July 13, 2017

Evelyn L. Remaley, Deputy Associate Administrator National Telecommunications and Information Administration U.S. Department of Commerce 1401 Constitution Avenue N.W., Room 4725, Washington, D.C. 20230

Re: Request for Public Comment on Promoting Stakeholder Action Against Botnets and Other Automated Threat

Dear Deputy Associate Administrator Remaley:

NCSL appreciates the opportunity to comment on the National Telecommunications and Information Administration, U.S. Department of Commerce Request for Public Comment on Promoting Stakeholder Action Against Botnets and Other Automated Threats (RIN 0660-XC035). NCSL is specifically responding to the request for comments titled Governance and Collaboration and Policy and the Role of Government. Currently, the federal government is in a unique position to establish a strong communication system that allows for robust state-federal engagement to enhance national resiliency to cyber-attacks. It is important to recognize that cybersecurity encompasses more than just the security of federal systems, but the security of state and local systems as well. State governments are necessary and equal partners in properly securing all government networks and personally identifiable information data. All fifty states have some form of legislation or administrative action in data security, and can provide key insight to the federal government. The federal government should view states as critical stakeholders, partner with states to secure cyber infrastructure, and establish structured communication pipelines with state CIOs and CISOs.

States should be involved in developing and executing policies, standards, practices and technologies, because they are already active in this space. Legislators appropriate funds and hold oversight hearings to understand the threat landscape, and provide the policies to enable the executive to protect state systems. In an area where technology is constantly changing and advancing, states are already responding to threats in dynamic ways. All 50 states have some form of computer crime law, and many have enacted legislation to combat specific cyber issues. A total of 25 states have legislation to address Denial of Service, or D.O.S. attacks. Many states
also address Ransomware specifically, others have criminal statutes combating computer
trespass and malware in general. Where possible, states have acted to address cybercrime.

Many states have existing standards, practices and technologies which the federal
government can draw from to develop national policies that complement and enhance these
state actions. State legislation has addressed issues of identity theft, phishing, and ransomware.
Thirty-one states and Puerto Rico have laws requiring the destruction and disposal of personal
information to ensure the security of personal data. Twenty states, Guam and Puerto Rico have
anti-spyware statutes. Additionally, 23 states and Guam have specific anti-phishing statutes.
Many other computer crime laws can be applied to spyware.

Data security has been an important priority for states and the federal government can
learn from the 19 states that statutorily require government agencies to have specific policies in
place to ensure the security of their data. Similarly, the federal government should draw on
state expertise in the 14 states that require the destruction or disposal of personal information.
Similarly, engaging with the 12 states that have data security laws that apply to private entities
could also assist the federal government in framing national cyber policy.

Cybersecurity is critical to identity theft policy and states are moving forward legislatively
with addressing this issue. Twenty-nine states, Washington, D.C., Guam and Puerto Rico have
specific restitution provisions for identity theft. Five states have forfeiture provisions for
identity theft crimes, and 11 states have identity theft passport provisions, and states continue
to address cybersecurity as a risk management issue requiring continuous thought and
improvement. Over the past two years, states have continued to innovate in cybersecurity
while in 2016, 28 states proposed bills related to cybersecurity; 15 states enacted such
legislation. Additionally, in 2017, 41 states introduced cyber bills while 16 enacted cybersecurity
laws. The federal government can build on the strong foundation for cyber policy, which
currently exists at the state level.

States already implement incentives and other public policies that can drive change and inform
the federal government, and are acting on an administrative level to protect their networks’
infrastructure. Almost every state provides some form of cybersecurity training for their
employees. Best practices for employee network uses reduce risk and limit vulnerability.
Additionally, 13 states are prioritizing cybersecurity through statewide task forces,
commissions, or advisory councils. Georgia and Indiana have created additional legislative study
committees. There is clear investment at the state level in studying best practices. Within state
executive branches, positions have been created to insure the smooth implementation of
cybersecurity policies. Every state has a single statewide Chief Information Officer or equivalent
official. Nine states have additional Chief Information Security Officers. Responsibilities of these
officers include creating statewide security policies and IT standards, requiring information
security plans and periodic security training for employees. States have the infrastructure in
place, further solidifying their role as stakeholders and partners in securing national networks.

As cyber technology has developed, states have addressed developing security needs as
well. Through legislation and administrative action, state governments have taken steps to
modernize information technology. Each state has its own cybersecurity system, its own infrastructure, and is at different stages in cyber development. Combining resources with the federal government would assist states in moving forward with enhanced cybersecurity protocols.

The federal government should be the convener and information hub for cybersecurity, but must assume this role with the recognition and understanding that state governments are ideal partners for innovation in developing cyber policy. They can provide resources, ideas, and insight in the area of cyber security and botnet prevention. As such, the National Conference of State Legislatures encourages the National Telecommunications and Information Administration to work together with us and with individual state governments to build a robust and secure cybersecurity network.

Thank you for your consideration of NCSL’s concerns. For additional information, please contact Susan Parnas Frederick (susan.frederick@ncsl.org) or Danielle Dean (danielle.dean@ncsl.org) in NCSL’s Washington, D.C. office.

Respectfully,

[Signature]

William T. Pound
Executive Director

National Conference of State Legislatures