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

To amend the Homeland Security Act of 2002 to provide for the remediation of cybersecurity vulnerabilities, and for other purposes.
Be it enacted by the Senate and House of Representa-
tives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Cybersecurity Vulner-
ability Remediation Act”.

SEC. 2. CYBERSECURITY VULNERABILITIES.

Section 2209 of the Homeland Security Act of 2002
(6 U.S.C. 659) is amended—

(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; and

(4) by adding at the end the following new subsection:

“(n) PROTOCOLS TO COUNTER CYBERSECURITY VULNERABILITIES.—The Director may, as appropriate, identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities, 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 (m) 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 (n) of such section (as added by section 2) to disseminate actionable protocols to mitigate cybersecurity vulnerabilities, 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 (m) and (n) of such section 2209.

(3) Any plans to make further improvements to how information provided pursuant to such sub-
sections can be shared (as such term is defined in such section 2209) between the Department and industry 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 liberties 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 incentive-based program that allows industry, individuals, academia, and others to compete in providing remediation solutions for cybersecurity vulnerabilities (as such term is defined in section 2209 of the Homeland Security Act of 2002, as amended by section 2).