NASCIO Representing Chief Information Officers of the States

Call for Action

April 2009

Advancing Cyber Security in the States: Establish Pilot Program to Protect the Digital Infrastructure

Issue: The Current State IT Environment Faces Growing Threats
The digital 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 digital infrastructure includes electronic information and communications systems, and the information contained in those systems. These threats are growing in numbers, as well as severity. As prime targets, cyber 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

As part of the nation's critical infrastructure, state information communication and technology assets must be protected. This protection is not only essential to preserve the states' ability to effectively serve citizens, but is also necessary to secure federal programs (such as Medicaid, TANF, SNAP and others) administered by the state, preserve the privacy of personal and sensitive information, and to support mission-critical homeland security activities. The states' digital infrastructure must be secure, protected, and continually upgraded to thwart highly sophisticated, unseen enemies because this would threaten national security. With billions of dollars flowing from the American Recovery and Reinvestment Act (ARRA) for technology investments, securing these systems must be included in these modernization efforts.

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 extremely difficult for state CIOs. Cyber security protection must compete for funding

Copyright © 2009 NASCIO • All rights reserved
NASCIO • 201 East Main Street, Suite 1405 • Lexington, KY 40507
P :: (859) 514-9153 • F :: (859) 514-9166 • E :: NASCIO@AMRms.com • W :: www.nascio.org

against more visible and politically appealing homeland security applications. When funding is provided, it is inadequate to support the unmet needs in critical digital infrastructure protection. The result is uneven investments in state cyber infrastructure protection and inconsistencies among the states in their level of cyber preparedness. NASCIO believes that this problem, gone unaddressed, 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 Pilot Program
Making government digital infrastructure 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 establish a state cyber security pilot program to share federal and state best practices, innovation and knowledge transfer regarding cyber security within state governments. 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 $50 million for the two-year pilot.

Requested Statutory Language:
Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following:
In General- There is established within the Department a State Cyber Security Pilot Program (in this section referred to as the `Pilot Program') to demonstrate best practices, innovation, and knowledge transfer regarding cyber security within State governments.
(b) Administration - The Secretary, through the Assistant Secretary for Cyber Security and Communications, shall be responsible for administering the Pilot Program.
(c) Diversity in Participation - The Secretary shall ensure the maintenance of geographic and population diversity among selected Pilot Program participants.
(d) Allocation Limitations - Amounts allocated to a State under this section shall not exceed $2,000,000.
(e) Sunset - The authorization for the Pilot Program established under this section shall expire 2 years following the date of enactment of this section.
(f) Authorization of Appropriations- There are authorized to be appropriated up to $25,000,000 in each of fiscal years 2010 and 2011 to carry out the Pilot Program established under this section.

Contact: Pam Walker, NASCIO Director of Government Affairs, (202) 624-8477, pwalker@AMRms.com

Copyright © 2009 NASCIO • All rights reserved