NASCIO
Representing Chief Information Officers of the States

Contact
Meghan Penning
NASCIO Membership &
Communications Coordinator
859.514.9217
mpenning@NASCIO.org

FOR IMMEDIATE RELEASE

NASCIO Issues Guidance for States on Cyber Disruption Response Planning

LEXINGTON, Ky., Thursday, April 7 — Recognizing that a major cyber-attack can disrupt the business of state government, the National Association of State Chief Information Officers (NASCIO) today released guidance on state government cyber disruption response planning. Cybersecurity protection, response, resiliency and recovery dominate the agendas of chief information officers, both in the public and private sector. With the reality that a cyber-attack on critical infrastructure is no longer a theory, state governments must be prepared to respond and be resilient.

“This guide is both a practical implementation document and a call to action for states to develop state cyber disruption response plans,” said Darryl Ackley, cabinet secretary for the New Mexico Department of Information Technology and NASCIO president. “We’ve provided guidance on how to get started and who needs to be engaged. Further, we see this first version as one that will be further developed with input from the states and other stakeholders.”

From the perspective of state information technology leaders, cybersecurity has been on the annual *State CIO Top Ten Priorities* published by NASCIO since the inception of the list in 2006. Since then, the frequency, magnitude and sophistication of cyber-attacks has continued to increase at an accelerated pace. States must develop, mature and test capabilities for dealing with the aftermath of such events that could disrupt the continuity of government.

“Michigan was an early proponent of cyber disruption response planning and collaboration with key state leaders outside of information technology,” said David Behen, chief information officer for the state of Michigan and co-chair of NASCIO’s Cybersecurity Committee. “One of the many things we are emphasizing in our NASCIO guidance is collaboration and integration.”

“With support from the U.S. Department of Justice, Bureau of Justice Assistance, NASCIO is focusing on cyber disruption response planning guidance to help states begin to develop an approach that brings together various agencies such as homeland security, law enforcement, emergency management and the National Guard,” said Doug Robinson, NASCIO executive director.” “Cybersecurity is a team sport and these partners bring the necessary capabilities for responding to a major cyber event that could have dire consequences.”

The guidance is made up of a three volume set that includes: a report on cyber disruption response planning, a comprehensive checklist and a cross functional process description. Together these documents provide guidance on governance, communications and operating discipline for cyber disruption response planning.

Read the guidance report at www.nascio.org/cyberdisruption

# # #

About NASCIO
The National Association of State Chief Information Officers is the premier network and resource for state CIOs and a leading advocate for technology policy at all levels of government. NASCIO represents state chief information officers and information technology executives from the states, territories, and the District of Columbia. For more information about NASCIO visit www.nascio.org.

AMR Management Services provides NASCIO’s executive staff. For more information about AMR visit www.AMRms.com.