

Union Calendar No.

116TH CONGRESS
1ST SESSION

H. R. 3710

[Report No. 116-]

To amend the Homeland Security Act of 2002 to provide for the remediation of cybersecurity vulnerabilities, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 11, 2019

Ms. JACKSON LEE (for herself, Mr. PAYNE, and Mr. LANGEVIN) introduced the following bill; which was referred to the Committee on Homeland Security

AUGUST --, 2019

Committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

A BILL

To amend the Homeland Security Act of 2002 to provide for the remediation of cybersecurity vulnerabilities, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Cybersecurity Vulner-

5 ability Remediation Act”.

6 **SEC. 2. CYBERSECURITY VULNERABILITIES.**

7 Section 2209 of the Homeland Security Act of 2002

8 (6 U.S.C. 659) is amended—

9 (1) in subsection (a)—

10 (A) in paragraph (5), by striking “and”

11 after the semicolon at the end;

12 (B) by redesignating paragraph (6) as

13 paragraph (7); and

14 (C) by inserting after paragraph (5) the

15 following new paragraph:

16 “(6) the term ‘cybersecurity vulnerability’ has

17 the meaning given the term ‘security vulnerability’

18 in section 102 of the Cybersecurity Information

19 Sharing Act of 2015 (6 U.S.C. 1501); and”.

20 (2) in subsection (c)—

21 (A) in paragraph (5)—

22 (i) in subparagraph (A), by striking

23 “and” after the semicolon at the end;

24 (ii) by redesignating subparagraph

25 (B) as subparagraph (C);

1 (iii) by inserting after subparagraph

2 (A) the following new subparagraph:

3 “(B) sharing mitigation protocols to counter cy-
4 bersecurity vulnerabilities pursuant to subsection
5 (n); and”; and

6 (iv) in subparagraph (C), as so redes-
7 igned, by inserting “and mitigation pro-
8 tocols to counter cybersecurity
9 vulnerabilities in accordance with subpara-
10 graph (B)” before “with Federal”;

11 (B) in paragraph (7)(C), by striking
12 “sharing” and inserting “share”; and

13 (C) in paragraph (9), by inserting “mitiga-
14 tion protocols to counter cybersecurity
15 vulnerabilities,” after “measures,”;

16 (3) in subsection (e)(1)(G), by striking the
17 semicolon after “and” at the end; and

18 (4) by adding at the end the following new sub-
19 section:

20 “(n) PROTOCOLS TO COUNTER CYBERSECURITY
21 VULNERABILITIES.—The Director may, as appropriate,
22 identify, develop, and disseminate actionable protocols to
23 mitigate cybersecurity vulnerabilities, including in cir-
24 cumstances in which such vulnerabilities exist because

1 software or hardware is no longer supported by a ven-
2 dor.”.

3 **SEC. 3. REPORT ON CYBERSECURITY VULNERABILITIES.**

4 (a) REPORT.—Not later than one year after the date
5 of the enactment of this Act, the Director of the Cyberse-
6 curity and Infrastructure Security Agency of the Depart-
7 ment of Homeland Security shall submit to the Committee
8 on Homeland Security of the House of Representatives
9 and the Committee on Homeland Security and Govern-
10 mental Affairs of the Senate a report on how the Agency
11 carries out subsection (m) of section 2209 of the Home-
12 land Security Act of 2002 to coordinate vulnerability dis-
13 closures, including disclosures of cybersecurity
14 vulnerabilities (as such term is defined in such section),
15 and subsection (n) of such section (as added by section
16 2) to disseminate actionable protocols to mitigate cyberse-
17 curity vulnerabilities, that includes the following:

18 (1) A description of the policies and procedures
19 relating to the coordination of vulnerability dislo-
20 cures.

21 (2) A description of the levels of activity in fur-
22 therance of such subsections (m) and (n) of such
23 section 2209.

24 (3) Any plans to make further improvements to
25 how information provided pursuant to such sub-

1 sections can be shared (as such term is defined in
2 such section 2209) between the Department and in-
3 dustry and other stakeholders.

4 (4) Any available information on the degree to
5 which such information was acted upon by industry
6 and other stakeholders.

7 (5) A description of how privacy and civil lib-
8 erties are preserved in the collection, retention, use,
9 and sharing of vulnerability disclosures.

10 (b) FORM.—The report required under subsection (b)
11 shall be submitted in unclassified form but may contain
12 a classified annex.

13 **SEC. 4. COMPETITION RELATING TO CYBERSECURITY**
14 **VULNERABILITIES.**

15 The Under Secretary for Science and Technology of
16 the Department of Homeland Security, in consultation
17 with the Director of the Cybersecurity and Infrastructure
18 Security Agency of the Department, may establish an in-
19 centive-based program that allows industry, individuals,
20 academia, and others to compete in providing remediation
21 solutions for cybersecurity vulnerabilities (as such term is
22 defined in section 2209 of the Homeland Security Act of
23 2002, as amended by section 2).