

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.

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the  
5 “Securing America’s Voting Equipment Act of 2017” or  
6 the “SAVE Act”.

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

Sec. 1. Short title; table of contents.  
 Sec. 2. Definitions.

TITLE I—INFORMATION SHARING WITH STATE ELECTION  
 OFFICIALS

Sec. 101. Information sharing with State election officials.

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

Sec. 201. Designation of voting systems as critical infrastructure.  
 Sec. 202. Voting system threat assessment.  
 Sec. 203. Grant program for upgrading voting systems.

TITLE III—COOPERATIVE HACK THE ELECTION PROGRAM

Sec. 301. Establishment of program.  
 Sec. 302. Activities under program.  
 Sec. 303. Safe harbor.  
 Sec. 304. Bug bounty programs.

TITLE IV—VOTING SYSTEM INTEGRITY AUDIT

Sec. 401. Audit.

3 **SEC. 2. DEFINITIONS.**

4 In this Act:

5 (1) CHIEF STATE ELECTION OFFICIAL.—The  
 6 term “chief State election official” means the chief  
 7 State election official of a State designated under  
 8 section 10 of the National Voter Registration Act of  
 9 1993 (52 U.S.C. 20509).

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

1           (3) DEPARTMENT.—The term “Department”  
2 means the Department of Homeland Security.

3           (4) SECRETARY.—The term “Secretary” means  
4 the Secretary of Homeland Security.

5           (5) SECTOR-SPECIFIC AGENCY.—The term  
6 “sector-specific agency” has the meaning given that  
7 term in Presidential Policy Directive–21, issued Feb-  
8 ruary 12, 2013 (relating to critical infrastructure se-  
9 curity and resilience), or any successor thereto.

10          (6) STATE.—The term “State” means each of  
11 the 50 States, the District of Columbia, the Com-  
12 monwealth of Puerto Rico, and the territories and  
13 possessions of the United States.

14          (7) VOTING SYSTEM.—The term “voting sys-  
15 tem” has the meaning given the term in section  
16 301(b) of the Help America Vote Act of 2002 (52  
17 U.S.C. 21081(b)).

18 **TITLE I—INFORMATION SHAR-**  
19 **ING WITH STATE ELECTION**  
20 **OFFICIALS**

21 **SEC. 101. INFORMATION SHARING WITH STATE ELECTION**  
22 **OFFICIALS.**

23 (a) SECURITY CLEARANCES.—

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

1 National Intelligence shall sponsor a security clear-  
2 ance up to the top secret level for each eligible chief  
3 State election official of a State, and up to 1 eligible  
4 designee of such an election official, at the time that  
5 the chief State election official or designee assumes  
6 such position.

7 (2) DETERMINATION OF LEVELS.—

8 (A) IN GENERAL.—The Director of Na-  
9 tional Intelligence shall determine the level of  
10 clearances for the positions described in para-  
11 graph (1).

12 (B) INTERIM CLEARANCES.—The Director  
13 of National Intelligence, or his designee, may  
14 issue interim clearances, for a period to be de-  
15 termined by the Director of National Intel-  
16 ligence, to a chief State election official as de-  
17 scribed in paragraph (1) and up to 1 designee  
18 of such official under such paragraph.

19 (b) INFORMATION SHARING.—

20 (1) IN GENERAL.—The Director of National In-  
21 telligence shall share appropriate classified informa-  
22 tion related to threats to voting systems and to the  
23 integrity of the election process with chief State elec-  
24 tion officials and such designees who have received  
25 a security clearance under subsection (a).

1           (2) REPORTS.—The Director of National Intel-  
2           ligence shall transmit reports on such information  
3           sharing to the respective chief State election official  
4           of any affected State.

5 **TITLE II—PRESERVING THE SE-**  
6 **CURITY AND INDEPENDENCE**  
7 **OF STATE VOTING SYSTEMS**

8 **SEC. 201. DESIGNATION OF VOTING SYSTEMS AS CRITICAL**  
9 **INFRASTRUCTURE.**

10           (a) IN GENERAL.—The Secretary, acting through the  
11 Assistant Secretary of the National Protection and Pro-  
12 grams Directorate, shall—

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

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

18           (3) conduct a campaign to proactively educate  
19 local election officials about the designation of voting  
20 systems as critical infrastructure and election offi-  
21 cials at all levels of government of voting system  
22 threats.

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

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

4 **SEC. 202. VOTING SYSTEM THREAT ASSESSMENT.**

5 (a) **THREAT ASSESSMENT.**—The Secretary shall, in  
6 conjunction with State election officials and the sector spe-  
7 cific agencies—

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

11 (2) develop recommended best practices for ad-  
12 dressing risks assessed under paragraph (1) in con-  
13 sultation with the National Association of Secre-  
14 taries of State, National Association of State Elec-  
15 tion Directors, and National Institute of Standards  
16 and Technology.

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

20 (c) **REPORT.**—Not later than 1 year after the date  
21 of enactment of this Act, the Secretary shall submit a re-  
22 port to Congress and the Director of National Intelligence  
23 on the threat assessment conducted under subsection (a),  
24 which shall include an estimate of the total cost of imple-  
25 menting the recommended best practices developed under

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

3 **SEC. 203. GRANT PROGRAM FOR UPGRADING VOTING SYS-**  
4 **TEMS.**

5 (a) IN GENERAL.—The Secretary, acting in conjunc-  
6 tion with a sector specific agency, shall award grants to  
7 States to assist in the development of security solutions  
8 for State voting systems.

