Sen. Johnson: Legislation that helps CISA warn critical infrastructure owners of cyber threats included in Senate NDAA

Posted on Wednesday, Jul 22, 2020

WASHINGTON — Legislation that would help the Cybersecurity and Infrastructure Security Agency (CISA) warn the owner or operator of critical infrastructure computer systems that it is vulnerable to cyberattacks was included in the Senate's 2021 National Defense Authorization Act (NDAA). This legislation was introduced by 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.). Sens. Angus King (I-Maine) and Ron Wyden (D-Ore) also cosponsored the legislation.

Sens. Johnson and Hassan 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."**

"When CISA identifies a potential cyber vulnerability in an electrical grid or other critical infrastructure, it cannot always identify the owner of the

company in order to alert the company about the vulnerability," said Senator Hassan. **"This common-sense proposal gives CISA the ability to get the information it needs from an Internet Service Provider in order to reach out to critical infrastructure companies to help prevent damaging cyberattacks. I will keep working with Senator Johnson and our colleagues on both sides to get this signed into law as part of the National Defense Authorization Act."**

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.

###