs have identified services they have or are considering moving to the cloud. While moving to cloud computing platforms and services, states must have the ability and flexibility to negotiate with providers on how to best secure its own citizens' data. Some states have privacy laws prohibiting its states data from leaving its borders. By preempting states from protecting its own data, the federal government distorts the state CIOs IT business operation model.

Recommendation: Cyber threats facing the federal, state, local and tribal governments represent a national risk with economic consequences. NASCIO urges DHS to continue to work with the states in protecting our nation's digital assets. NASCIO also strongly urges that FEMA and DHS give higher priority to state cyber security grants program to assist state CIOs/CISOs and support enhancement of cyber security preparedness, protection, response and recovery in the states.

NASCIO requests the results of the recently completed [National Cyber Security Review \(NCSR\)](#) be utilized to not only identify gaps in state cyber security protection and recommend improvements, but for rationale to support additional federal SHSG funds directed at advancing cyber security in the states.

NASCIO objects to any provisions prohibiting states from protecting its citizens' data when moving to cloud computing.

III. Reallocation of D-Block Spectrum to Public Safety

NASCIO supports the reallocation of the D-Block to public safety and the establishment of a national interoperable mobile wireless broadband network that will improve our nation's homeland security and provide first responders with new voice, video, and data communications technologies that are urgently and desperately needed. As a strong advocate for enterprise architecture and open standards, NASCIO supports a uniform foundation for public safety communications. Rather than relying on slices of disparate spectrum for public safety, a nationwide architecture is needed to reduce complexity, promote advance services and direct future investments toward true interoperability. We need comprehensive spectrum legislation to build a 21st century digital infrastructure that provides public safety with the D-Block spectrum, adequate funding and a strong governance model that will include the proper structure to insure nationwide build out while allowing for local control of the network.

On a daily basis, State Chief Information Officers support public safety activities through the statewide communications infrastructure. Our country's local, state, tribal, and federal law enforcement, fire, medical, and other emergency professionals must have access to the most modern and reliable wireless broadband technologies to communicate with each other and with federal officials across agencies and geography during emergencies. The ability for public safety to have seamless nationwide roaming capability on a wireless broadband network that is

hardened to public safety requirements is achievable and essential for public safety to meet its ever-increasing responsibilities.

Legislation needs to ensure that states and localities are provided maximum flexibility in developing public and private partnerships that include utilities, critical infrastructure, transportation, public works and other non-public safety users to assure sustainability, efficiency and effectiveness. We are concerned that some legislation has attempted to prohibit states and localities from allowing secondary users on the network and contracting with the widest possible range of qualified providers. States should not be limited as to who uses the network or contract with in implementing and operating the broadband systems. NASCIO's members will vigorously resist such anti-competitive, federal mandates.

NASCIO opposes requiring public safety to giveback the 700 MHz narrowband language. Thousands of licenses have been granted to use the spectrum, and today hundreds of thousands of users rely on the 700 MHz narrowband mobile radios for both day-to-day operations and when responding to acute natural and manmade disasters. State and local governments have invested an average of between \$100 - \$400 million to build out their networks, and many of these 700 MHz narrowband systems have only come online within the last couple of years or will be coming on line within the next year.

NASCIO also opposes the “administrator” governance model language contained in some legislation. We support the bipartisan Rockefeller-Hutchison bill ([S. 911; Public Safety Spectrum and Wireless Innovation Act of 2011](#)), which envisions a public-private non-profit corporation to oversee the construction and operation of the network. Public safety and state and local government would be represented on the board of the proposed corporation, and we strongly believe this system ensures better transparency and accountability, especially to the end-users.

Recommendation: The allocation of the D-Block spectrum and funding to public safety is critical to building a nationwide wireless broadband network that provides the capacity needed to transmit mission critical real-time high-resolution video, voice and data. NASCIO urges Congress to pass - *Public Safety Spectrum and Wireless Innovation Act of 2011 (S. 911)* - the only bipartisan bill that has passed out of committee that has all the proper elements (funding, flexibility and governance) to successfully build and sustain a nationwide network.

IV. Support the Adoption and Expansion of the National Information Exchange Model

Government must be able to respond efficiently and effectively in delivering citizen services. Cross line of business collaboration will continue to become more routine and necessary in serving the citizen as well as designing and deploying integrative government processes that require information from multiple state agencies. The *National Strategy for Information Sharing* calls for “common standards” to maximize access to shared information among federal, state, local, and tribal governments; and the private sector. Government effectiveness and citizen centric government services require effective cross line of business collaboration and communication. 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.

