[118H7447]

.....

(Original Signature of Member)

119TH CONGRESS
1ST SESSION

H. R. _____

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

Mr. VALADAO introduced the following bill; which was referred to the Committee on _____

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Strengthening Election Cybersecurity to Uphold Respect for Elections through Independent Testing Act'' or the ''SECURE IT Act''.

SEC. 2. REQUIRING PENETRATION TESTING AS PART OF THE TESTING AND CERTIFICATION OF VOTING SYSTEMS.

Section 231 of the Help America Vote Act of 2002 (52 U.S.C. 20971) is amended by adding at the end the following new subsection:

''(e) REQUIRED PENETRATION TESTING.—

''(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this subsection, the Commission shall provide for the conduct of penetration testing as part of the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories under this section.

''(2) ACCREDITATION.—The Director of the National Institute of Standards and Technology shall recommend to the Commission entities the Director proposes be accredited to carry out penetration testing under this subsection and certify compliance with the penetration testing-related guidelines required by this subsection. The Commission shall vote on the accreditation of any entity recommended.

The requirements for such accreditation shall be a subset of the requirements for accreditation of laboratories under subsection (b) and shall only be based on consideration of an entity's competence to conduct penetration testing under this subsection.''.

SEC. 3. INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PROGRAM FOR ELECTION SYSTEMS.

(a) IN GENERAL.—Subtitle D of title II of the Help America Vote Act of 2002 (42 U.S.C. 15401 et seq.) is amended by adding at the end the following new part:

''PART 7—INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PILOT PROGRAM FOR ELECTION SYSTEMS

''SEC. 297. INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PILOT PROGRAM FOR ELECTION SYSTEMS.

''(a) ESTABLISHMENT.—The Commission, in consultation with the Secretary, shall establish an Independent Security Testing and Coordinated Vulnerability Disclosure Pilot Program for Election Systems (VDP–E) (in this section referred to as the 'program') in order to

test for and disclose cybersecurity vulnerabilities in election systems.

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

''(c) REQUIREMENTS.—In carrying out the program, the Commission, in consultation with the Secretary, shall—

''(1) establish a mechanism by which an election systems vendor may make their election system (including voting machines and source code) available to cybersecurity researchers participating in the program;

''(2) provide for the vetting of cybersecurity researchers prior to their participation in the program, including the conduct of background checks;

''(3) establish terms of participation that—

''(A) describe the scope of testing permitted under the program;

''(B) require researchers to—

''(i) notify the vendor, the Commission, and the Secretary of any cybersecurity vulnerability they identify with respect to an election system; and

''(ii) otherwise keep such vulnerability confidential for 180 days after such notification;

''(C) require the good faith participation of all participants in the program; and

''(D) require an election system vendor, after receiving notification of a critical or high vulnerability (as defined by the National Institute of Standards and Technology) in an election system of the vendor, to—

''(i) send a patch or propound some other fix or mitigation for such vulnerability to the appropriate State and local election officials, in consultation with the researcher who discovered it; and

''(ii) notify the Commission and the Secretary that such patch has been sent to such officials;

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

''(A) for the expedited review of such patch or fix within 90 days after receipt by the Commission; and

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

''(5) 180 days after the disclosure of a vulnerability under paragraph (3)(B)(i), notify the Director of the Cybersecurity and Infrastructure Security Agency of the vulnerability for inclusion in the database of Common Vulnerabilities and Exposures.

''(d) VOLUNTARY PARTICIPATION; SAFE HARBOR.—

''(1) VOLUNTARY PARTICIPATION.—Participation in the program shall be voluntary for election systems vendors and researchers.

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

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

"(B) The research and publication shall be exempt from the anti-circumvention rule of section 1201 of title 17, United States Code (commonly known as the 'Digital Millennium Copyright Act'), and the election system vendor will not bring a claim against a researcher for circumvention of technology controls.

"(3) RULE OF CONSTRUCTION.—Nothing in this subsection may be construed to limit or otherwise affect any exception to the general prohibition against the circumvention of technological measures under subparagraph (A) of section 1201(a)(1) of title 17, United States Code, including with respect to any use that is excepted from that general prohibition by the Librarian of Congress under subparagraphs (B) through (D) of such section 1201(a)(1).

"(4) EXEMPT FROM DISCLOSURE.—Cybersecurity vulnerabilities discovered under the program shall be exempt from section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act).

"(e) DEFINITIONS.—In this section:

"(1) CYBERSECURITY VULNERABILITY.—The term 'cybersecurity vulnerability' means, with re-

spect to an election system, any security vulnerability that affects the election system.

''(2) ELECTION INFRASTRUCTURE.—The term 'election infrastructure' means—

''(A) storage facilities, polling places, and centralized vote tabulation locations used to support the administration of elections for public office; and

''(B) related information and communications technology, including—

''(i) voter registration databases;

''(ii) election management systems;

''(iii) voting machines;

''(iv) electronic mail and other communications systems (including electronic mail and other systems of vendors who have entered into contracts with election agencies to support the administration of elections, manage the election process, and report and display election results); and

''(v) other systems used to manage the election process and to report and display election results on behalf of an election agency.

''(3) ELECTION SYSTEM.—The term 'election system' means any information system that is part of an election infrastructure, including any related information and communications technology described in paragraph (2)(B).

''(4) ELECTION SYSTEM VENDOR.—The term 'election system vendor' means any person providing, supporting, or maintaining an election system on behalf of a State or local election official.

''(5) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

''(6) SECRETARY.—The term 'Secretary' means the Secretary of Homeland Security.

''(7) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).''.

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

''PART 7—INDEPENDENT SECURITY TESTING AND COORDINATED CYBERSECURITY VULNERABILITY DISCLOSURE PROGRAM FOR ELECTION SYSTEMS

''Sec. 297. Independent security testing and coordinated cybersecurity vulnerability disclosure program for election systems.''.