Homeland Security SECURE Technology Act Passes Congress

The bill creates a bug bounty program and establishes vulnerability reporting policy.

Amanda Ziadeh

Thu, 12/20/2018 - 11:52

Photo Credit: Gwengoat/iStock

The Homeland Security Department might soon establish a bug bounty program and security vulnerability reporting process, thanks to the SECURE Technology Act, which cleared both houses of Congress this week.

It's not a law yet, but the bipartisan national security bill introduced by Rep. Will Hurd, R-Texas, who serves on the House Homeland Security and Intelligence Committees, passed both the House of Representatives and Senate Dec. 19 and 20. It has three core parts: improve national security by creating guidelines for addressing security vulnerabilities at DHS, establish a bug bounty program at DHS to incentivize people to find and fix holes in the system, and establish a federal process to address critical supply chain risks.

Those components come from three bipartisan initiatives previously introduced in both the House and Senate: the Public-Private Cybersecurity Cooperation Act, the Hack the Department of Homeland Security of 2018 and the Federal Acquisition Supply Chain Security Act of 2018.

The Public-Private Cybersecurity Cooperation Act directs DHS to establish a policy for reporting security vulnerabilities on DHS public websites, develop a process for mitigation or fixing reported security vulnerabilities, work with other federal departments and non-government security researchers to develop the policy, submit that policy to Congress and make it publicly available.

The Federal Acquisition Supply Chain Security Act looks to establish a Federal Acquisition Security Council and to "provide executive agencies with authorities relating to mitigating supply chain risks in the procurement of information technology."

The Hack the DHS 2018 bill directs DHS' Office of the Chief Information Officer to establish a bug bounty pilot program to find vulnerabilities in the department's internet and public-facing websites and applications. This includes providing compensation for unique vulnerability reports, and awarding a contract to manage the pilot.

And this contract includes executing the remediation of vulnerabilities identified by the program, which is something HackerOne CEO Mårten Mickos advised agencies do when developing policy around bug bounty programs.

"If your company or organization holds customer information in your system, or you're operating things that are for the benefit of consumers, you must have a way of fixing bugs," Mickos said in an August interview with GovernmentCIO Media. "And I think the government should pass such a law — it would be very useful."

The federal government isn't new to bug bounties. In fact, the Defense Department has been issuing bug bounty programs since its first Hack the Pentagon in 2016, which was followed by Hack the Army, Hack the Air Force and Hack the Marine Corps, all led with hacker-powered security platform HackerOne.

In fact, the third Hack the Air Force recently concluded after a month-long hacking period. The Air Force fixed more than 120 security vulnerabilities and awarded hackers more than $130,000 in bounties, according to a press release. And from the three Air Force bug bounty challenges, HackerOne and the Air Force fixed more than 430 security vulnerabilities.

And it’s not just DOD. In September, the General Service Administration’s Technology Transformation Service awarded HackerOne with a multi-year (period of performance for up to five years) contract to run a bug bounty program too. But GSA was the first federal civilian agency to get involved with a bug bounty program after 18F executed a vulnerability disclosure program with HackerOne in 2017.

The SECURE Technology Act still needs presidential approval, but if passed, DHS will follow suit with the various government agencies implementing, mandating or piloting bug bounty programs to improve digital and cybersecurity.

View PDF
DHS
bug bounties
HackerOne
cybersecurity
DOD
hacking
GSA