NASCIO recommends the adoption of the [National Information Exchange Model \(NIEM\)](#) for enabling collaborative information exchanges across the state government enterprise and with federal and local government partners. NIEM should be integrated into state government enterprise architecture and data management strategy specifically for planning and implementing inter-governmental information exchanges. NIEM provides a broad range of products and capabilities for planning and implementing enterprise-wide information exchanges. As a community, NIEM provides the training, technical assistance, and the relationships necessary for assisting government in developing the knowledge and skills to effectively employ NIEM.

The [Justice Information Sharing and Technology Program](#) helps state, local, and tribal law enforcement and criminal justice agencies take full advantage of justice information sharing by providing grant funding, training and technical assistance to support the modernization and enhancement of state and local justice information systems. The Justice Information Sharing and Technology Programs have established enterprise-wide information exchanges such as NIEM. The NIEM established standards and processes that enable jurisdictions to effectively share critical information in emergencies, as well as support the day-to-day operations of agencies throughout the nation.

Recommendation: NASCIO strongly urges federal agencies and states to adopt NIEM as an essential component of state and federal government data management strategy to help facilitate inter-governmental data exchanges and collaboration across all levels of government. NASCIO urges Congress to continue funding for the program in the Commerce-Justice-Science Appropriations bill.

V. Support State Role in Identity Management and Verification Solutions

Federal, state, local, and tribal governments currently issue numerous credentials to constituents for access to facilities or services based on a variety of endorsements. Many of the endorsements provide citizens with access to federally funded programs, but the issuance of credentials remains program-specific and has become a redundant process for many agencies and departments. In an effort to reduce risk and achieve compliance of government directives, robust and interoperable trust frameworks for identity and access management are needed. By issuing a virtual or digital identity that has multi-platform credentialing options, it will result in improved efficiency and convenience for both users and issuers. To the extent such credential is honored by commercial entities, it will also improve efficiency and security of commercial transactions, including on-line transactions.

Both the state and federal government have compelling reasons to support a national ecosystem of identity management. These include:

- Identity management is a critical cross boundary activity
- A standards-based architecture to facilitate interoperability

- Need for a uniformly accepted electronic identity approach necessary to support online transactions, licensing, eligibility, benefits enrollment, registration, etc.
- Cost reduction and business efficiency - paper and outmoded processes which waste time, energy and money
- Potential for reducing improper payments, fraud, waste and abuse with an enterprise approach to digital identity
- Citizen inconvenience and frustration with managing multiple credentials

In order for states to improve program integrity, reduce costs, streamline access, prevent fraud and curtail identity theft, effective policies must enable trust across organizational, operational, physical, and network boundaries. The resulting framework will promote data security, privacy, and the high assurance authentication needed to secure information sharing and transparency in government. Guidance on the approach to identity management will encourage a shift away from stove-piped applications to an enterprise view of identity that enables use without creating redundant sources that are difficult to protect and keep current.

With more states moving services online, NASCIO supports the [National Strategy for Trusted Identities in Cyberspace \(NSTIC\)](#) that would create a voluntary identity ecosystem to make online transactions more secure, private, and more convenient. NSTIC would promote privacy-enhancing technologies. NSTIC offers a vision of the future where the private sector, civil societies, and the public sector collaborate to create the standards and policies needed for interoperable trusted credentials that would reduce identity theft and fraud.

Recommendation:

With greater need for cross-boundary collaboration and program integrity, state governments need to leverage the existing federal initiatives on digital identity management and credentialing. Federal agencies need to coordinate with states and work toward an a federated type solution that is standards based and competitively sourced to ensure interoperability across governments. NASCIO supports the vision of NSTIC and requests that states be included in the governance structure and be considered for pilot projects to explore creating interoperable credentials, streamline business process and protect personal information in our when conducting transactions online.

For more information contact:

Pamela Richardson Walker
Director of Government Affairs
NASCIO
Hall of States
444 North Capitol Street NW, Suite 642
Washington, D.C. 20001-1511
P: (202) 624-8477
F: (202) 624-7745
C: (202) 215-2015
E: pwalker@AMRms.com
W: www.nascio.org