



## ***State Governments at Risk: Secure Citizen Data and State Infrastructure***

As states are experiencing the worst economic crisis since the Great Depression, funding for vital services and programs like cybersecurity are being cut and under invested. 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. Cybersecurity 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 Cybersecurity Study, the states are not making the appropriate investments in strengthening their cyber security posture, while the dynamic nature of the threats and risks to government operations make this an imperative.

NASCIO firmly believes that all levels of governments and the private sector must partner and collaborate in cybersecurity 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. Nevertheless, based on the daily attacks, known threats and risks, cybersecurity 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, cybersecurity will most likely not receive the resource commitment it desperately requires. Cybersecurity 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.

**Recommendation:** Cyber threats facing the federal, state, local and tribal governments represent a national risk with economic consequences. NASCIO strongly urges that FEMA and DHS give higher priority to state cybersecurity grants program to assist state CIOs/CISOs and support enhancement of cyber security preparedness, protection, response and recovery in the states. NASCIO also urges DHS to continue to involve the states in planning the Nationwide Cyber Security Review strategy as required by the Department of Homeland Security FY 2010 Appropriations (P.L. 111-8) in order to learn where states and local government are vulnerable and strong. In addition, NASCIO supports the Administration efforts to educate and brief the new class of Governors about the importance of cybersecurity in protecting all levels of government critical assets.

**For more information, contact Pamela Richardson Walker of the National Association of State Chief Information Officers at (202) 624- 8477 or via email [pwalker@amrms.com](mailto:pwalker@amrms.com).**