

U.S. Sens. Johnson, Hassan: Introduce CISA ISP subpoena legislation

Posted on Friday, Dec 13, 2019

>> **WisPolitics is now on the State Affairs network. Get custom keyword notifications, bill tracking and all WisPolitics content. [Get the app or access via desktop.](#)**

WASHINGTON – U.S. Sens. Ron Johnson (R-Wis.), chairman of the Senate Homeland Security and Governmental Affairs Committee, and committee member Maggie Hassan (D-N.H.) introduced legislation Thursday to allow the Cybersecurity and Infrastructure Security Agency (CISA) to issue subpoenas compelling Internet Service Providers (ISPs) to offer information when vulnerabilities are detected on critical infrastructure systems.

The senators had this to say about the bill:

“Every day our adversaries target our critical infrastructure, including our electric grids, dams, and airports. And every day, CISA is made aware of vulnerabilities to these systems - some easily fixable - but is powerless to warn the potential victims. This legislation gives CISA the authority necessary to reach out and warn owners of critical infrastructure that they are open and vulnerable to cyberattacks before they become a victim,” said Sen. Johnson. **“We ask Americans: if you see something, say something. With this legislation we are empowering CISA to do the same.”**

“An attack on critical infrastructure could have devastating consequences, from shutting down heating and cooling systems of hospitals to manipulating industrial controls of water treatment facilities to blacking out an entire city,” said Senator Hassan. **“CISA already has a system to identify cybersecurity vulnerabilities in critical infrastructure, and the**

bipartisan bill we are introducing today helps to ensure that if CISA finds a vulnerability, it has the tools and information it needs to reach out to the entity maintaining the system. Importantly, our bill is narrowly-tailored to protect the privacy rights of all entities, giving CISA only the bare minimum of information necessary.”

Background:

In June 2019, DHS submitted a legislative proposal to Congress that would authorize the Cybersecurity and Infrastructure Security Agency (CISA) to issue administrative subpoenas to telecommunications companies in an effort to identify owners and operators of critical infrastructure systems and devices that were at risk to cyberattacks.

- The legislation gives CISA a limited authority to detect, identify, and receive information only related to critical infrastructure systems for a cybersecurity purpose.
- The purpose of this legislation is to provide CISA the legal means necessary to notify the owner of the critical infrastructure system who was the subject of the subpoena, as a result CISA must notify the vulnerable party within 7 days of receiving their information. Additionally, to ensure the privacy of affected parties or entities CISA must destroy personally identifiable information (PII) after 6 months.
- The legislation includes an annual report to both Congress and the public. It requires reporting on the number of cybersecurity vulnerabilities that have been mitigated and number of entities warned because of this new authority. This allows Congress and the public to better understand whether CISA’s administrative subpoena program has been effective at making U.S. critical infrastructure more secure.
- The bill requires subpoenas to be authenticated by electronic signature, or

similar future technology, so that the internet service provider (ISP) knows it is coming from CISA and has not been fraudulently generated to unlawfully access the PII of ISP subscribers.

###