

## *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.

**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](mailto:pwalker@AMRms.com)  
W: [www.nascio.org](http://www.nascio.org)