



Call for Action

April 2008

Strengthening Cyber Security in the States: Providing Directive Grants to Address Critical Needs

Issue: The Current State IT Environment Faces Growing Threats

The cyber infrastructure that enables state government to both conduct business and protect federal programs administered by the states is under attack each day by external and internal threats. This cyber infrastructure includes electronic information and communications systems, and the information contained in those systems. These threat vectors continue to grow in numbers, as well as severity. Today's cyber security threats directed at state governments may be characterized as:

- Constantly evolving due to rapidly emerging technologies
- Growing ever more sophisticated, target-specific and virulent
- Disruptive and profitable by organized crime and a preferred method for generating income through cybercrime activities
- Increasing geopolitical and criminal exploit attempts directed against the states'
- Escalating internal threats as data becomes increasingly mobile and employees are unwittingly lured to release sensitive information into the public domain

The protection of state information technology and communication (ITC) assets and resources is particularly important for the government as it depends on this cyber infrastructure to operate. IT 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 to support mission-critical homeland security activities. States' ITC resources must be secure, protected, and continually upgraded to thwart highly sophisticated, unseen enemies.

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. The cyber threat is not always given this priority, however and is a weak link in our critical infrastructure preparedness. The security of state networks has serious implications for homeland security, as network security affects both continuity of government and the operations of critical infrastructure. Cyber attacks have disrupted state government networks, systems and operations, and could potentially impact first-responder communications during an attack on our homeland. In addition, this preparation must include plans for restoring networks and systems in the event of a cyber attack, terrorist event or natural disaster. The states continue to make investments in strengthening their security posture, however the dynamic nature of the threats makes it challenging.

Federal Funding for Cyber Security: A "Crisis of Prioritization"

Despite this situation there has been a lack of federal attention and funding to support state cyber security efforts. The states and federal government must be partners and collaborate in cyber security protection, recovery and restoration. The National Infrastructure Protection Plan (NIPP) and supporting Sector-Specific Plans (SSPs) outline this coordinated approach and protection responsibilities for federal, state, local, tribal, and private sector security partners. While a stated purpose of the State Homeland Security Program (SHSP) is to "help states to develop or enhance cyber security plans, develop or enhance cyber risk mitigation plans,

and conduct cyber risk and vulnerability assessments,” obtaining a portion of this block funding for cyber security has proven difficult for state CIOs. Cyber security protection must compete for funding against more visible and politically appealing homeland security applications. When funding is provided, it is inadequate to support the unmet needs in ITC critical infrastructure protection. The result is uneven investments in state cyber infrastructure protection and gross inconsistencies among the states in their level of cyber preparedness. NASCIO believes that this problem, gone unresolved, will only become larger in scale.

As the only part of our nation’s critical infrastructure that is attacked on a daily basis, it is critically important that we provide states the resources they need to protect our nation’s cyber assets.

How Congress and the Administration Can Help: Provision of a Cyber Grants Program

Making government ITC more secure is a large and complex issue. There is no single program or effort that will resolve the problem. However, NASCIO firmly believes that a critical element in enhancing the protection of this infrastructure is to provide a Cyber Security Grants Program under the State and Local Programs Heading of the FY2009 Homeland Security Appropriations bill to specifically fund state cyber security efforts. Such efforts should be directed by the State Chief Information Officers or their functional equivalent and funding would be used for a variety of purposes, to include but not limited to, supporting the enhancement of cyber security preparedness in the states by assisting the states procure network sensing, intrusion detection and security related operations equipment, expanding security awareness campaigns, assisting in restoration and recovery efforts in the event of a cyber attack, and providing technical training and certification for protecting programs administered by the states. NASCIO further recommends that this program be funded at a level of \$200 million for FY2009.

Requested Statutory Language:

STATE AND LOCAL PROGRAMS

For grants, contracts, cooperative agreements, and other activities, \$XXX million shall be allocated as follows:

“(13) \$200 million shall be made available to the State Cyber Security Grants Program under section 2004 of the Homeland Security Act of 2002 (6 U.S.C. 605) as amended by Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53)”

Suggested Report Language

"The Committee recommends that a State Cyber Security Grants Program be provided to protect national cyber assets, a significant part of our nation's critical infrastructure that is attacked on a daily basis. The Committee notes with concern the increased geopolitical and criminal exploit attempts directed against many state information technology networks and systems. Funding for the State Cyber Security Grants Program shall be made available to the state Chief Information Officers or their functional equivalent and used to support the enhancement of cyber security preparedness in the states by assisting the states procure network sensing, intrusion detection and security related operations equipment, expanding security awareness campaigns, assisting in restoration and recovery efforts in the event of a cyber attack, and providing technical training and certification for protecting programs administered by the states, and for other purposes."

Contact: Doug Robinson, NASCIO Executive Director, (859) 514-9153, drobinson@AMRms.com