

118TH CONGRESS
2D SESSION

H. R. 7447

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 HOUSE OF REPRESENTATIVES

FEBRUARY 23, 2024

Ms. SPANBERGER (for herself and Mr. VALADAO) introduced the following bill; which was referred to the Committee on House Administration, and in addition to the Committee on Science, Space, and Technology, 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

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) ESTABLISHMENT.—The Commission, in con-
22 sultation with the Secretary, shall establish an Inde-
23 pendent Security Testing and Coordinated Vulnerability
24 Disclosure Pilot Program for Election Systems (VDP–E)
25 (in this section referred to as the ‘program’) in order to

1 test for and disclose cybersecurity vulnerabilities in elec-
2 tion systems.

3 “(b) DURATION.—The program shall be conducted
4 for a period of 5 years.

5 “(c) REQUIREMENTS.—In carrying out the program,
6 the Commission, in consultation with the Secretary,
7 shall—

8 “(1) establish a mechanism by which an elec-
9 tion systems vendor may make their election system
10 (including voting machines and source code) avail-
11 able to cybersecurity researchers participating in the
12 program;

13 “(2) provide for the vetting of cybersecurity re-
14 searchers prior to their participation in the program,
15 including the conduct of background checks;

16 “(3) establish terms of participation that—

17 “(A) describe the scope of testing per-
18 mitted under the program;

19 “(B) require researchers to—

20 “(i) notify the vendor, the Commis-
21 sion, and the Secretary of any cybersecu-
22 rity vulnerability they identify with respect
23 to an election system; and

1 “(ii) otherwise keep such vulnerability
2 confidential for 180 days after such notifi-
3 cation;

4 “(C) require the good faith participation of
5 all participants in the program; and

6 “(D) require an election system vendor,
7 after receiving notification of a critical or high
8 vulnerability (as defined by the National Insti-
9 tute of Standards and Technology) in an elec-
10 tion system of the vendor, to—

11 “(i) send a patch or propound some
12 other fix or mitigation for such vulner-
13 ability to the appropriate State and local
14 election officials, in consultation with the
15 researcher who discovered it; and

16 “(ii) notify the Commission and the
17 Secretary that such patch has been sent to
18 such officials;

19 “(4) in the case where a patch or fix to address
20 a vulnerability disclosed under paragraph (3)(B)(i)
21 is intended to be applied to a system certified by the
22 Commission, provide—

23 “(A) for the expedited review of such patch
24 or fix within 90 days after receipt by the Com-
25 mission; and

1 “(B) if such review is not completed by the
2 last day of such 90-day period, that such patch
3 or fix shall be deemed to be certified by the
4 Commission; and

5 “(5) 180 days after the disclosure of a vulner-
6 ability under paragraph (3)(B)(i), notify the Direc-
7 tor of the Cybersecurity and Infrastructure Security
8 Agency of the vulnerability for inclusion in the data-
9 base of Common Vulnerabilities and Exposures.

10 “(d) VOLUNTARY PARTICIPATION; SAFE HARBOR.—

11 “(1) VOLUNTARY PARTICIPATION.—Participa-
12 tion in the program shall be voluntary for election
13 systems vendors and researchers.

14 “(2) SAFE HARBOR.—Research conducted
15 under the program, and any subsequent publication
16 of such research, shall be treated as follows:

17 “(A) The research and publication shall be
18 treated as authorized in accordance with section
19 1030 of title 18, United States Code (commonly
20 known as the ‘Computer Fraud and Abuse
21 Act’), (and similar State laws), and the election
22 system vendor will not initiate or support legal
23 action against the researcher for accidental,
24 good faith violations of the program.

1 “(B) The research and publication shall be
2 exempt from the anti-circumvention rule of sec-
3 tion 1201 of title 17, United States Code (com-
4 monly known as the ‘Digital Millennium Copy-
5 right Act’), and the election system vendor will
6 not bring a claim against a researcher for cir-
7 cumvention of technology controls.

8 “(3) RULE OF CONSTRUCTION.—Nothing in
9 this subsection may be construed to limit or other-
10 wise affect any exception to the general prohibition
11 against the circumvention of technological measures
12 under subparagraph (A) of section 1201(a)(1) of
13 title 17, United States Code, including with respect
14 to any use that is excepted from that general prohi-
15 bition by the Librarian of Congress under subpara-
16 graphs (B) through (D) of such section 1201(a)(1).

17 “(4) EXEMPT FROM DISCLOSURE.—Cybersecu-
18 rity vulnerabilities discovered under the program
19 shall be exempt from section 552 of title 5, United
20 States Code (commonly referred to as the Freedom
21 of Information Act).

22 “(e) DEFINITIONS.—In this section:

23 “(1) CYBERSECURITY VULNERABILITY.—The
24 term ‘cybersecurity vulnerability’ means, with re-

1 spect to an election system, any security vulner-
2 ability that affects the election system.

3 “(2) ELECTION INFRASTRUCTURE.—The term
4 ‘election infrastructure’ means—

5 “(A) storage facilities, polling places, and
6 centralized vote tabulation locations used to
7 support the administration of elections for pub-
8 lic office; and

9 “(B) related information and communica-
10 tions technology, including—

11 “(i) voter registration databases;

12 “(ii) election management systems;

13 “(iii) voting machines;

14 “(iv) electronic mail and other com-
15 munications systems (including electronic
16 mail and other systems of vendors who
17 have entered into contracts with election
18 agencies to support the administration of
19 elections, manage the election process, and
20 report and display election results); and

21 “(v) other systems used to manage
22 the election process and to report and dis-
23 play election results on behalf of an elec-
24 tion agency.

1 “(3) ELECTION SYSTEM.—The term ‘election
2 system’ means any information system that is part
3 of an election infrastructure, including any related
4 information and communications technology de-
5 scribed in paragraph (2)(B).

6 “(4) ELECTION SYSTEM VENDOR.—The term
7 ‘election system vendor’ means any person providing,
8 supporting, or maintaining an election system on be-
9 half of a State or local election official.

10 “(5) INFORMATION SYSTEM.—The term ‘infor-
11 mation system’ has the meaning given the term in
12 section 3502 of title 44, United States Code.

13 “(6) SECRETARY.—The term ‘Secretary’ means
14 the Secretary of Homeland Security.

15 “(7) SECURITY VULNERABILITY.—The term
16 ‘security vulnerability’ has the meaning given the
17 term in section 102 of the Cybersecurity Information
18 Sharing Act of 2015 (6 U.S.C. 1501).”.

19 (b) CLERICAL AMENDMENT.—The table of contents
20 of such Act is amended by adding at the end of the items
21 relating to subtitle D of title II the following:

“PART 7—INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSE-
CURITY VULNERABILITY DISCLOSURE PROGRAM FOR ELECTION SYSTEMS

“Sec. 297. Independent security testing and coordinated cybersecurity vulner-
ability disclosure program for election systems.”.

○