NATIONAL CONFERENCE *of* STATE LEGISLATURES

The Forum for America's Ideas

December 7, 2015

The Honorable Jeb Hensarling
Chairman
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable Maxine Waters
Ranking Member
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Hensarling and Representative Waters:

On behalf of the National Conference of State Legislatures (NCSL), I write to urge you to recognize states as equal partners and critical stakeholders in cybersecurity regulation and privacy concerns. Additionally I urge you to acknowledge the necessity of sharing the federal government's threat information with states. NCSL recognizes that the security of the nation's information infrastructure is quickly becoming one of the most serious threats our country faces. In order to combat this growing threat, Congress has an obligation to work with states to devise appropriate solutions.

As you review cybersecurity legislation, NCSL wishes to impress upon the members of the Financial Services Committee the importance of considering some key principles and values.

1. State and local governments must be viewed as critical stakeholders in national cybersecurity efforts. States operate and manage critical infrastructure including data centers and networks which are necessary for basic homeland security and emergency management functions. The federal government must work with state and local government to share threat information and to provide technical support to protect computer networks and other related critical infrastructure. H.R. 2205 requires states to report data breach information to the federal government as a superior monitoring body, overlooking the need for the federal government to share similar data breach information with states. This would hinder the states' ability to identify and prosecute violators.

2. The federal government should partner with states to examine ways to avoid unnecessary preemption of state laws. Provisions of H.R. 2205 that expressly preempt state law should be removed. We acknowledge the need for a national standard on data breach notifications, but this standard must be a floor for the states and not a ceiling. The uniform data breach standard in H.R. 2205 as currently drafted would undermine data breach notification laws in 47 States, and in some cases would lower existing standards.

3. The federal government must avoid unfunded mandates on state and local partners. Public budgets are still strained at all levels of government, and while state and local stakeholders wish to contribute to the overall cybersecurity effort, the ability to independently fund initiatives at this time is unlikely. The federal government should not mandate the development, implementation and maintenance of information security programs under H.R. 2205 irrespective of existing state and local governments' statutes.

Denver
7700 East First Place
Denver, Colorado 80230-7143
Phone 303.364.7700 Fax 303.364.7800

Washington
444 North Capitol Street, N.W. Suite 515
Washington, D.C. 20001
Phone 202.624.5400 Fax 202.737.1069

Website www.ncsl.org
Email info@ncsl.org

4. Federal, state and local governments should collaborate to invest in cybersecurity awareness, education and training for public sector employees, contractors and private citizens.

5. The civil liberties and privacy of all citizens must be maintained while also establishing the safety and stability of the internet and electronic communications. This is especially critical as governments continue to expand online and electronic services. Safeguarding public sector data when reporting data breach incidents under H.R. 2205, that includes personal information of citizens, will require cooperation and collaboration on data standards and cybersecurity methodology at all levels of government.

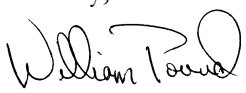
6. Many federal initiatives fund internet and information security programs. However, without cross-cutting communication and coordinated assets, the efforts will not realize maximum efficiency and impact. If there are privacy and security requirements that are preconditions of federal programs and funding they must be uniformly interpreted and implemented across all agencies and levels.

The combined capacity of federal, state, and local governments to adequately safeguard the Nation's critical infrastructure systems remains essential to ensuring effective operations across the full spectrum of the threats we face. Furthermore, in order for communities to effectively manage emergency situations, cybersecurity networks must be resilient to acts of terrorism attacks, and natural disasters.

As you develop the legislative strategy moving forward, we hope you will seriously consider these principles and the impact on states and our mutual citizens.

Should you have any questions or require additional information, please contact Susan Frederick (202-624-3566; susan.frederick@ncsl.org), Jon Adame (202-624-8686; Jon.Adame@ncsl.org), or Danielle Dean (202-624-8698; danielle.dean@ncsl.org).

Sincerely,



William Pound
Executive Director, NCSL