Wrong Approach for Addressing Computer Crime: Whitehouse Amendment No. 2626 Undermines Cybersecurity and Over-Penalizes Vague Legal Violations

CFAA Is Outdated and Undermines Cybersecurity:

The Computer Fraud and Abuse Act (CFAA), the primary federal anti-hacking statute, is in need of reform. Several of its provisions are vague, and it fails to provide clear exceptions for the work of security researchers.

- **Vagueness of "Exceeding Authorized Access":** The CFAA makes "exceeding authorized access" of a computer system a crime. Despite the statute's failure to clearly define what constitutes a violation of this provision, individuals who are being investigated or prosecuted for such a violation could face lengthy terms of imprisonment: up to a decade or longer. There have even been aggressive prosecutions, such as in the case of Aaron Swartz, who committed suicide after being threatened with decades in jail as punishment for a minor violation of a terms of service agreement. The Whitehouse amendment would not address this vagueness.

- **No Exception for Security Research:** Additionally, the CFAA fails to provide adequate exceptions for security researchers whose activities could be read to technically violate its provisions, even though they are not seeking to attack or maliciously hack into other people's computers, but rather are attempting to identify vulnerabilities so that they may be addressed. Thus, the CFAA chills the efforts of security researchers who abstain from penetration testing (a real world test of the effectiveness of cyber defenses) or from notifying companies of newly discovered vulnerabilities out of fear that their work to enhance cybersecurity will result in prosecution and lengthy jail terms under the CFAA.

Whitehouse Amendment Would Exacerbate Rather Than Fix CFAA's Problems:

Senator Whitehouse's Amendment No. 2626 would further undermine cybersecurity rather than enhance it. It would expand the category of CFAA violations in a way that would further chill security research. It could also be read to authorize courts to compel companies to hack at the government's behest. Finally, it would establish a new, overbroad violation concerning critical infrastructure.

- **Expanding Violations Dealing with Access Devices:** The Whitehouse Amendment expands the category of some violations by foreign persons concerning access devices owned or operated by financial institutions or other US companies by removing the requirement that the alleged violator possess or transport either an article used to commit the violation, or the proceeds of the violation. This is concerning because it expands an already problematic category of a CFAA violation without providing for an exception for the legitimate activities of security researchers that support cybersecurity.

  For example, a researcher who seeks to reveal to a credit card company a vulnerability in its system that allowed the researcher to access all of their users' passwords could be subject to prosecution under this amended provision of the CFAA. Because a CFAA violation would no longer require that an individual attempt to transmit or benefit from the passwords that they accessed, the researcher could be prosecuted even if their intentions were purely to strengthen to company's cyber defenses by alerting them to a problem, and their actions were limited to accomplishing this goal.

FOR MORE INFORMATION, CONTACT ROBYN GREENE, POLICY COUNSEL AT
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE: greene@opentechinstitute.org

- **Requirement that Companies Hack for the Government:** The Whitehouse Amendment would undermine cybersecurity by expanding the scope of authorized "computer network exploitations" (also known as hacking). It could be interpreted to grant courts the authority to compel companies to hack its own customers' or users' on the government's behalf. The companies could be compelled to do so in cases involving certain problematic CFAA violations, so long as those violations could affect at least 100 computers. The amendment would not resolve the current ambiguities in the CFAA that lead to over-prosecution and the chilling of security research, as described above. It would, however, ensure that companies are paid for hacking into their customers' or users' accounts services, or devices. The amendment would also protect them from liability should innocent third parties be harmed as a result of the company hacking.

  Thus, this provision of the Whitehouse amendment could serve to expand the scope of government hacking which may result in inadvertent or incidental harm innocent third parties. Additionally, it could further undermine consumer trust, which has been significantly eroded as a result of the NSA revelations of the last two years.

- **New Overbroad CFAA Violation Involving Critical Infrastructure:** The Whitehouse Amendment would create a new category of CFAA violation that is overbroad and carries excessive penalties. The amendment would make it a crime, subject to up to 20 years imprisonment, to damage or attempt to damage any computer connected to critical infrastructure, even if this damage would cause no harm to critical infrastructure itself. The definition of critical infrastructure is broader than necessary, and is interpreted by government agencies to include 16 sectors, which include places of public assembly like stadiums and zoos, movie theaters, shopping malls, and even campgrounds.

  This broad new category means that any person who damages or attempts to damage even one computer connected to any of these entities - such as a ticket dispenser at a movie theater - could be subject to up to 20 years of imprisonment and significant fines, at the discretion of the prosecutor. While the amendment's proponents likely do not intend for this provision to be interpreted so broadly, the amendment has not been drafted in a way that makes clear that such an aggressive application would not be permitted, let alone that it would be inappropriate. As a result, the amendment would severely over-criminalize actions that pose little threat to the broader public.

  It is important to protect our nation's critical critical infrastructure that supports our national security, and our communications, financial, and medical systems from cyber attacks. However, this amendment fails to do so in a manner that is properly tailored to its goals, and as a result, it would create more problems in an already plagued statute.

A chart analyzing all 22 potential CISA amendments is available at http://bit.ly/1Jd1WZ6.

FOR MORE INFORMATION, CONTACT ROBYN GREENE, POLICY COUNSEL AT
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE: greene@opentechinstitute.org