115TH CONGRESS
1ST SESSION

S. 2035

To provide increased security for the voting systems of the United States, to protect against intrusion, theft, manipulation, and deletion of voter registration data and ballots, or votes cast, and to prevent cyberattacks from malicious computer hackers, and for other purposes.

IN THE SENATE OF THE UNITED STATES

OCTOBER 31, 2017

Mr. HEINRICH (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 provide increased security for the voting systems of the United States, to protect against intrusion, theft, manipulation, and deletion of voter registration data and ballots, or votes cast, and to prevent cyberattacks from malicious computer hackers, and for other purposes.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Securing America's Voting Equipment Act of 2017'' or the ''SAVE Act''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 2. DEFINITIONS.

In this Act:

(1) CHIEF STATE ELECTION OFFICIAL.—The term ''chief State election official'' means the chief State election official of a State designated under section 10 of the National Voter Registration Act of 1993 (52 U.S.C. 20509).

(2) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given the term in section 1016 of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c(e)).

(3) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

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

(5) SECTOR-SPECIFIC AGENCY.—The term ''sector-specific agency'' has the meaning given that term in Presidential Policy Directive–21, issued February 12, 2013 (relating to critical infrastructure security and resilience), or any successor thereto.

(6) STATE.—The term ''State'' means each of the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and the territories and possessions of the United States.

(7) VOTING SYSTEM.—The term ''voting system'' has the meaning given the term in section 301(b) of the Help America Vote Act of 2002 (52 U.S.C. 21081(b)).

TITLE I—INFORMATION SHARING WITH STATE ELECTION OFFICIALS

SEC. 101. INFORMATION SHARING WITH STATE ELECTION OFFICIALS.

(a) SECURITY CLEARANCES.—

(1) IN GENERAL.—Not later than 30 days after the date of enactment of this Act, the Director of

National Intelligence shall sponsor a security clearance up to the top secret level for each eligible chief State election official of a State, and up to 1 eligible designee of such an election official, at the time that the chief State election official or designee assumes such position.

(2) DETERMINATION OF LEVELS.—

(A) IN GENERAL.—The Director of National Intelligence shall determine the level of clearances for the positions described in paragraph (1).

(B) INTERIM CLEARANCES.—The Director of National Intelligence, or his designee, may issue interim clearances, for a period to be determined by the Director of National Intelligence, to a chief State election official as described in paragraph (1) and up to 1 designee of such official under such paragraph.

(b) INFORMATION SHARING.—

(1) IN GENERAL.—The Director of National Intelligence shall share appropriate classified information related to threats to voting systems and to the integrity of the election process with chief State election officials and such designees who have received a security clearance under subsection (a).

(2) REPORTS.—The Director of National Intelligence shall transmit reports on such information sharing to the respective chief State election official of any affected State.

TITLE II—PRESERVING THE SECURITY AND INDEPENDENCE OF STATE VOTING SYSTEMS

SEC. 201. DESIGNATION OF VOTING SYSTEMS AS CRITICAL INFRASTRUCTURE.

(a) IN GENERAL.—The Secretary, acting through the Assistant Secretary of the National Protection and Programs Directorate, shall—

(1) designate voting systems used in the United States as critical infrastructure;

(2) include threats of compromise, disruption, or destruction of voting systems in national planning scenarios; and

(3) conduct a campaign to proactively educate local election officials about the designation of voting systems as critical infrastructure and election officials at all levels of government of voting system threats.

(b) SECTOR-SPECIFIC AGENCIES.—The Department and the Election Assistance Commission shall be the sector-specific agencies responsible for coordinating with Sec-

retaries of State and the chief State election officials to promote and ensure the security and resilience of State voting systems.

SEC. 202. VOTING SYSTEM THREAT ASSESSMENT.

(a) THREAT ASSESSMENT.—The Secretary shall, in conjunction with State election officials and the sector specific agencies—

(1) conduct a threat assessment of the physical and electronic risks to voting systems in the United States; and

(2) develop recommended best practices for addressing risks assessed under paragraph (1) in consultation with the National Association of Secretaries of State, National Association of State Election Directors, and National Institute of Standards and Technology.

(b) VOLUNTARY PARTICIPATION.—Participation by a State in the threat assessment conducted under subsection (a) shall be voluntary and at the discretion of the State.

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit a report to Congress and the Director of National Intelligence on the threat assessment conducted under subsection (a), which shall include an estimate of the total cost of implementing the recommended best practices developed under

subsection (a)(2) through the grant program established under section 203.

SEC. 203. GRANT PROGRAM FOR UPGRADING VOTING SYSTEMS.

(a) IN GENERAL.—The Secretary, acting in conjunction with a sector specific agency, shall award grants to States to assist in the development of security solutions for State voting systems.

(b) USE OF FUNDS.—

(1) IN GENERAL.—Subject to paragraph (2), a grant awarded under this section shall be used by a State to upgrade the voting systems of the State to ensure the security and integrity of the physical, electronic, and administrative components of the voting system based upon the threat assessment conducted, and recommended best practices developed, under section 202.

