118TH CONGRESS
1ST SESSION

S. 1500

To amend the Help America Vote Act of 2002 to require the Election Assistance Commission to provide for the conduct of penetration testing as part of the testing and certification of voting systems and to provide for the establishment of an Independent Security Testing and Coordinated Vulnerability Disclosure Pilot Program for Election Systems.

IN THE SENATE OF THE UNITED STATES

MAY 9, 2023

Mr. WARNER (for himself and Ms. COLLINS) introduced the following bill; which was read twice and referred to the Committee on Rules and Administration

---

A BILL

To amend the Help America Vote Act of 2002 to require the Election Assistance Commission to provide for the conduct of penetration testing as part of the testing and certification of voting systems and to provide for the establishment of an Independent Security Testing and Coordinated Vulnerability Disclosure Pilot Program for Election Systems.

1   *Be it enacted by the Senate and House of Representa-*

2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the "Strengthening Election

3 Cybersecurity to Uphold Respect for Elections through

4 Independent Testing Act" or the "SECURE IT Act".

5 **SEC. 2. REQUIRING PENETRATION TESTING AS PART OF**

6 **THE TESTING AND CERTIFICATION OF VOT-**

7 **ING SYSTEMS.**

8 Section 231 of the Help America Vote Act of 2002

9 (52 U.S.C. 20971) is amended by adding at the end the

10 following new subsection:

11 "(e) REQUIRED PENETRATION TESTING.—

12 "(1) IN GENERAL.—Not later than 180 days

13 after the date of the enactment of this subsection,

14 the Commission shall provide for the conduct of pen-

15 etration testing as part of the testing, certification,

16 decertification, and recertification of voting system

17 hardware and software by accredited laboratories

18 under this section.

19 "(2) ACCREDITATION.—The Director of the

20 National Institute of Standards and Technology

21 shall recommend to the Commission entities the Di-

22 rector proposes be accredited to carry out penetra-

23 tion testing under this subsection and certify compli-

24 ance with the penetration testing-related guidelines

25 required by this subsection. The Commission shall

26 vote on the accreditation of any entity recommended.

1   The requirements for such accreditation shall be a

2   subset of the requirements for accreditation of lab-

3   oratories under subsection (b) and shall only be

4   based on consideration of an entity's competence to

5   conduct penetration testing under this subsection.''.

6 **SEC. 3. INDEPENDENT SECURITY TESTING AND COORDI-**

7 **NATED CYBERSECURITY VULNERABILITY**

8 **DISCLOSURE PROGRAM FOR ELECTION SYS-**

9 **TEMS.**

10   (a) IN GENERAL.—Subtitle D of title II of the Help

11 America Vote Act of 2002 (42 U.S.C. 15401 et seq.) is

12 amended by adding at the end the following new part:

13 **"PART 7—INDEPENDENT SECURITY TESTING AND**

14 **COORDINATED CYBERSECURITY VULNER-**

15 **ABILITY DISCLOSURE PILOT PROGRAM FOR**

16 **ELECTION SYSTEMS**

17 **"SEC. 297. INDEPENDENT SECURITY TESTING AND COORDI-**

18 **NATED CYBERSECURITY VULNERABILITY**

19 **DISCLOSURE PILOT PROGRAM FOR ELEC-**

20 **TION SYSTEMS.**

21   "(a) IN GENERAL.—

22   "(1) ESTABLISHMENT.—The Commission, in

23   consultation with the Secretary, shall establish an

24   Independent Security Testing and Coordinated Vul-

25   nerability Disclosure Pilot Program for Election Sys-

1 tems (VDP–E) (in this section referred to as the

2 'program') in order to test for and disclose cyberse-

3 curity vulnerabilities in election systems.

4   "(2) DURATION.—The program shall be con-

5 ducted for a period of 5 years.

6   "(3) REQUIREMENTS.—In carrying out the pro-

7 gram, the Commission, in consultation with the Sec-

8 retary, shall—

9   "(A) establish a mechanism by which an

10 election systems vendor may make their election

11 system (including voting machines and source

12 code) available to cybersecurity researchers par-

13 ticipating in the program;

14   "(B) provide for the vetting of cybersecu-

15 rity researchers prior to their participation in

16 the program, including the conduct of back-

17 ground checks;

18   "(C) establish terms of participation

19 that—

20   "(i) describe the scope of testing per-

21 mitted under the program;

22   "(ii) require researchers to—

23   "(I) notify the vendor, the Com-

24 mission, and the Secretary of any cy-

25 bersecurity vulnerability they identify

1 with respect to an election system;

2 and

3 "(II) otherwise keep such vulner-

4 ability confidential for 180 days after

5 such notification;