9 (b) USE OF FUNDS.—

10 (1) IN GENERAL.—Subject to paragraph (2), a  
11 grant awarded under this section shall be used by a  
12 State to upgrade the voting systems of the State to  
13 ensure the security and integrity of the physical,  
14 electronic, and administrative components of the vot-  
15 ing system based upon the threat assessment con-  
16 ducted, and recommended best practices developed,  
17 under section 202.

18 (2) IMPLEMENTATION OF BEST PRACTICES.—A  
19 State receiving a grant under this section shall use  
20 the grant funds solely to implement the rec-  
21 ommended best practices developed under section  
22 202, or alternative practices that are equivalent to  
23 or exceed such best practices subject to certification  
24 described in subsection (c)(3), before using the grant

1 to carry out any other uses described in paragraph  
2 (1).

3 (c) APPLICATION.—

4 (1) IN GENERAL.—A State seeking a grant  
5 under this section shall submit to the Secretary an  
6 application at such time, in such manner, and con-  
7 taining such information as the Secretary may re-  
8 quire.

9 (2) REQUIRED CONTENTS.—An application sub-  
10 mitted under paragraph (1) shall include, at a min-  
11 imum—

12 (A) an explanation of how the State will  
13 use the grant funds to implement the best prac-  
14 tices developed by the Secretary under section  
15 202;

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

21 (C) a description of—

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



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

4           (iii) in the case of a State that choos-  
5           es to implement an alternative practice  
6           that meets or exceeds the best practices,  
7           and a certification pursuant to paragraph  
8           (3), the reasons for not choosing the rec-  
9           ommended best practices developed under  
10          section 202.

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

13           (A) has met the recommended best prac-  
14           tices developed under section 202; or

15           (B) has adopted alternative practices for  
16           addressing risks, and the alternative practices  
17           have been verified by the National Association  
18           of Secretaries of State, National Association of  
19           State Election Directors, or National Institute  
20           of Standards and Technology as being equiva-  
21           lent to or exceeding the recommended best  
22           practices developed under section 202.

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

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

7 (e) AUTHORIZATION OF APPROPRIATIONS.—There  
 8 are authorized to be appropriated such sums as are esti-  
 9 mated in the report required to be submitted by the Sec-  
 10 retary under section 202(c) to be necessary to carry out  
 11 this section.

## 12 **TITLE III—COOPERATIVE HACK** 13 **THE ELECTION PROGRAM**

### 14 **SEC. 301. ESTABLISHMENT OF PROGRAM.**

15 (a) IN GENERAL.—Not later than 1 year after the  
 16 date of the enactment of this title, the Secretary shall de-  
 17 velop a program to be known as the “Cooperative Hack  
 18 the Election Program”.

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

1 **SEC. 302. ACTIVITIES UNDER PROGRAM.**

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

4 (1) create an annual competition for hacking  
5 into State voting and voter registration systems dur-  
6 ing periods when such systems are not in use for  
7 elections;

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

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

12 **SEC. 303. SAFE HARBOR.**

13 (a) IN GENERAL.—Notwithstanding section 1030 of  
14 title 18, United States Code, and except as provided in  
15 subsection (b), it shall not be unlawful for a person acting  
16 in compliance with the “Cooperative Hack the Election  
17 Program” or a bug bounty program implemented under  
18 section 304 to take actions necessary to discover and re-  
19 port a cybersecurity vulnerability in a voting system if the  
20 person reports the cybersecurity vulnerability to the Sec-  
21 retary.

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

24 (1) acts outside the scope of the “Cooperative  
25 Hack the Election Program” or a bug bounty pro-

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

3           (2) exploits a cybersecurity vulnerability de-  
4       scribed in subsection (a); or

5           (3) publicly exposes a cybersecurity vulner-  
6       ability described in subsection (a) before reporting  
7       the cybersecurity vulnerability to the Secretary.

8       **SEC. 304. BUG BOUNTY PROGRAMS.**

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

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

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

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

21           (4) the Permanent Select Committee on Intel-  
22      ligence of the House of Representatives.

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

25           (1) an assessment on—

1 (A) the effectiveness of the “Hack the  
 2 Pentagon” pilot program carried out by the De-  
 3 partment of Defense in 2016 and subsequent  
 4 bug bounty programs in identifying and report-  
 5 ing vulnerabilities within the information sys-  
 6 tems of the Department of Defense; and

7 (B) private sector bug bounty programs,  
 8 including such programs implemented by lead-  
 9 ing technology companies in the United States;  
 10 and

11 (2) recommendations on the feasibility of initi-  
 12 ating bug bounty programs at appropriate agencies  
 13 and departments of the United States.

14 **TITLE IV—VOTING SYSTEM**  
 15 **INTEGRITY AUDIT**

16 **SEC. 401. AUDIT.**

17 (a) IN GENERAL.—Not later than December 31,  
 18 2019, and once every 4 years thereafter, the Comptroller  
 19 General of the United States shall conduct a robust audit  
 20 of State voting systems to ensure that elections held using  
 21 equipment upgraded using grants awarded under section  
 22 203 have been conducted in a manner consistent with the  
 23 goals of the grant program.

24 (b) LIMITATION.—Each audit conducted under sub-  
 25 section (a) shall include only States that received a grant

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

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

○