Section 407 of CISA Needs to Be *Rejected* by Congress

Backdoor Regulation Harms Security and Is Contrary to Voluntary Information Sharing

The Protecting America's Cyber Networks Coalition (the coalition)—a partnership of roughly 50 leading business associations representing nearly every sector of the U.S. economy—opposes including section 407 of S. 754, the Cybersecurity Information Sharing Act of 2015 (CISA), in the final House-Senate cybersecurity information-sharing legislation, which is nearing completion. This defective provision needs to be rejected by lawmakers for at least three reasons.

- **Security "strategy" masks backdoor regulation.** Section 407 requires the Department of Homeland Security (DHS) and other federal agencies to develop a cybersecurity strategy for each so-called covered critical infrastructure. This apparent regulatory push comes at a time when federal agencies don't seem able to manage their own cybersecurity adequately.

  The list of entities covered by section 407 is not fixed. It is reviewed and updated annually—meaning that it is only a matter of time before DHS and other regulatory bodies expand their reach as part of an effort to dictate the cybersecurity practices of more and more companies. Industry recommended including language in the section saying that the legislation should not be construed to authorize new regulations, but it was rebuffed by supporters of section 407.

  Businesses share the goal of mitigating cybersecurity risks and are committing billions of dollars to the security and resilience of their enterprises. Most observers agree that regulations cannot possibly keep pace with bad actors and would lead to check-the-box security mandates that are costly, time-consuming, and ineffective—thus pulling businesses' limited resources away from cybersecurity and toward compliance. Such an outcome would harm both the nimbleness needed by companies to respond to incidents and public safety—it's the exact opposite effect that Congress is trying to achieve.

- **"Voluntary" information sharing must be voluntary.** A broad consensus has developed around the principle that information sharing between the private sector and the government must be based on a collaborative partnership in order to work. After more than four years of legislative effort, a cybersecurity information-sharing measure is nearing enactment because it is based on this principle. Section 407 is a glaring exception.

  The provision threatens to unravel this fundamental understanding by placing the private sector in an untenably arm's-length, nonvoluntary relationship with DHS and the federal bureaucracy related to incident reporting, rather than encouraging partnerships and collaborative relationships. Industry rejects section 407 because it would lead to incident reporting by private entities that is compelled rather than voluntary in practice—which cuts against the grain of a collaborative threat-sharing program.

- **A lack of transparency and little support mark the provision.** Section 407 was neither approved during a closed committee markup, nor was it included in a list of floor amendments to CISA that could be fairly vetted by stakeholders.

  Hence, it came as a big surprise to many in industry and several lawmakers when section 407 suddenly appeared in the final version of CISA late in the Senate floor process. Good policy can withstand tough scrutiny. But bad policy relies on opaque tactics to advance, which characterizes the path of section 407.

Anticipated conferees to cybersecurity information-sharing legislation have been briefed on the coalition's view that section 407 must be struck from a final House-Senate bill. It is the belief of many industry groups that if this provision remains in the legislation it would represent a major step backward in terms of the public-private collaboration and could threaten passage of the bill.