(2) IMPLEMENTATION OF BEST PRACTICES.—A State receiving a grant under this section shall use the grant funds solely to implement the recommended best practices developed under section 202, or alternative practices that are equivalent to or exceed such best practices subject to certification described in subsection (c)(3), before using the grant

to carry out any other uses described in paragraph (1).

(c) APPLICATION.—

(1) IN GENERAL.—A State seeking a grant under this section shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(2) REQUIRED CONTENTS.—An application submitted under paragraph (1) shall include, at a minimum—

(A) an explanation of how the State will use the grant funds to implement the best practices developed by the Secretary under section 202;

(B) an explanation of how the State will update and secure the election machines, vote tally systems, voter registration databases, and voting administration procedures of the State from electronic and physical threats; and

(C) a description of—

(i) the plans of the State for pre- and post-election security and accuracy audits;

(ii) the methods to be implemented by the State for preserving a durable record of votes cast; and

(iii) in the case of a State that chooses to implement an alternative practice that meets or exceeds the best practices, and a certification pursuant to paragraph (3), the reasons for not choosing the recommended best practices developed under section 202.

(3) CERTIFICATION.—A certification described in this paragraph is a certification that the State—

(A) has met the recommended best practices developed under section 202; or

(B) has adopted alternative practices for addressing risks, and the alternative practices have been verified by the National Association of Secretaries of State, National Association of State Election Directors, or National Institute of Standards and Technology as being equivalent to or exceeding the recommended best practices developed under section 202.

(d) ANNUAL AUDIT.—Not later than 1 year after the first fiscal year in which a grant is awarded under this section, and each year thereafter, the Inspector General

of the Department shall conduct an audit of each State that has received a grant during the previous fiscal year to evaluate whether the State has appropriately used the grant funds to upgrade and secure the voting system of the State by implementing the best practices identified in the approved application of the State.

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as are estimated in the report required to be submitted by the Secretary under section 202(c) to be necessary to carry out this section.

TITLE III—COOPERATIVE HACK THE ELECTION PROGRAM

SEC. 301. ESTABLISHMENT OF PROGRAM.

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this title, the Secretary shall develop a program to be known as the ''Cooperative Hack the Election Program''.

(b) PURPOSES OF PROGRAM.—The purpose of the Cooperative Hack the Election Program is to strengthen electoral systems from outside interference by encouraging entrants to work cooperatively with election system vendors to penetrate inactive voting and voter registration systems to discover vulnerabilities of, and develop defenses for, such systems.

SEC. 302. ACTIVITIES UNDER PROGRAM.

In carrying out the Cooperative Hack the Election Program, the Secretary shall—

(1) create an annual competition for hacking into State voting and voter registration systems during periods when such systems are not in use for elections;

(2) award competitors for the discovery of the most significant vulnerabilities of such systems; and

(3) share all discovered vulnerabilities with the relevant vendors of the systems.

SEC. 303. SAFE HARBOR.

(a) IN GENERAL.—Notwithstanding section 1030 of title 18, United States Code, and except as provided in subsection (b), it shall not be unlawful for a person acting in compliance with the ''Cooperative Hack the Election Program'' or a bug bounty program implemented under section 304 to take actions necessary to discover and report a cybersecurity vulnerability in a voting system if the person reports the cybersecurity vulnerability to the Secretary.

(b) LIMITATION.—Subsection (a) shall not apply to any person that—

(1) acts outside the scope of the ''Cooperative Hack the Election Program'' or a bug bounty pro-

gram implemented under section 304, as the case may be;

(2) exploits a cybersecurity vulnerability described in subsection (a); or

(3) publicly exposes a cybersecurity vulnerability described in subsection (a) before reporting the cybersecurity vulnerability to the Secretary.

SEC. 304. BUG BOUNTY PROGRAMS.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Under Secretary for National Protection and Programs Directorate of the Department shall submit a strategic plan to implement bug bounty programs at appropriate agencies and departments of the United States to—

(1) the Committee on Homeland Security and Governmental Affairs of the Senate;

(2) the Select Committee on Intelligence of the Senate;

(3) the Committee on Homeland Security of the House of Representatives; and

(4) the Permanent Select Committee on Intelligence of the House of Representatives.

(b) ASSESSMENT.—The plan under subsection (a) shall include—

(1) an assessment on—

(A) the effectiveness of the ''Hack the Pentagon'' pilot program carried out by the Department of Defense in 2016 and subsequent bug bounty programs in identifying and reporting vulnerabilities within the information systems of the Department of Defense; and

(B) private sector bug bounty programs, including such programs implemented by leading technology companies in the United States; and

(2) recommendations on the feasibility of initiating bug bounty programs at appropriate agencies and departments of the United States.

TITLE IV—VOTING SYSTEM INTEGRITY AUDIT

SEC. 401. AUDIT.

(a) IN GENERAL.—Not later than December 31, 2019, and once every 4 years thereafter, the Comptroller General of the United States shall conduct a robust audit of State voting systems to ensure that elections held using equipment upgraded using grants awarded under section 203 have been conducted in a manner consistent with the goals of the grant program.

(b) LIMITATION.—Each audit conducted under subsection (a) shall include only States that received a grant

under section 203 during the time period covered by the audit.

(c) REPORT.—The Comptroller General of the United States shall submit a report to Congress on each audit conducted under subsection (a).

○