Oct 27 2015

Warner Praises Senate Passage of Cybersecurity Information Sharing Act

Legislation includes key provisions championed by Sen. Warner

WASHINGTON – Today, U.S. Sen. Mark R. Warner (D-VA), a member of the Senate Intelligence Committee, applauded Senate passage of the Cybersecurity Information Sharing Act (CISA), which will strengthen cybersecurity efforts by encouraging private companies to voluntarily share information while ensuring individual privacy and civil liberties. The bipartisan legislation, which now needs to be merged with cybersecurity legislation that passed the House of Representatives before it heads to the President for signature, includes two provisions championed by Sen. Warner to strengthen the Department of Homeland Security's (DHS) authorities to protect federal civilian networks and to conduct threat assessments of critical cyber infrastructure affecting public health or safety, economic, or national security.

"Cyber-attacks present one of the most critical national and economic threats that this nation faces. It's time to get serious about a comprehensive cybersecurity strategy, and this legislation is a step in the right direction," **Sen. Warner said.** "This is a serious problem that isn't limited to government, as we've already seen with recent breaches involving Anthem, CareFirst, Target, Neiman Marcus, Home Depot, and banks like JPMorgan. Both the private and public sector need to be better prepared for an increasing number of these cyberattacks. It is critical we encourage increased coordination and information sharing, between companies and the government, in order to identify and protect against real threats."

Following the recent cyber-attack at the Office of Personnel Management (OPM) that compromised the personal information of at least 22 million individuals, Sen. Warner and Sen. Susan Collins (R-ME) introduced the bipartisan **Federal Information Security Management Reform** (FISMA Reform) Act of 2015 that will bolster the Department of Homeland Security's (DHS) ability to protect federal civilian (.gov) networks.

"The attack on OPM has been a painful example of how behind-the-curve many federal agencies have become when it comes to effective cybersecurity," **said Sen. Warner.** "These breaches allowed cyber attackers to access personal information of more than 22 million federal employees and others. If we want to be better prepared to meet this threat in the future, we have to make sure that the Department of Homeland Security has the tools it needs to adequately secure our federal civilian networks. This bipartisan amendment empowers DHS to deploy effective tools to better ensure that government agencies are properly protected."

While DHS has the responsibility for safeguarding the cyber domain for federal civilian agencies (.gov), DHS has limited authority to actually act. At present, DHS does not have the authority to monitor the networks of government agencies without permission from that agency. DHS also cannot regularly deploy countermeasures to block malware without permission as well. This limited authority hinders the security of .gov information systems which, as evidenced by the recent OPM attack, contain highly sensitive personal data such as finger prints, Social Security numbers, home addresses, dates of birth, and in some cases, extensive background information of federal employees, retirees, and contractors.

The five important steps from the Warner-Collins bill included in the Cybersecurity Information Sharing Act of 2015 include:

1. Legislation that would allow the Secretary of Homeland Security to operate intrusion detection and prevention capabilities on all federal agencies on the .gov domain.

2. Legislation that permits the Secretary of Homeland Security to conduct risk assessments of any network within the government domain.

3. Legislation that allows the Secretary of Homeland Security to operate defensive countermeasures on these networks once a cyber threat has been detected.

4. Legislation to strengthen and streamline the authority Congress gave to DHS last year to issue binding operational directives to federal agencies, especially to respond to substantial cyber security threats in emergency circumstances.

5. Legislation that requires the Office of Management and Budget to report to Congress annually on the extent to which OMB has exercised its existing authority to enforce government wide cyber security standards.

Additionally, CISA includes another provision on critical infrastructure cybersecurity reporting, championed by Sen. Warner, that requires DHS and appropriate regulatory entities to assess whether the government receives adequate information from those critical infrastructure entities whose failure due to cyberattacks would cause “catastrophic” consequences by threatening access to life-sustaining services, causing catastrophic economic damage, or that would severely degrade our national security or national security capabilities – including systems such as airline traffic control, water systems, electrical grids, or significant financial systems.

Permalink: **http://www.warner.senate.gov/public/index.cfm/2015/10/warner-praises-senate-passage-of-cybersecurity-information-sharing-act**