Speaker Paul Ryan
United States House of Representatives
H-232 The Capitol
Washington, DC 20515

December 15, 2015

Dear Speaker Ryan,

We, the undersigned free market organizations, wish to express our deep concern over the extra-procedural revision of three bills related to cybersecurity and information sharing: the Protecting Cyber Networks Act (PCNA), National Cybersecurity Protection Advancement Act of 2015 (NCPAA), and the Cybersecurity Information Sharing Act of 2015 (CISA). The version of these three bills included in the omnibus spending bill, the Cybersecurity Act of 2015, includes a number of provisions that may have troubling implications for the privacy and security of average Americans. Contrary to Republican pledges about restoring normal legislative order, the final revision of these bills was done in a hurried fashion, with little substantive impact from the NCPAA's author, House Homeland Security Committee Chairman Michael McCaul.

As we and others have consistently stated over the past few months, the provisions contained in many of these bills—in particular those in CISA—are unlikely to increase the government's ability to detect, intercept, and thwart cybersecurity attacks, yet *would* decrease accountability and public trust. They are also likely to institute broad, undefined data-collection capabilities even as Congress and the American public have pushed for greater rule of law and accountability at the intersection of national security and privacy.

There is simply no need to rush such controversial provisions into law. These issues deserve full, considered review, which cannot happen when addressed through end-of-year omnibus legislation.

Before sending legislation on these issues to the President, Congress should take the best provisions of all three while disregarding the most contentious elements. Such a bill should include:

1. Clearly establishing DHS as the sole (present and future) portal for information sharing. Under no circumstance should a portal be set up at a law enforcement agency, such as the FBI, or any national security agency, including the NSA, the ODNI, or the CIA. Nor should information be automatically shared with the NSA and DOD;
2. Requiring that companies use due care to remove personally identifiable information that is unrelated to a cyberthreat;
3. Limiting any non-cybersecurity law enforcement use to circumstances of true "imminence" (*i.e.*, death, serious bodily injury, terrorism, and serious economic harm).

Including a requirement for a "specific threat" is not sufficient to address the concern about how the information might be used; and

4. Ensuring that companies sharing information through a designated portal are held liable for any gross negligence pertaining to the handling of personally identifiable information.

Strengthening cybersecurity should not come at the expense of exposing Americans' personal information to malicious agents. Nor should it be necessary to extend law enforcement use authorizations to non-cybersecurity purposes.

We oppose any inclusion of the Cybersecurity Act of 2015 in the omnibus text. The reconciliation process failed to include a key architect of one of the "conferenced" bills and the language included in the omnibus fails to address the most pressing issues related to cybersecurity. As such, we oppose the inclusion of the Cybersecurity Act of 2015 in the omnibus legislation currently being negotiated in Congress and urge you to remove the language from the final omnibus bill.

Sincerely,

FreedomWorks
Niskanen Center
R Street Institute
TechFreedom