



Call for Action

July 2006

NASCIO Staff Contact: Doug Robinson; (859) 514-9153; drobinson@AMRms.com

Strengthening National Cybersecurity – The Role of the State CIO

The Issue

NASCIO has long seen the natural linkage between homeland security and the state and local CIOs, who oversee information and communications technologies that support the key public service. Section 7(c) of Homeland Security Presidential Directive (HSPD)-7 declares that “It is the policy of the United States to enhance the protection of our Nation’s critical infrastructure and key resources against terrorist acts that could...undermine State and local government capacities to maintain order and to deliver minimum essential public services.” Section 15 designates “emergency services”—most of which are delivered by state and local authorities—as being among the nation’s “critical infrastructure sectors.” Moreover, recent increases in politically motivated attacks and improvements in cyber-attack technologies mark at least an increased potential for cyber terrorism.¹

The Problem

The U.S. Department of Homeland Security’s (DHS) State Homeland Security Assessment and Strategy process (SHSAS) does not specifically require states to include “cyber” preparedness in their statewide strategies. This has resulted in state cybersecurity-preparedness planning falling far behind planning for other types of attacks and hazards incidents. This weak link in our infrastructure preparedness is putting the first responders who rely on information and communications technology at high risk.

How Congress and the Administration Can Help

NASCIO applauds the inclusion of the following language in the Senate Homeland Security Appropriations Report. As Congress continues to consider legislation relating to the security of our nation’s cyber assets, NASCIO requests that the promotion of enhanced information sharing among Federal, State, and local levels of government be considered a priority.

“The Committee directs the Under Secretary for Preparedness to request the State Homeland Security Directors to jointly develop with the State Chief Information Officers a State cyber security strategy for critical information and communications technology systems and assets needed to support State and local government services as identified in Homeland Security Presidential Directive 7 {HSPD 7}. The Under Secretary should encourage States to consider risk and needs assessments which account for the multitude of threats relevant to cyber systems; and encourage information sharing between State Homeland Security Directors, State Chief Information Officers and the Department to develop and promulgate a consistent methodology for developing such strategies. The Under Secretary should also institutionalize a routine systematic review of such strategies.”

¹ For more information, see John Leyden, “Politically motivated attacks soar in 2005,” *SecurityFocus*, 27 February 2006, <<http://www.securityfocus.com/news/11028>> (17 April 2006) and William Jackson, “Trends in botnets: smaller, smarter,” *GCN*, 5 April 2006, <http://www.gcn.com/online/vol1_no1/40334-1.html> (17 April 2006).