HR 2774

Hack DHS Act

Congress: 115 (2017–2019, Ended)
Chamber: House
Policy Area: Government Operations and Politics
Introduced: Jun 6, 2017
Current Status: Referred to the Subcommittee on Cybersecurity and Infrastructure Protection.
Latest Action: Referred to the Subcommittee on Cybersecurity and Infrastructure Protection. (Jun 15, 2017)
Official Text: https://www.congress.gov/bill/115th-congress/house-bill/2774

Sponsor

Name: Rep. Lieu, Ted [D-CA-33]
Party: Democratic • **State:** CA • **Chamber:** House

Cosponsors (7 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Taylor, Scott [R-VA-2]	R · VA		Jun 6, 2017
Rep. Khanna, Ro [D-CA-17]	D · CA		Jun 12, 2017
Rep. Meehan, Patrick [R-PA-7]	R · PA		Jun 12, 2017
Rep. Evans, Dwight [D-PA-2]	D · PA		Jul 10, 2017
Rep. Jayapal, Pramila [D-WA-7]	D · WA		Jul 10, 2017
Rep. Kelly, Robin L. [D-IL-2]	D · IL		Jul 10, 2017
Rep. Kilmer, Derek [D-WA-6]	D · WA		Jul 10, 2017

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security Committee	House	Referred to	Jun 15, 2017

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

Bill	Relationship	Last Action
115 S 1281	Related bill	**Sep 25, 2018:** Placed on the Union Calendar, Calendar No. 752.
115 HR 3868	Related bill	**Sep 28, 2017:** Referred to the Committee on Financial Services, and in addition to the Committee on Ways and Means, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.

Summary (as of Jun 6, 2017)

Hack the Department of Homeland Security Act of 2017 or the Hack DHS Act

This bill directs the Department of Homeland Security (DHS) to establish a bug bounty pilot program to minimize vulnerabilities to DHS information systems.

"Bug bounty program" is a program under which an approved computer security specialist or security researcher is temporarily authorized to identify and report vulnerabilities within DHS information systems in exchange for cash payment.

Under such program, DHS shall:

- provide monetary compensation for reports of previously unidentified security vulnerabilities within the websites, applications, and other DHS information systems that are accessible to the public;
- develop an expeditious process by which computer security researchers can register for the program, submit to a background check, and receive a determination as to approval for program participation;
- designate mission-critical operations within DHS that should be excluded;
- consult with the Department of Justice on how to ensure that program participants are protected from prosecution for activities authorized under the program;
- award competitive contracts to manage the program and for executing the remediation of identified vulnerabilities; and
- engage interested persons, including commercial sector representatives, about the structure of the program.

Actions Timeline

- **Jun 15, 2017:** Referred to the Subcommittee on Cybersecurity and Infrastructure Protection.
- **Jun 6, 2017:** Introduced in House
- **Jun 6, 2017:** Referred to the House Committee on Homeland Security.