Suspend the Rules and Pass the Bill, H.R. 2980, With an Amendment

(The amendment strikes all after the enacting clause and inserts a new text)

117TH CONGRESS
1ST SESSION

H. R. 2980

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

MAY 4, 2021

Ms. JACKSON LEE introduced the following bill; which was referred to the Committee on Homeland Security

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-

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”.

Be it enacted by the Senate and House of Representa-
tives of the United States of America in Congress assembled,
SEC. 2. CYBERSECURITY VULNERABILITIES.


(1) in subsection (a)—

(A) in paragraph (5), by striking “and” after the semicolon at the end;

(B) by redesignating paragraph (6) as paragraph (7); and

(C) by inserting after paragraph (5) the following new paragraph:

“(6) the term ‘cybersecurity vulnerability’ has the meaning given the term ‘security vulnerability’ in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501); and”.

(2) in subsection (c)—

(A) in paragraph (5)—

(i) in subparagraph (A), by striking “and” after the semicolon at the end;

(ii) by redesignating subparagraph (B) as subparagraph (C);

(iii) by inserting after subparagraph (A) the following new subparagraph:

“(B) sharing mitigation protocols to counter cybersecurity vulnerabilities pursuant to subsection (n); and”; and
(iv) in subparagraph (C), as so redesignated, by inserting “and mitigation protocols to counter cybersecurity vulnerabilities in accordance with subparagraph (B)” before “with Federal”;

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

(C) in paragraph (9), by inserting “mitigation protocols to counter cybersecurity vulnerabilities,” after “measures,”;

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

(4) by redesignating subsection (o) as subsection (p); and

(5) by inserting after subsection (n) following new subsection:

“(o) PROTOCOLS TO COUNTER CERTAIN CYBERSECURITY VULNERABILITIES.—The Director may, as appropriate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor.”.
SEC. 3. REPORT ON CYBERSECURITY VULNERABILITIES.

(a) REPORT.—Not later than one year after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on how the Agency carries out subsection (n) of section 2209 of the Homeland Security Act of 2002 to coordinate vulnerability disclosures, including disclosures of cybersecurity vulnerabilities (as such term is defined in such section), and subsection (o) of such section (as added by section 2) to disseminate actionable protocols to mitigate cybersecurity vulnerabilities to information systems and industrial control systems, that includes the following:

(1) A description of the policies and procedures relating to the coordination of vulnerability disclosures.

(2) A description of the levels of activity in furtherance of such subsections (n) and (o) of such section 2209.

(3) Any plans to make further improvements to how information provided pursuant to such subsections can be shared (as such term is defined in
such section 2209) between the Department and indus-
try and other stakeholders.

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

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

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

SEC. 4. COMPETITION RELATING TO CYBERSECURITY
VULNERABILITIES.

The Under Secretary for Science and Technology of
the Department of Homeland Security, in consultation
with the Director of the Cybersecurity and Infrastructure
Security Agency of the Department, may establish an in-
centive-based program that allows industry, individuals,
academia, and others to compete in identifying remedi-
ation solutions for cybersecurity vulnerabilities (as such
term is defined in section 2209 of the Homeland Security
Act of 2002, as amended by section 2) to information sys-
tems (as such term is defined in such section 2209) and
industrial control systems, including supervisory control
and data acquisition systems.
SEC. 5. TITLE XXII TECHNICAL AND CLERICAL AMENDMENTS.

(a) Technical Amendments.—


(A) in the first section 2215 (6 U.S.C. 665; relating to the duties and authorities relating to .gov internet domain), by amending the section enumerator and heading to read as follows:

“SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV INTERNET DOMAIN.”;

(B) in the second section 2215 (6 U.S.C. 665b; relating to the joint cyber planning office), by amending the section enumerator and heading to read as follows:

“SEC. 2216. JOINT CYBER PLANNING OFFICE.”;

(C) in the third section 2215 (6 U.S.C. 665c; relating to the Cybersecurity State Coordinator), by amending the section enumerator and heading to read as follows:

“SEC. 2217. CYBERSECURITY STATE COORDINATOR.”;

(D) in the fourth section 2215 (6 U.S.C. 665d; relating to Sector Risk Management
Agencies), by amending the section enumerator and heading to read as follows:

“SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.”;

(E) in section 2216 (6 U.S.C. 665e; relating to the Cybersecurity Advisory Committee), by amending the section enumerator and heading to read as follows:

“SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE.”; and

(F) in section 2217 (6 U.S.C. 665f; relating to Cybersecurity Education and Training Programs), by amending the section enumerator and heading to read as follows:

“SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING PROGRAMS.”.

(2) Consolidated Appropriations Act, 2021.—Paragraph (1) of section 904(b) of division U of the Consolidated Appropriations Act, 2021 (Public Law 116–260) is amended, in the matter preceding subparagraph (A), by inserting “of 2002” after “Homeland Security Act”.

(b) Clerical Amendment.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the items relating to sections 2214 through 2217 and inserting the following new items:

“Sec. 2214. National Asset Database.
“Sec. 2215. Duties and authorities relating to .gov internet domain.
“Sec. 2216. Joint cyber planning office.
“Sec. 2217. Cybersecurity State Coordinator.
“Sec. 2218. Sector Risk Management Agencies.
“Sec. 2219. Cybersecurity Advisory Committee.
“Sec. 2220. Cybersecurity Education and Training Programs.”