6 "(iii) require the good faith participa-

7 tion of all participants in the program; and

8 "(iv) require an election system ven-

9 dor, after receiving notification of a critical

10 or high vulnerability (as defined by the

11 National Institute of Standards and Tech-

12 nology) in an election system of the ven-

13 dor, to—

14 "(I) send a patch or propound

15 some other fix or mitigation for such

16 vulnerability to the appropriate State

17 and local election officials, in con-

18 sultation with the researcher who dis-

19 covered it; and

20 "(II) notify the Commission and

21 the Secretary that such patch has

22 been sent to such officials;

23 "(D) in the case where a patch or fix to

24 address a vulnerability disclosed under subpara-

1 graph (C)(ii)(I) is intended to be applied to a

2 system certified by the Commission, provide—

3   "(i) for the expedited review of such

4   patch or fix within 90 days after receipt by

5   the Commission; and

6   "(ii) if such review is not completed

7   by the last day of such 90 day period, that

8   such patch or fix shall be deemed to be

9   certified by the Commission; and

10   "(E) 180 days after the disclosure of a

11 vulnerability under subparagraph (C)(ii)(I), no-

12 tify the Director of the Cybersecurity and In-

13 frastructure Security Agency of the vulner-

14 ability for inclusion in the database of Common

15 Vulnerabilities and Exposures.

16   "(4) VOLUNTARY PARTICIPATION; SAFE HAR-

17 BOR.—

18   "(A) VOLUNTARY PARTICIPATION.—Par-

19   ticipation in the program shall be voluntary for

20   election systems vendors and researchers.

21   "(B) SAFE HARBOR.—When conducting

22   research under this program, such research and

23   subsequent publication shall be considered to

24   be:

1   "(i) Authorized in accordance with
2   section 1030 of title 18, United States
3   Code (commonly known as the 'Computer
4   Fraud and Abuse Act'), (and similar State
5   laws), and the election system vendor will
6   not initiate or support legal action against
7   the researcher for accidental, good faith
8   violations of the program.

9   "(ii) Exempt from the anti-circumven-
10   tion rule of section 1201 of title 17, United
11   States Code (commonly known as the 'Dig-
12   ital Millennium Copyright Act'), and the
13   election system vendor will not bring a
14   claim against a researcher for circumven-
15   tion of technology controls.

16   "(C) RULE OF CONSTRUCTION.—Nothing
17   in this paragraph may be construed to limit or
18   otherwise affect any exception to the general
19   prohibition against the circumvention of techno-
20   logical measures under subparagraph (A) of
21   section 1201(a)(1) of title 17, United States
22   Code, including with respect to any use that is
23   excepted from that general prohibition by the
24   Librarian of Congress under subparagraphs (B)
25   through (D) of such section 1201(a)(1).

1   "(5) EXEMPT FROM DISCLOSURE.—Cybersecu-

2 rity vulnerabilities discovered under the program

3 shall be exempt from section 552 of title 5, United

4 States Code (commonly referred to as the Freedom

5 of Information Act).

6   "(6) DEFINITIONS.—In this subsection:

7   "(A) CYBERSECURITY VULNERABILITY.—

8 The term 'cybersecurity vulnerability' means,

9 with respect to an election system, any security

10 vulnerability that affects the election system.

11   "(B) ELECTION INFRASTRUCTURE.—The

12 term 'election infrastructure' means—

13   "(i) storage facilities, polling places,

14 and centralized vote tabulation locations

15 used to support the administration of elec-

16 tions for public office; and

17   "(ii) related information and commu-

18 nications technology, including—

19   "(I) voter registration databases;

20   "(II) election management sys-

21 tems;

22   "(III) voting machines;

23   "(IV) electronic mail and other

24 communications systems (including

25 electronic mail and other systems of

1 vendors who have entered into con-

2 tracts with election agencies to sup-

3 port the administration of elections,

4 manage the election process, and re-

5 port and display election results); and

6 "(V) other systems used to man-

7 age the election process and to report

8 and display election results on behalf

9 of an election agency.

10 "(C) ELECTION SYSTEM.—The term 'elec-

11 tion system' means any information system that

12 is part of an election infrastructure, including

13 any related information and communications

14 technology described in subparagraph (B)(ii).

15 "(D) ELECTION SYSTEM VENDOR.—The

16 term 'election system vendor' means any person

17 providing, supporting, or maintaining an elec-

18 tion system on behalf of a State or local elec-

19 tion official.

20 "(E) INFORMATION SYSTEM.—The term

21 'information system' has the meaning given the

22 term in section 3502 of title 44, United States

23 Code.

24 "(F) SECRETARY.—The term 'Secretary'

25 means the Secretary of Homeland Security.

1   "(G) SECURITY VULNERABILITY.—The

2   term 'security vulnerability' has the meaning

3   given the term in section 102 of the Cybersecu-

4   rity Information Sharing Act of 2015 (6 U.S.C.

5   1501).".

6   (b) CLERICAL AMENDMENT.—The table of contents

7 of such Act is amended by adding at the end of the items

8 relating to subtitle D of title II the following:

○